Cisco Unified Communications システム リリース 8.*x* SRND

Cisco Unified Communications System Release 8.x SRND

2011 年 7 月 29 日

Text Part Number: OL-21733-09-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Unified Communications システム 8.x SRND

CONTENTS

はじめに

このマニュアルでは、Cisco Unified Communications Manager 8.*x* および Cisco Unified Communications システムのその他のさまざまなコンポーネントを含む、Cisco Unified Communications システム リリース 8.*x* を配置するための設計上の考慮事項およびガイドラインについて説明します。

このマニュアルは、次の Web サイトで入手可能な他のマニュアルとあわせてお読みください。

- ソリューション リファレンス ネットワーク デザイン（SRND）に関するその他のマニュアル：
  http://www.cisco.com/go/ucsrnd
- Cisco Unified Communications システムの詳細：
  http://www.cisco.com/go/unified-techinfo
  http://www.cisco.com
- Cisco Unified Communications Manager の詳細：
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/tsd_products_support_series_home.html
  http://www.cisco.com
- その他のシスコ設計ガイド：
  http://www.cisco.com/go/designzone

新規情報、またはこのリリースからの変更情報

（注） 特に指定のない限り、このマニュアルの情報は、Cisco Unified Communications システム リリース 8.*x* およびそのコンポーネントに適用されます。

このマニュアルの各章では、新規情報および改訂情報を、「*この章の新規情報*」の項にリストしています。

このマニュアルの内容の多くは、以前のリリースの SRND に似ていますが、Cisco Unified Communications システムのアーキテクチャをより正確に反映するために、大幅に再編成されています。このマニュアルの構造とシステム アーキテクチャをよく理解するために、マニュアル全体を確認することを推奨します。

マニュアルの変更履歴

このマニュアルは、予告なしに更新されることがあります。このマニュアルの最新バージョンは、次の URL から入手できます。

http://www.cisco.com/go/ucsrnd

この Cisco.com の Web サイトを定期的に参照し、お手元のマニュアルの改訂日と Web サイトにあるマニュアルの改訂日とを比較して、更新されているかどうかを確認してください。

次の表では、このマニュアルに対する改訂の履歴をリストしています。

改訂日	マニュアル部品番号	備考
2011 年 7 月 29 日	OL-21733-09-J	さまざまな章を定期的に更新しました。詳細については、各章の「*この章の新規情報*」を参照してください。
2011 年 6 月 30 日	OL-21733-08	さまざまな章を定期的に更新しました。詳細については、各章の「*この章の新規情報*」を参照してください。
2011 年 6 月 2 日	OL-21733-07	Cisco Unified Communications システム Release 8.6 向けに更新しました。
2011 年 3 月 31 日	OL-21733-06	さまざまな章を定期的に更新しました。詳細については、各章の「*この章の新規情報*」を参照してください。
2011 年 2 月 28 日	OL-21733-05	さまざまな章を定期的に更新しました。詳細については、各章の「*この章の新規情報*」を参照してください。
2011 年 1 月 31 日	OL-21733-04	さまざまな章を定期的に更新しました。詳細については、各章の「*この章の新規情報*」を参照してください。
2010 年 11 月 15 日	OL-21733-03	Cisco Unified Communications システム Release 8.5 向けに更新しました。
2010 年 7 月 23 日	OL-21733-02	Cisco Unified Communications システム Release 8.0(2) 向けに更新しました。
2010 年 4 月 2 日	OL-21733-01	Cisco Unified Communications システム 8.0 を対象にしたこのマニュアルの初版です。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

シスコ製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、次の URL で参照できます。

http://www.access.gpo.gov/bis/ear/ear_data.html

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス *時間を節約する*方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「警告」の意味です。人為ミスを予防するための注意事項が記述されています。**

CHAPTER 1

概要

Cisco Unified Communications システムは、標準ベースの Internet Protocol（IP; インターネット プロトコル）を使用して、単一のネットワーク インフラストラクチャ上でデータ、音声、およびビデオを伝送できるようにすることで、完全な統合通信を実現します。Cisco Unified Communications システムは、Cisco IP ハードウェアおよびソフトウェア製品によって提供されるフレームワークを利用して、企業環境における現在および今後の通信ニーズに対応する、比類のないパフォーマンスと高機能をお届けします。またこの製品ファミリは、機能を最適化し、必要な設定と保守を減らし、他のさまざまなアプリケーションとの相互運用性を提供するように設計されています。さらにこのシステムは、このような機能を提供すると同時に、ネットワークで高レベルの可用性、Quality of Service（QoS）、およびセキュリティをも適正に維持します。

Cisco Unified Communications システムには、次の主要な通信技術が内蔵および統合されています。

- IP テレフォニー

  IP テレフォニーとは、IP 標準を使用して、ネットワーク上で音声通信を伝送するためのテクノロジーです。Cisco Unified Communications には、コール処理エージェント、IP Phone（有線と無線の両方）、音声メッセージング システム、ビデオ デバイス、および多数の特殊アプリケーションなど、多彩なハードウェアおよびソフトウェア製品が含まれています。

- カスタマー コンタクト センター

  Cisco IP Contact Center は、グローバルに展開されたネットワークにおいて、効率的かつ効果的なカスタマー コミュニケーションを促進するための方法とアーキテクチャを組み合せた製品です。このソリューションを利用することにより、より広範なリソースを駆使したカスタマー サービスが可能になります。たとえば、大規模なエージェント プールへのアクセス、複数のコミュニケーション手段、およびカスタマー セルフヘルプ ツールなどが用意されています。

- ビデオ テレフォニー

  Cisco Unified Video Advantage 製品を使用すると、Cisco Unified Communications と同じ IP ネットワークおよびコール処理エージェントを使用して、リアルタイムのビデオ通信およびコラボレーションを行うことができます。Cisco Unified Video Advantage では、電話番号をダイヤルするのと同じくらい簡単にビデオ コールを発信できます。

- リッチメディア会議

  Cisco Unified MeetingPlace、Cisco Unified Videoconferencing、および Cisco WebEx Software-as-a-Service は、音声、ビデオ、および Web 会議に対応した IP ベースの統合ツール セットにより、仮想的な会議環境を拡張します。

- モビリティ

  シスコのワイヤレスおよびモビリティ ソリューションは、ロケーションやクライアント デバイスに関係なくネットワーク リソースやアプリケーションへの安全なアクセスを可能にすることで、ユーザの生産性と応答性を高めます。

- TelePresence

  Cisco TelePresence は、高度なビジュアル、オーディオ、そしてコラボレーション テクノロジーにより、仕事や私生活において、人と人、場所と場所をつなぎ、リアルタイムな対面式の対話を可能にします。これらのテクノロジーは、実物大の高解像度画像と空間ディスクリート オーディオによって、たとえお互いが世界の反対側にいようとも、まるで同じ部屋で会話をしているような臨場感を可能にします。

- アプリケーション

  シスコでは、数多くの組み込みアプリケーションを提供する以外に、最先端の企業と協力して、メッセージング、カスタマー ケア、およびワークフォース オプティマイゼーションなど、重要なビジネス ニーズに焦点を当てた革新的なサードパーティ製ユニファイド コミュニケーション アプリケーションおよび製品を種類豊富に提供しています。

このマニュアルでは、これらのテクノロジーおよびアプリケーションを Cisco Unified Communications システムに展開するための、設計上の考慮事項を中心に説明します。

Cisco Unified Communications システムのその他の要素については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/go/ucsrnd

http://www.cisco.com/go/unified-techinfo

Cisco Unified Communications 製品ファミリのその他のマニュアルは、次の Web サイトにもあります。

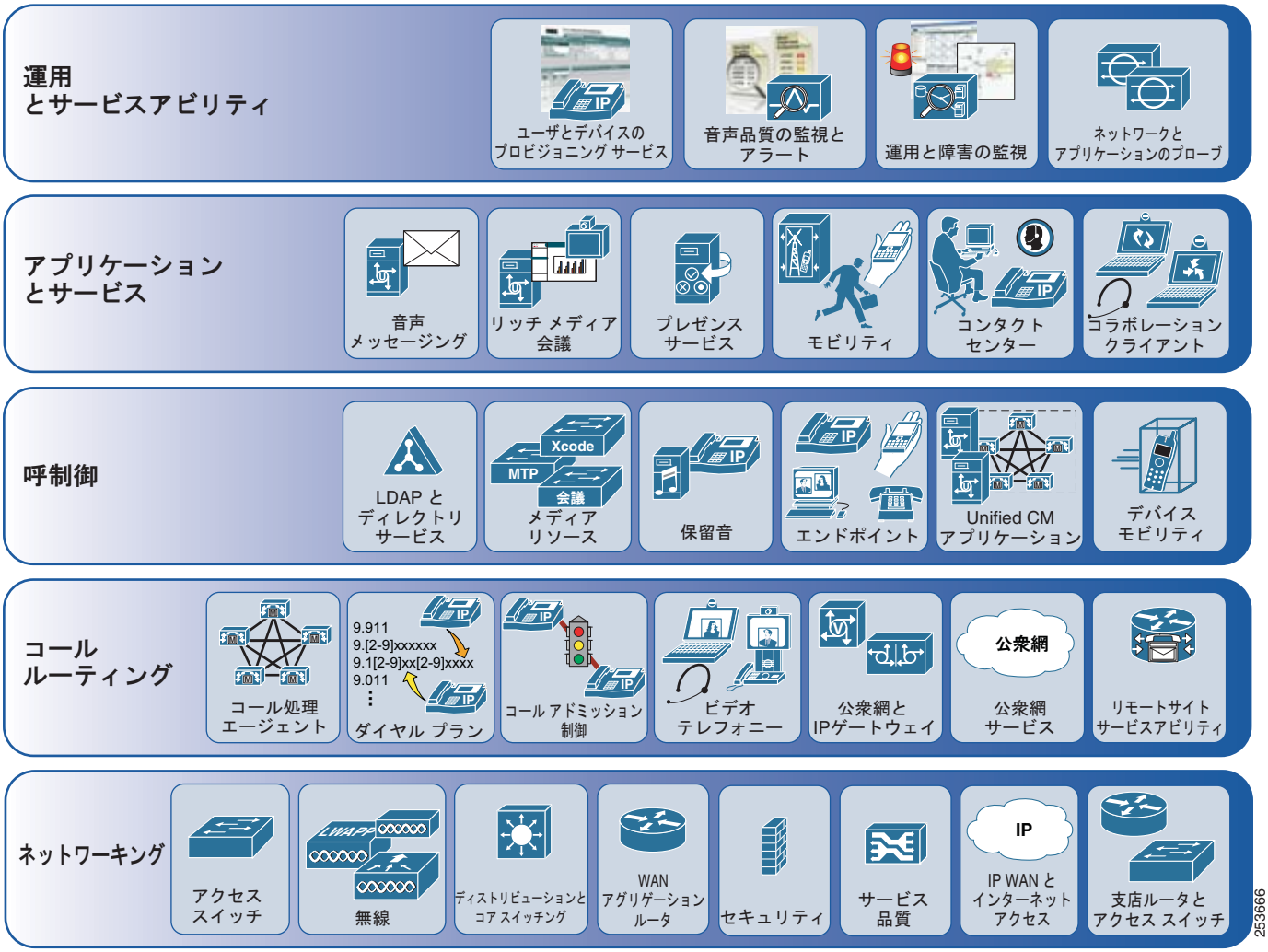
http://www.cisco.com

（注） このマニュアルに記載された設計指針は、エンタープライズ向けの Unified Communications ソリューションの展開を考えているお客様またはパートナーに適用されます。ホスト型または管理型の Unified Communications ソリューションに興味がある方は、http://www.cisco.com/go/hostedcollab にアクセスして詳細を確認してください。

Cisco Unified Communications システムのアーキテクチャ

図 1-1 は、Cisco Unified Communications システムのアーキテクチャ レイヤを示しています。

図 1-1　Cisco Unified Communications システムのアーキテクチャ



Cisco Unified Communications システムのさまざまなレイヤで、次の主要なタスクおよび役割が実行されます。

- ネットワーキング

  このレイヤでは、Unified Communications ネットワークの基盤が形成されます。このレイヤには、次の機能および能力を提供するコンポーネントが含まれます。

  – ネットワーク インフラストラクチャでは、Quality of Service（QoS）を Unified Communications アプリケーションで使用可能にすることで、冗長性と復元性を備えたネットワーク基盤が保証されます。

- 音声セキュリティでは、一般的なセキュリティ ポリシー、および強固でセキュアなネットワーキング基盤が Unified Communications アプリケーションに保証されます。
- Unified Communications の配置モデルでは、テスト済みのモデル以外に、Unified Communications システムを配置するためのベスト プラクティスと設計ガイドラインを提供します。
- IP テレフォニーの移行オプションでは、音声、ビデオ、およびコラボレーションのスタンドアロン システムから統合 Cisco Unified Communications システムへの移行を計画および着手する方法に関するガイドラインを提供します。

ネットワーキング レイヤの詳細については、「Cisco Unified Communications ネットワーキングの概要」（P.2-1）を参照してください。

- コール ルーティング

  このレイヤでは、システム全体のコールの処理およびルーティングを行います。このレイヤには、次の機能および能力を提供するコンポーネントが含まれます。

  - コール処理エージェントでは、テレフォニー サービスとコール ルーティングの機能を提供します。
  - ダイヤル プランでは、ユーザが行うことができるコールのタイプを制限するために、エンドポイントの番号、ダイヤルされる番号の分析、および制限クラスを提供します。
  - コール アドミッション制御では、コール処理コンポーネントおよびネットワーク帯域幅の全体的なコール キャパシティに基づいて、所定の時間にネットワーク上で許可するコール数を制限することにより、ネットワーク帯域幅のオーバーサブスクリプションを回避するメカニズムを提供します。
  - ビデオ テレフォニー サービスでは、ビデオ エンドポイントをプロビジョニングおよび登録する機能以外に、ネットワーク上でビデオ コールを設定、ルーティング、および維持する機能を提供します。
  - PSTN ゲートウェイおよびプロバイダーの音声とデータ サービスでは、PSTN、インターネット、サービス プロバイダー IP ベースのトランクなど、企業外部の音声およびデータ ネットワークへのアクセスを提供します。
  - リモート サイトのサバイバビリティでは、ネットワーク接続の障害またはフラッピングが原因で中央サイトのテレフォニー サービスが使用できなくなった場合に、基本的なテレフォニー サービスをリモート サイトで継続して使用できるようにします。

  コール ルーティング レイヤの詳細については、「Cisco Unified Communications コール ルーティングの概要」（P.7-1）を参照してください。

- 呼制御

  このレイヤによって、ユーザはコールを開始および管理できます。このレイヤには、次の機能および能力を提供するコンポーネントが含まれます。

  - 中央の Lightweight Directory Access Protocol（LDAP）ディレクトリとの統合により、企業は、Unified Communications アプリケーションが利用できる単一リポジトリにすべてのユーザ情報を集中化させることができます。追加、移動、および変更が簡単であるため、保守コストも大幅に削減されます。
  - メディア リソースにアクセスして、会議、メディア ターミネーション、トランスコーディング、エコー キャンセレーション、シグナリング、ストリームのパケット化、オーディオのストリーミング（Annunciator）などのメディア処理機能を実行できます。
  - 保留音では、発信者の通話が保留、転送、一時保留（コール パーク）、または ad-hoc 会議に追加されるときに、発信者に音楽（または通知）を流します。

- Unified Communications のエンドポイントおよび機能セットは、IP 環境内の通常のアナログ電話をサポートするゲートウェイから、さまざまな機能をエンド ユーザに提供するネイティブ IP Phone の拡張的なセットに至るまで、多岐にわたります。
- デバイス モビリティ機能により、モバイル ユーザは、エンドポイント デバイスを使用して 1 つのサイトから別のサイトにローミングし、動的に割り当てられたローミング サイトの設定を取得して、コール ルーティング、コーデックの選択、メディア リソースの選択などを実行できます。
- 呼制御ソフトウェアに組み込まれたアプリケーションでは、クリックコール ダイヤル、マネージャ アシスタント アプリケーション、ユーザによる任意の電話へのログイン機能などの機能を提供するほか、ユーザのデスクトップ電話機上で直接実行できる Web ベースのアプリケーションをサポートしています。

呼制御レイヤの詳細については、「Cisco Unified Communications の呼制御の概要」（P.15-1）を参照してください。

- アプリケーションとサービス

  このレイヤには、既存の Cisco Unified Communications インフラストラクチャの最上位に配置して、システムに拡張ユーザ機能を追加できる多数のアプリケーションとサービスが含まれています。このレイヤには、次の機能および能力を提供するコンポーネントが含まれます。

  - 音声メッセージングでは、ボイスメール サービスおよびメッセージ待機インジケータを提供します。
  - リッチ メディア会議では、音声会議とビデオ会議、および Web ベースのアプリケーションとドキュメント共有を提供します。
  - プレゼンス サービスでは、ユーザ デバイスおよびクライアントでのユーザの応答可能性を確認します。
  - モビリティ サービスでは、企業レベルの Unified Communications 機能を企業外部のユーザに提供します。
  - コンタクト センター アプリケーションでは、大規模コールのコール処理、キューイング、およびモニタリングを提供します。
  - コラボレーション クライアント サービスでは、Unified Communications サービスとの統合を提供し、さまざまなアプリケーションを活用できるようにします。

  アプリケーションとサービスのレイヤの詳細については、「Cisco Unified Communications アプリケーションおよびサービスの概要」（P.20-1）を参照してください。

- 運用とサービスアビリティ

  このレイヤには、Unified Communications のネットワークとアプリケーションをモニタおよび管理するためのシステムレベルのサービスが含まれています。このレイヤには、次の機能および能力を提供するコンポーネントが含まれます。

  - ユーザとデバイスのプロビジョニング サービスは、ユーザとデバイスの集中型プロビジョニングおよび設定を Unified Communications アプリケーションおよびサービスで可能にします。
  - 音声品質のモニタリングおよびアラートは、システム内のさまざまなコール フローをモニタして、音声品質が許容できるかどうかを判別し、音声品質が許容できない場合は、管理者に警告します。
  - 運用と障害のモニタリングは、アプリケーションとサービスのすべての処理をモニタし、ネットワークおよびアプリケーションの障害に関して管理者に警告します。
  - ネットワークとアプリケーションのプローブは、配置全体のさまざまなロケーションでネットワークとアプリケーションのトラフィック情報をプローブおよび収集し、管理者がこの情報を中央ロケーションから取得できるようにします。

運用とサービスアビリティのレイヤの詳細については、「Cisco Unified Communications の運用とサービスアビリティの概要」（P.27-1）を参照してください。

（注）　このマニュアルでの設計上の推奨をレビューし、Cisco Borderless Network Smart Business Architecture（SBA）との一貫性が取れていることを確認しました。SBA の詳細については、シスコ担当者にお問い合せください。

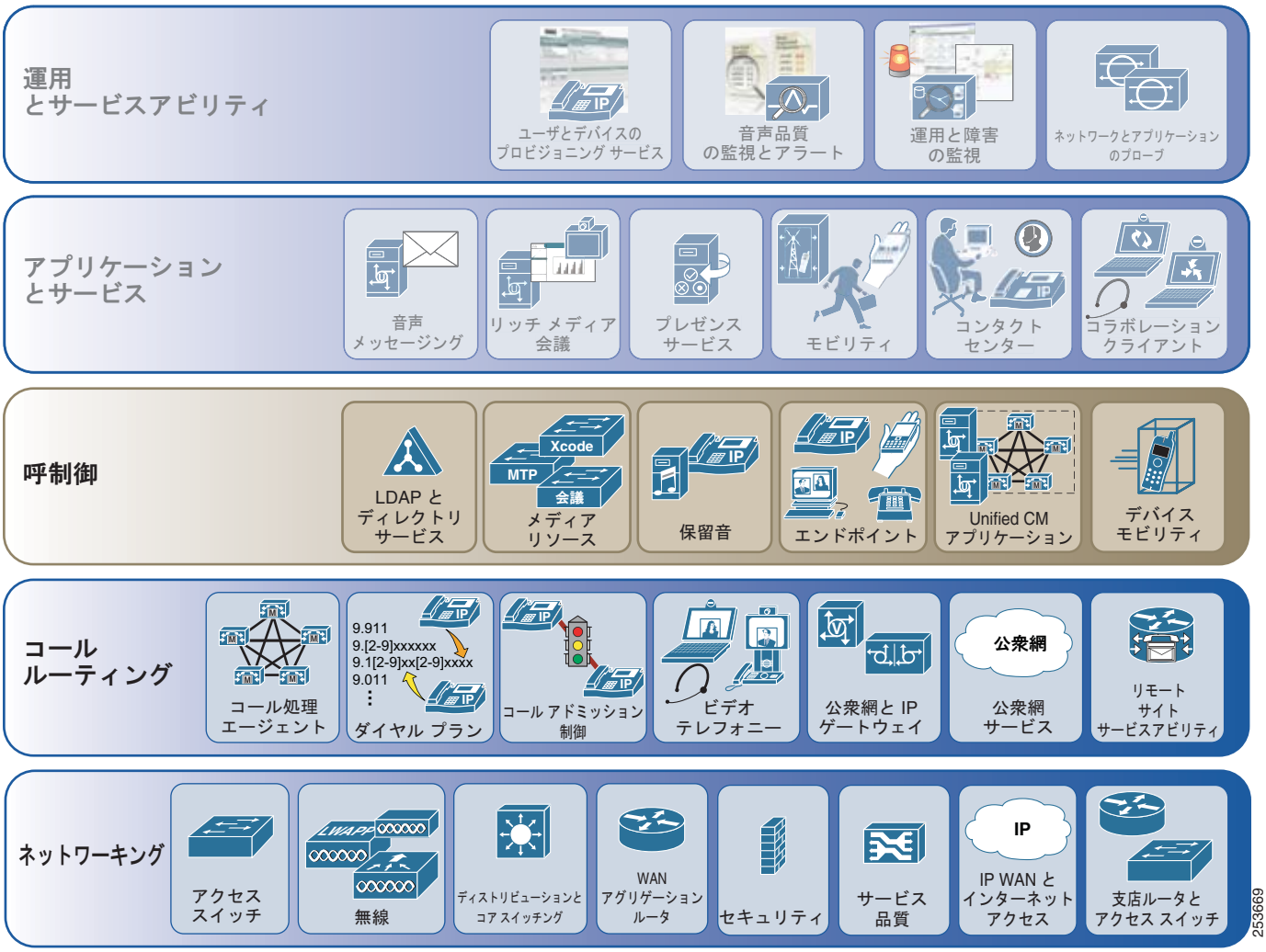
この設計マニュアルの使用方法

このマニュアルでは、Cisco Unified Communications システムを配置するための、設計上の考慮事項、ガイドライン、およびベスト プラクティスについて説明します。前の項で説明したように、Cisco Unified Communications システムのアーキテクチャは、5 つのレイヤで構成されています。このマニュアルは、これら 5 つのアーキテクチャ レイヤに対応する 5 つのパートに分かれています。このマニュアルの各パートには、対応するアーキテクチャ レイヤに関するコンポーネントおよび設計上のガイドラインを説明する章が含まれています。

適切な Unified Communications システムの構築プロセスは、家の建築に似ています。最初に安定したインフラストラクチャと基盤を確立し、その上に他のすべてのレイヤを構築する必要があります。また、他のレイヤを追加する場合は、特定の順序で行う必要があります。通常は、下から上に追加します（たとえば、家の壁を作った後、その上に屋根を作ります）。Unified Communications システムの場合は、ネットワーキング レイヤがインフラストラクチャを提供し、他のレイヤは、図 1-1 に示す順序で下から上に追加する必要があります。このマニュアルのパートおよび章は、これと同じ順序で編成されているため、Unified Communications システムを設計するための論理プロセスの確立に役立ちます。

このマニュアルの各パートの最初の章では、そのパートに含まれている情報の概要を示しています。概要には、Cisco Unified Communications システムの 5 つのアーキテクチャ レイヤの図が含まれており、このマニュアルのそのパートで説明されるレイヤが強調されています。たとえば、図 1-2 は、このマニュアルの呼制御パートの図です。呼制御レイヤは、このマニュアルのそのパートで説明するレイヤであることを示すために、異なる色で強調されています。その下のレイヤ（ネットワーキングとコール ルーティング）は、呼制御レイヤを実装する前にすでに配置されている必要があるため、強調されています。その上のレイヤ（アプリケーションとサービス、および運用とサービスアビリティ）は、現在のレイヤ（ここでは呼制御レイヤ）が配置されるまで実装できないことを示すために淡色となっています。

図 1-2　Cisco Unified Communications の呼制御アーキテクチャ



新しい Unified Communications システムを設計する場合は、このマニュアルに示す順序およびガイドラインに従って設計を進めることを推奨します。システムの一部のレイヤがすでに配置されており、そこに他のレイヤを追加する場合は、少なくとも、このマニュアルで既存のレイヤに関係する項を確認して、ご使用のシステムですべてのガイドラインが確実に準拠されるようにしてください。

PART 1

Unified Communications ネットワーキング

CHAPTER 2

Cisco Unified Communications ネットワーキングの概要

Unified Communications システムを企業環境に適切に構築するには、安定したネットワーク インフラストラクチャが必要となります。ネットワーク アーキテクチャでは、これ以外に、音声セキュリティ、ユニファイド コミュニケーション配置モデル、および移行計画が重要な側面となります。

IP テレフォニー、リッチ メディア、コラボレーション、およびその他の多数の機能を含む Unified Communications では、IP パケット損失、パケット遅延、および遅延変動（またはジッタ）について、厳しい要件を課します。したがって、ネットワーク全体の Cisco スイッチおよびルータで使用できる QoS メカニズムの大部分を使用可能にする必要があります。これと同じ理由で、可用性の高いインフラストラクチャを保証するには、ネットワーク障害またはトポロジ変更の発生後に迅速に収束する、冗長なデバイスおよびネットワーク リンクも重要です。次に、Unified Communications ネットワーキングのトピックに不可欠な側面を、重要度および相互に関連する順序で示します。

- ネットワーク インフラストラクチャ：QoS を Unified Communications アプリケーションで使用可能にすることで、冗長性と復元性を備えた基盤を保証します。
- 音声セキュリティ：Unified Communications アプリケーションの一般的なセキュリティ ポリシーを保証し、これらのアプリケーションが依存する強固でセキュアなネットワーキング基盤を保証します。
- Unified Communications 配置モデル：Unified Communications 呼制御およびアプリケーションを配置するためのテスト済みモデル以外に、Unified Communications 配置に適用するためのベスト プラクティスと設計ガイドラインを提供します。
- IP テレフォニーの移行オプション：音声、ビデオ、およびコラボレーションの個々のスタンドアロン システムから統合 Cisco Unified Communications システムへの移行を計画および着手する方法に関するガイドラインを提供します。

本 SRND のこの章では、上記のネットワーキング項目について説明します。各章では、対象となる項目の概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。各章では、設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこの部分に含まれる章は、次のとおりです。

- 「ネットワーク インフラストラクチャ」（P.3-1）

  この章では、企業環境で Cisco Unified Communications システムを構築するために必要なネットワーク インフラストラクチャの要件について説明します。この章の各項では、LAN、WAN、およびワイヤレス LAN の各インフラストラクチャに関連する、ネットワーク インフラストラクチャ機能について説明します。各章では、各インフラストラクチャに関係する設計、ハイ アベイラビリティ、Quality of Service、および帯域幅プロビジョニングの領域について説明します。

- 「Unified Communications のセキュリティ」（P.4-1）

  この章では、Unified Communications ネットワークを保護するためのガイドラインと推奨事項について説明します。この章の各トピックの範囲は、ポリシーやインフラストラクチャ保護などの一般的なセキュリティから、VLAN、スイッチ ポート、および QoS での電話機のセキュリティまでにわたります。この章では、その他のセキュリティの側面として、アクセス コントロール リスト、ゲートウェイとメディア リソースの保護、ファイアウォール、データ センターの設計、アプリケーション サーバの保護、およびネットワーク バーチャライゼーションについて説明します。

- 「Unified Communications の配置モデル」（P.5-1）

  この章では、単一のサイトまたはキャンパス、マルチサイト環境、データ センター ソリューションなどのさまざまなネットワーク インフラストラクチャに関連する、Cisco Unified Communications Manager の配置モデルについて説明します。この章では、これらの配置モデル、および各モデルのベスト プラクティスと設計上の考慮事項にいて説明します。説明するモデルに関係するその他の多数のサブトピックについても説明します。

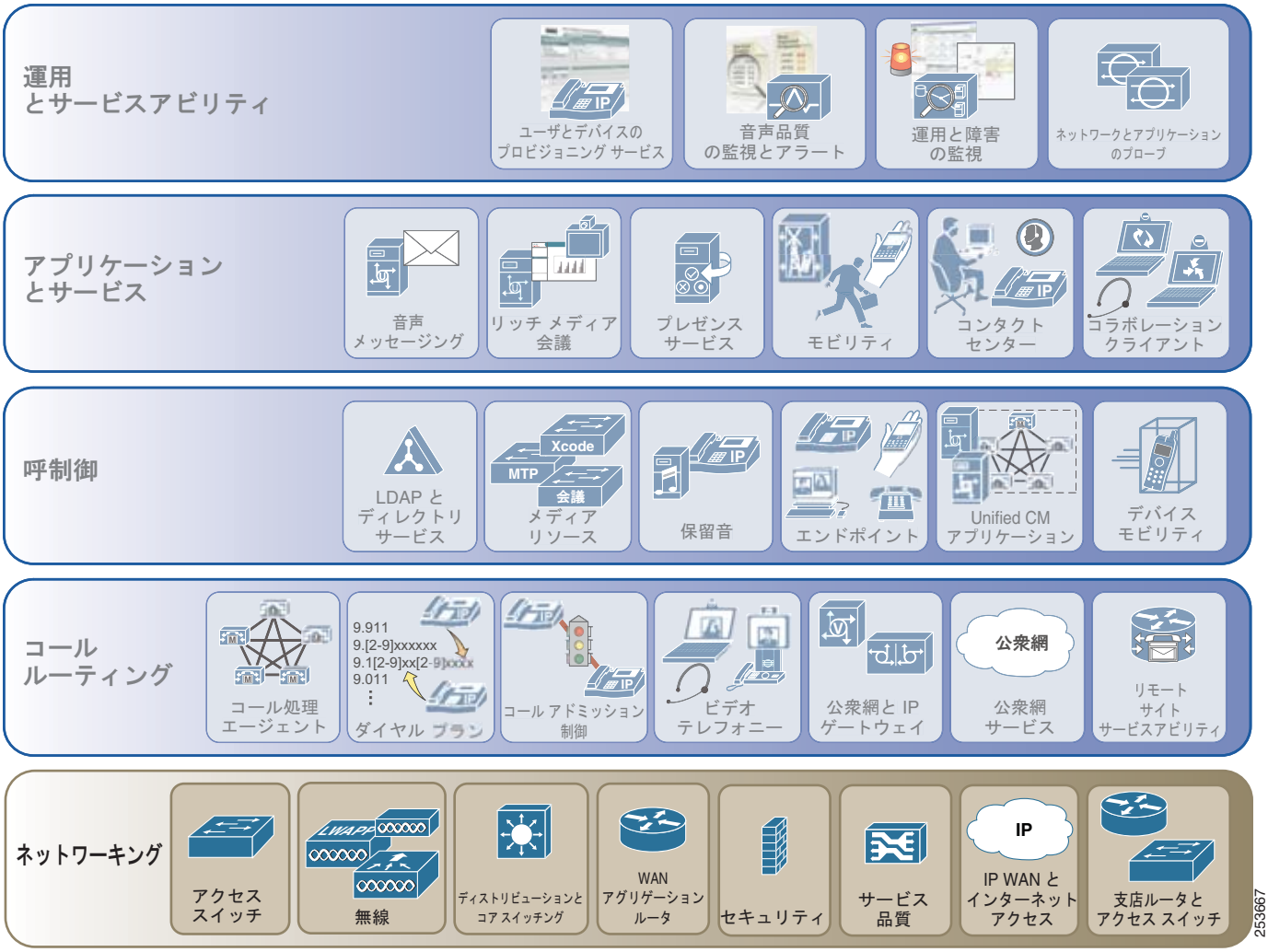
- 「IP テレフォニーの移行オプション」（P.6-1）

  この章では、音声、ビデオ、およびコラボレーションの個々のスタンドアロン システムから統合 Cisco Unified Communications システムに移行するための複数の方法について説明します。段階的な移行と並行カットオーバーの両方について、利点と欠点を説明します。Private Branch Exchange（PBX; 構内交換機）を新しい Unified Communications システムに接続するために必要なサービスについても説明します。この章で説明する主要なトピックには、IP テレフォニーの移行、ビデオの移行、および音声とデスクトップ コラボレーション システムの移行が含まれます。

アーキテクチャ

ネットワーキング アーキテクチャによって、Unified Communications システムのすべてのレイヤが配置される基盤が構築されます。図 2-1 は、Cisco Unified Communications システム アーキテクチャ全体におけるネットワーキング レイヤの論理ロケーションを示しています。

図 2-1　Cisco Unified Communications のネットワーキング アーキテクチャ



Unified Communications システムのその他のアーキテクチャ（コール ルーティング、呼制御、アプリケーションとサービス、運用とサービスアビリティなど）は、ネットワークが整備されていないと、サービスの提供が難しくなります。ネットワーキング レイヤは、アプリケーションがネットワーク サービスに確実にアクセスできるようにするために必要となる Quality of Service を提供するという点で、堅固な Unified Communications 基盤の最も重要な唯一の側面です。ネットワーキング レイヤによって、サーバの適切な配置およびエンドポイントとサービス用の適切な帯域幅が保証され、効率的かつ安全に通信することもできます。

ハイ アベイラビリティ

適切なネットワーク インフラストラクチャの設計では、堅固で冗長なネットワークをボトムアップに構築する必要があります。LAN をレイヤ モデル（アクセス レイヤ、ディストリビューション レイヤ、およびコア レイヤ）として構築し、LAN インフラストラクチャのモデルを 1 段階ずつ開発することで、可用性の高い、耐障害性のある冗長なネットワークを構築できます。統合されたネットワーク上で IP テレフォニーを正常に動作させるには、WAN インフラストラクチャを適切に設計することもきわめて重要です。インフラストラクチャを適切に設計するには、基本的な設定と設計に関するベスト プラクティスに従って、できるだけ可用性の高い、スループットを保証できる WAN を配置する必要があります。さらに、WAN インフラストラクチャを適切に設計するには、すべての WAN リンク上にエンドツーエンド QoS を配置する必要もあります。

統合されたネットワークのワイヤレス LAN（WLAN）部分に IP テレフォニーを追加する場合は、ワイヤレス LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless IP Phone 7921G、7925G などの無線 Unified Communications エンドポイントが追加されている場合、音声トラフィックは WLAN 上に移動しているため、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN インフラストラクチャの場合と同様、WLAN に音声を追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質を保証するために、QoS を理解してワイヤレス ネットワーク上に配置する必要もあります。

ネットワーク インフラストラクチャを適切に設計および実装すると、ネットワーク サービスとアプリケーション サービスをネットワーク全体に適切に追加できます。これにより、Unified Communications サービスを実行できる、可用性の高い基盤が提供されます。

キャパシティ プランニング

ネットワーク インフラストラクチャを拡張して、ネットワーク インフラストラクチャがサポートする必要がある Unified Communications アプリケーションとサービスを処理するには、アプリケーションによって発生する追加のトラフィック負荷を処理するために、適切で使用可能な帯域幅とキャパシティを提供する必要があります。

CHAPTER 3

ネットワーク インフラストラクチャ

この章では、企業環境で Cisco Unified Communications システムを構築するために必要なネットワーク インフラストラクチャの要件について説明します。図 3-1 はネットワーク インフラストラクチャを形成する各種のデバイスの役割を示し、表 3-1 はこれらの各役割をサポートするために必要な機能を要約したものです。

Unified Communications には、IP パケット損失、パケット遅延、および遅延変動（またはジッタ）について厳しい要件があります。したがって、ネットワーク全体の Cisco スイッチおよびルータで使用できる QoS メカニズムの大部分を使用可能にする必要があります。これと同じ理由で、可用性の高いインフラストラクチャを保証するには、ネットワーク障害またはトポロジ変更の発生後に迅速に収束する、冗長なデバイスおよびネットワーク リンクも重要です。

次の項では、関連するネットワーク インフラストラクチャの機能について説明します。

図 3-1　一般的なキャンパス ネットワーク インフラストラクチャ

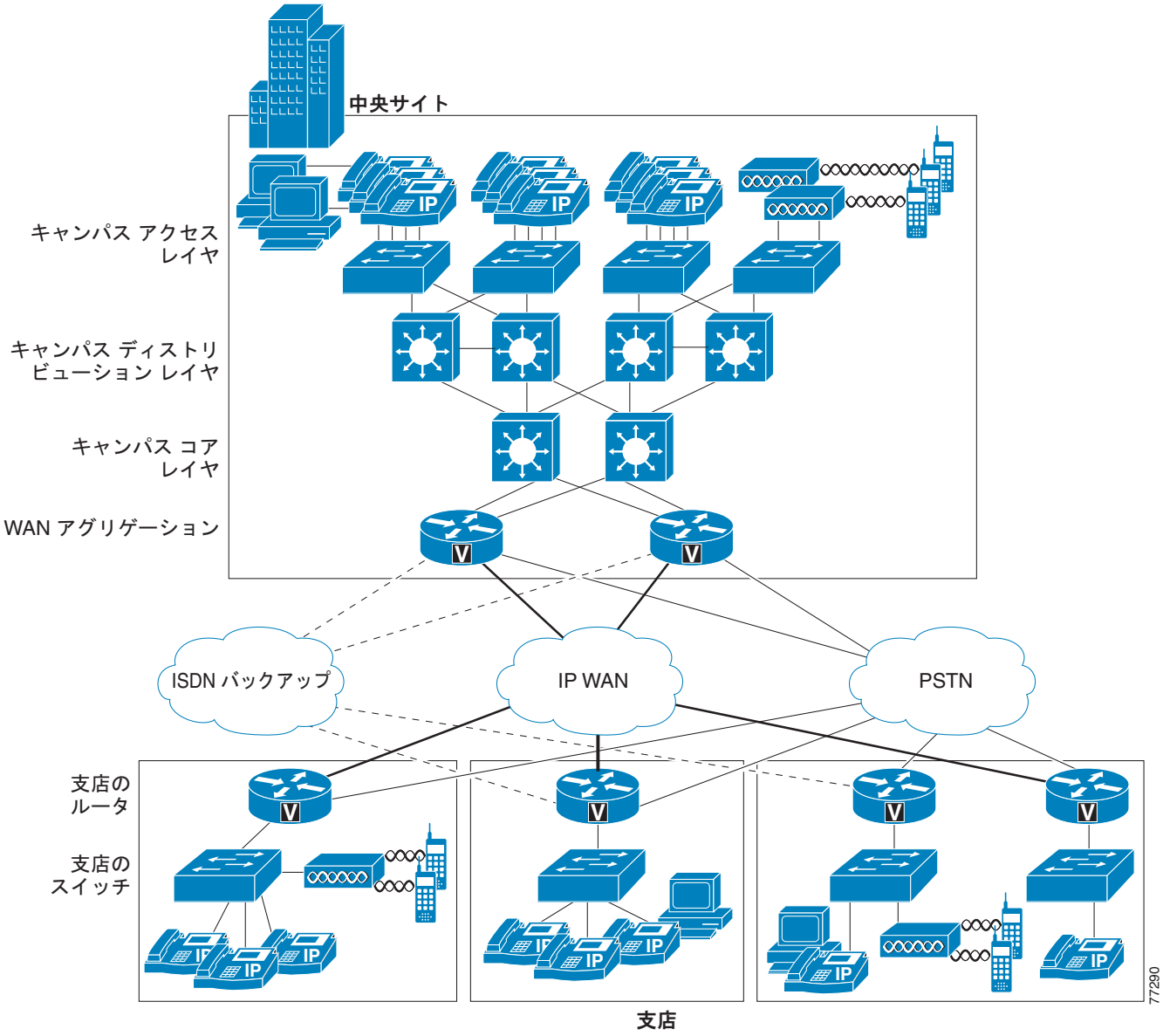


表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

インフラストラクチャの役割	必要な機能
キャンパス アクセス スイッチ	• インライン パワー[1] • 複数キュー サポート • 802.1p および 802.1Q • 高速リンク コンバージェンス
キャンパス ディストリビューション スイッチまたはコア スイッチ	• 複数キュー サポート • 802.1p および 802.1Q • トラフィック分類 • トラフィック再分類
WAN アグリゲーション ルータ（ネットワークのハブ サイト）	• 複数キュー サポート • トラフィック シェーピング • リンク フラグメンテーション/インターリーブ（LFI）[2] • リンク効率化 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店ルータ（スポーク サイト）	• 複数キュー サポート • LFI[2] • リンク効率化 • トラフィック分類 • トラフィック再分類 • 802.1p および 802.1Q
支店または小規模サイトのスイッチ	• インライン パワー[1] • 複数キュー サポート • 802.1p および 802.1Q

1. 推奨作業です。
2. リンク速度が 786 kbps を下回る場合。

この章の新規情報

表 3-2 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 3-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 6 月 2 日
仮想 Unified Communications システム	「Cisco UCS B シリーズ ブレード サーバを使用した仮想 Unified Communications に関する QoS 設計上の考慮事項」（P.3-20）	2010 年 4 月 2 日
Cisco IOS Service Advertisement Framework（SAF）	「Service Advertisement Framework（SAF）」（P.3-64）	2010 年 4 月 2 日

LAN インフラストラクチャ

統合されたネットワーク上で Unified Communications を正常に動作させるには、キャンパス LAN インフラストラクチャの設計が極めて重要です。LAN インフラストラクチャを適切に設計するには、次の基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。さらに、LAN インフラストラクチャを適切に設計するには、ネットワーク上にエンドツーエンド QoS を配置する必要もあります。次の項では、これらの要件について説明します。

- 「ハイ アベイラビリティのための LAN 設計」（P.3-4）
- 「LAN の QoS」（P.3-15）

ハイ アベイラビリティのための LAN 設計

LAN を適切に設計するには、堅牢かつ冗長なネットワークをトップダウン方式で構築する必要があります。LAN をレイヤ モデルとして構築し（図 3-1 を参照）、LAN インフラストラクチャのモデルを 1 段階ずつ開発することで、可用性の高い、耐障害性のある冗長なネットワークを構築できます。これらのレイヤを適切に設計してから、追加のネットワーク機能を提供するために、DHCP や TFTP などのネットワーク サービスを追加できます。次の項では、インフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「キャンパス アクセス レイヤ」（P.3-5）
- 「キャンパス ディストリビューション レイヤ」（P.3-10）
- 「キャンパス コア レイヤ」（P.3-12）
- 「ネットワーク サービス」（P.3-22）

キャンパスの設計の詳細については、次の Web サイトで入手可能な『*Design Zone for Campus*』を参照してください。

http://www.cisco.com/go/designzone

キャンパス アクセス レイヤ

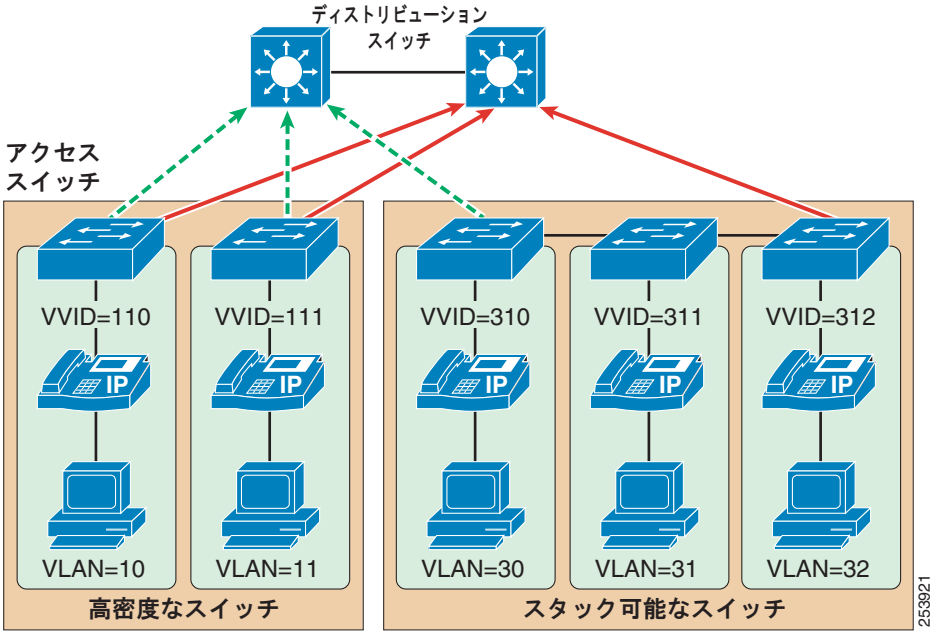
キャンパス LAN のアクセス レイヤに含まれるネットワーク部分は、デスクトップ ポートからワイヤリング クローゼット スイッチまでです。従来、アクセス レイヤ スイッチはディストリビューション レイヤへのレイヤ 2 アップリンクを持つレイヤ 2 デバイスとして設定されてきました。レイヤ 2 およびレイヤ 2 アクセス設計に対応するスパニング ツリーの推奨事項は、十分に実証されており、次に簡単に説明します。レイヤ 3 プロトコルをサポートする最新の Cisco Catalyst スイッチでは、新しいルーテッド アクセス設計が可能となり、コンバージェンス時間と設計の簡素化における改善が行われています。ルーテッド アクセス設計については、「ルーテッド アクセス レイヤ設計」（P.3-8）の項で詳しく説明します。

レイヤ 2 アクセス設計の推奨事項

アクセス レイヤを適切に設計するには、最初に、Virtual LAN（VLAN）ごとに単一の IP サブネットを割り当てます。一般に、VLAN は、複数のワイヤリング クローゼット スイッチにまたがってはいけません。つまり、ある VLAN が存在するアクセス レイヤ スイッチは 1 つだけである必要があります（図 3-2 を参照）。この方法にすると、レイヤ 2 からトポロジ上のループが排除されるため、スパニング ツリーのコンバージェンスによってフローが一時的に中断することがなくなります。ただし、標準ベースの IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）と 802.1s Multiple Instance Spanning Tree Protocol（MISTP）を導入すると、スパニング ツリーが収束する速度が大幅に高くなる可能性があります。さらに重要なことに、VLAN を単一のアクセス レイヤ スイッチに限定すると、ブロードキャスト ドメインのサイズが制限されます。単一の VLAN またはブロードキャスト ドメインにある多数のデバイスによって、大量のブロードキャスト トラフィックが定期的に生成される可能性があり、これが問題となる場合があります。そのため、VLAN ごとのデバイス数を 512 程度に制限することを推奨します。この数は、2 つのクラス C サブネット（つまり、23 ビットのサブネットがマスクされたクラス C アドレス）に相当します。キャンパス アクセス レイヤの詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html で入手可能なマニュアルを参照してください。

（注）　単一の Unified Communications VLAN におけるデバイス数を 512 ほどに制限する推奨事項は、ただ単に VLAN ブロードキャスト トラフィックの量を制御するためにだけ、必要な事項ではありません。Linux ベースの Unified CM サーバ プラットフォームでは、ARP キャッシュには 1024 デバイスの絶対的な制限があります。1024 を超えるデバイスを含む IP サブネットのある VLAN に Unified CM をインストールすると、Unified CM サーバの ARP キャッシュがすぐに満杯になる可能性があり、Unified CM サーバとその他の Unified Communications のエンドポイント間の通信に深刻な影響を及ぼす場合があります。Windows ベースの Unified CM サーバ プラットフォームで ARP キャッシュ サイズが動的に拡大される場合であっても、Unified CM サーバ プラットフォームで使用するオペレーティング システムに関係なく、任意の VLAN 内のデバイスを 512 に制限することを強く推奨します。

図 3-2　音声とデータに対応するアクセス レイヤ スイッチと VLAN



音声を配置する場合は、アクセス レイヤで、次の 2 つの VLAN を有効にすることを推奨します。1 つはデータ トラフィックに対応するネイティブ VLAN（図 3-2 の VLAN 10、11、30、31、および 32）で、もう 1 つは音声トラフィックに対応する、Cisco IOS の Voice VLAN または CatOS の Auxiliary VLAN（図 3-2 の VVID 110、111、310、311、および 312）です。

次の理由により、音声とデータの VLAN を分離することを推奨します。

- アドレス スペースの確保と、外部ネットワークからの音声デバイスの保護

  Voice VLAN または Auxiliary VLAN 上で電話機のプライベート アドレッシングを行うと、アドレスの確保が保証され、パブリック ネットワークを介して電話機に直接アクセスできないことが保証されます。PC とサーバは、一般に、パブリックにルーティングされるサブネット アドレスを使用してアドレス指定されます。ただし、音声エンドポイントは、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定されることがあります。

- QoS 信頼性境界の音声デバイスへの拡張

  QoS 信頼性境界を音声デバイスに拡張し、次に、QoS 機能を PC や他のデータ デバイスに拡張できます。

- 悪質なネットワーク攻撃からの保護

  VLAN アクセス コントロール、802.1Q、および 802.1p タギングを使用すると、音声デバイスを悪質な内部および外部ネットワーク攻撃から保護できます。このような攻撃には、ワーム、Denial of Service（DoS; サービス拒否）攻撃、データ デバイスがパケット タギングによってプライオリティ キューにアクセスする攻撃などがあります。

- 管理および設定の容易性

  アクセス レイヤで音声とデータの VLAN を分離すると、管理が容易になり、QoS 設定が簡素化されます。

高品質の音声を提供し、すべての音声機能セットを利用するには、アクセス レイヤで次の機能をサポートする必要があります。

- 電話機が接続されているポート上でレイヤ 2 CoS パケット マーキングを適切に処理するための 802.1Q トランキングおよび 802.1p
- RTP 音声パケット ストリームのプライオリティ キューイングを行う複数の出力キュー
- トラフィックを分類または再分類し、ネットワーク信頼性境界を設定する機能
- インライン パワー機能（インライン パワー機能は必須ではありませんが、アクセス レイヤ スイッチに使用することを強く推奨します）
- レイヤ 3 認識と、QoS アクセス コントロール リストを実装する機能（これらの機能が推奨されるのは、ソフトフォン アプリケーションを実行する PC など、拡張された信頼性境界を利用できない特定の Unified Communications エンドポイントを使用する場合です）

Spanning Tree Protocol（STP）

コンバージェンス時間を最小限に抑え、レイヤ 2 の耐障害性を最大限に高めるには、次の STP 機能を有効にします。

- PortFast

  すべてのアクセス ポート上で PortFast を有効にします。これらのポートに接続されている電話機、PC、またはサーバは、STP 動作に影響する可能性のあるブリッジ プロトコル データ ユニット（BPDU）を転送しません。PortFast により、電話機または PC が、ポートに接続されたときに、STP が収束するのを待たずにただちにトラフィックの送受信を開始できることが保証されます。

- ルート ガードまたは BPDU ガード

  すべてのアクセス ポート上でルート ガードまたは BPDU ガードを有効にすると、スパニング ツリーのルートになる可能性のある不良スイッチの導入を防止できるので、STP の再コンバージェンス イベントが発生したり、ネットワーク トラフィック フローが中断したりすることがなくなります。BPDU ガードによって **errdisable** 状態に設定されたポートについては、手動で再度有効にするか、または設定期間の経過後に errdisable 状態から自動的にポートを再度有効にするようにスイッチを設定する必要があります。

- UplinkFast と BackboneFast

  必要に応じてこれらの機能を有効にすると、レイヤ 2 ネットワークで変更が生じた場合に、STP ができるだけ迅速にコンバージしてハイ アベイラビリティを実現することが保証されます。シスコ製のスタック可能なスイッチを使用する場合は、Cross-Stack UplinkFast（CSUF）を有効にして、スタック内のスイッチに障害が発生したときにフェールオーバーおよびコンバージェンスが迅速に行われるようにします。

- 単方向リンク検出（UDLD）

  この機能を有効にすると、リンク障害や誤作動が発生したときのネットワーク上のコンバージェンスとダウンタイムが低減されるため、ネットワーク サービスの中断が最小限に抑えられることが保証されます。UDLD は、トラフィックが一方向に流れているリンクを検出し、サービスを落とします。この機能により、障害リンクが、スパニング ツリーおよびルーティング プロトコルによってネットワーク トポロジの一部と誤って見なされることが防止されます。

（注） RSTP 802.1w が導入されていれば、PortFast や UplinkFast などの機能は必要ありません。これは、これらのメカニズムはこの標準に組み込まれているためです。RSTP が Catalyst スイッチ上で有効になっていれば、これらのコマンドは必要ありません。

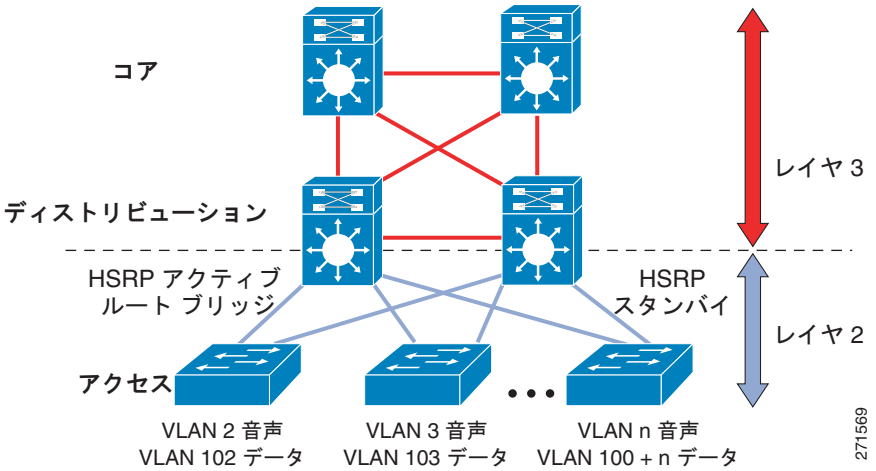
ルーテッド アクセス レイヤ設計

簡素化された設定、一般的なエンドツーエンドのトラブルシューティング ツール、および高速コンバージェンスを必要とするキャンパス設計では、アクセス レイヤ（ルーテッド アクセス）でのレイヤ 3 スイッチングとディストリビューション レイヤでのレイヤ 3 スイッチングを組み合せて使用する階層設計が音声およびデータ トラフィック フローの復旧時間を最小にします。

アクセス レイヤへの L2/L3 境界の移行

一般的な階層キャンパス設計では、ディストリビューション レイヤは、レイヤ 2、レイヤ 3、およびレイヤ 4 プロトコルとサービスの組み合せを使用して、最適なコンバージェンス、スケーラビリティ、セキュリティ、および管理性を提供します。最も一般的なディストリビューション レイヤの設定では、アクセス スイッチは高速トランク ポート上のトラフィックをディストリビューション スイッチに転送するレイヤ 2 スイッチとして設定されます。ディストリビューション スイッチは、図 3-3 に示すように、ダウンストリーム アクセス スイッチ トランク上のレイヤ 2 スイッチングとネットワークのコアに向けてのアップストリーム ポート上のレイヤ 3 スイッチングの両方をサポートするように設定されます。

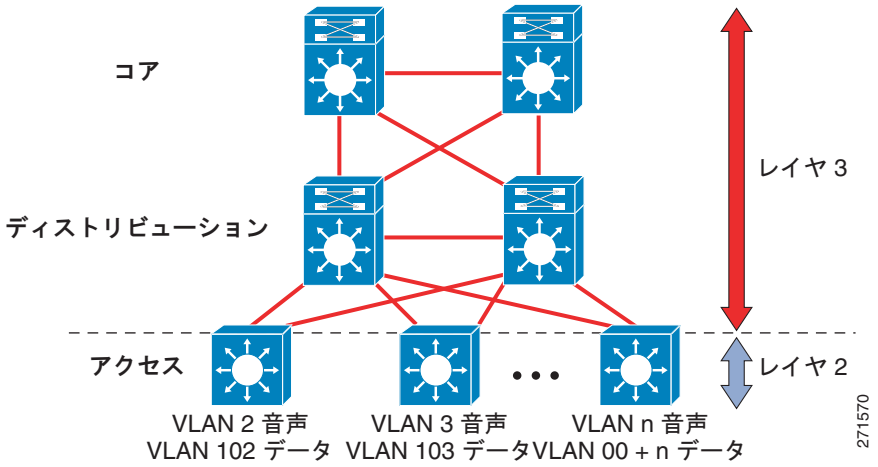
図 3-3　　従来のキャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 2 アクセス



この設計におけるディストリビューション スイッチの目的は、キャンパスのブリッジされたレイヤ 2 部分とルーティングされたレイヤ 3 部分の間に、デフォルト ゲートウェイ、レイヤ 3 ポリシー制御、および必要なすべてのマルチキャスト サービスのサポートを含む境界機能を提供することです。

従来のディストリビューション レイヤ モデル（図 3-3 に示される）に対する代替設定は、アクセス スイッチが完全なレイヤ 3 ルーティング ノード（レイヤ 2 スイッチングとレイヤ 3 スイッチングの両方を提供する）として機能し、ディストリビューションにアクセスするレイヤ 2 アップリンク トランクがレイヤ 3 ポイントツーポイント ルーテッド リンクに置き換えられるものです。レイヤ 2/3 の境界がディストリビューション スイッチからアクセス スイッチに移動する（図 3-4 に示されるように）この代替設定は、大規模な設計の変更のように見えますが、実際には設計上の現在のベスト プラクティスの拡張です。

図 3-4　ルーテッド アクセス キャンパス設計：レイヤ 3 ディストリビューションを使用したレイヤ 3 アクセス



従来のレイヤ 2 とレイヤ 3 ルーテッド アクセス設計の両方で、各アクセス スイッチは固有の音声およびデータ VLAN によって設定されます。レイヤ 3 設計では、これらの VLAN のデフォルト ゲートウェイとルート ブリッジは、ディストリビューション スイッチからアクセス スイッチに単純に移動します。すべての端末とデフォルト ゲートウェイに対するアドレッシングは同様です。VLAN および特定のポート設定は、アクセス スイッチ上で変わりません。各 VLAN のルータ インターフェイス設定、アクセス リスト、「ip helper」、およびその他すべての設定は同様のままですが、ディストリビューション スイッチではなくアクセス スイッチで定義された VLAN Switched Virtual Interface（SVI）上で設定されます。

アクセス スイッチに向かってのレイヤ 3 インターフェイスの移動に関連付けられた、いくつかの重要な設定変更があります。VLAN はすべてローカルになっているので、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）または Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）の仮想ゲートウェイ アドレスを「ルータ」インターフェイスとして設定する必要がなくなりました。同様に、各 VLAN で単一のマルチキャスト ルータを使用する場合、PIM 照会間隔の調整などの従来のマルチキャストの調整を行ったり、代表ルータをアクティブな HSRP ゲートウェイと必ず同期させたりする必要はありません。

ルーテッド アクセス コンバージェンス

レイヤ 3 アクセス設計の使用には、次のような多くの潜在的利点があります。

- コンバージェンスの改善
- マルチキャスト設定の簡素化
- 動的なトラフィック ロード バランシング
- 単一のコントロール プレーン
- 単一セットのトラブルシューティング ツール（ping、traceroute など）

これらの利点のうち、最も重要なものは、おそらく Enhanced Interior Gateway Routing Protocol（EIGRP）または Open Shortest Path First（OSPF）をルーティング プロトコルとして使用して設定されたルーテッド アクセス設計を使用した場合のネットワーク コンバージェンス時間の改善です。最適なレイヤ 2 アクセス設計（スパニング ツリー ループあり、ループなしのいずれか）のコンバージェンス時間とレイヤ 3 アクセス設計のコンバージェンス時間を比較した場合、レイヤ 2 設計の 800 ～ 900 ms からレイヤ 3 アクセス設計の 200 ms 未満まで、4 倍のコンバージェンス時間の改善が得られます。

ルーテッド アクセス設計の詳細については、次の Web サイトにある『*High Availability Campus Network Design – Routed Access Layer using EIGRP or OSPF*』ドキュメントを参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns432/c649/ccmigration_09186a0080811468.pdf

キャンパス ディストリビューション レイヤ

キャンパス LAN のディストリビューション レイヤに含まれるネットワーク部分は、ワイヤリング クローゼット スイッチからネクストホップ スイッチまでです。キャンパス ディストリビューション レイヤ スイッチの詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/switches/index.html

ディストリビューション レイヤでは、冗長性を確保してハイ アベイラビリティを保証することが重要です。たとえば、ディストリビューション レイヤ スイッチ（またはルータ）とアクセス レイヤ スイッチの間に冗長なリンクを確保します。レイヤ 2 にトポロジ上のループが発生しないようにするには、可能であれば、冗長なディストリビューション スイッチ間の接続にレイヤ 3 リンクを使用します。

ファーストホップ冗長プロトコル

ディストリビューション スイッチが L2/L3 境界となるキャンパス階層モデルでは、サポートする L2 ドメイン全体のデフォルト ゲートウェイとしても動作します。この環境は大規模になることがあり、デフォルト ゲートウェイとして動作するデバイスが停止した場合、大きな障害が発生する可能性があるので、いくつかの冗長性の形式が必要になります。

Gateway Load Balancing Protocol（GLBP; ゲートウェイ ロード バランシング プロトコル）、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）、および Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）は、すべてのファーストホップ冗長プロトコルです。シスコは、必要なデフォルト ゲートウェイの冗長性に対応するために、最初に HSRP を開発しました。その後、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）は、Virtual Router Redundancy Protocol（VRRP; 仮想ルータ冗長プロトコル）をデフォルト ゲートウェイの冗長性を備える標準ベースの方法として承認しました。最近になって、シスコは、HSRP および VRRP の両方に固有の制限の一部を解消するために、GLBP を開発しました。

Cisco 機能拡張に対応する HSRP および VRRP は、両方ともデフォルト ゲートウェイをバックアップする堅固な方法を備え、適切に調整された場合、冗長なディストリビューション スイッチに 1 秒未満でフェールオーバーを提供できます。

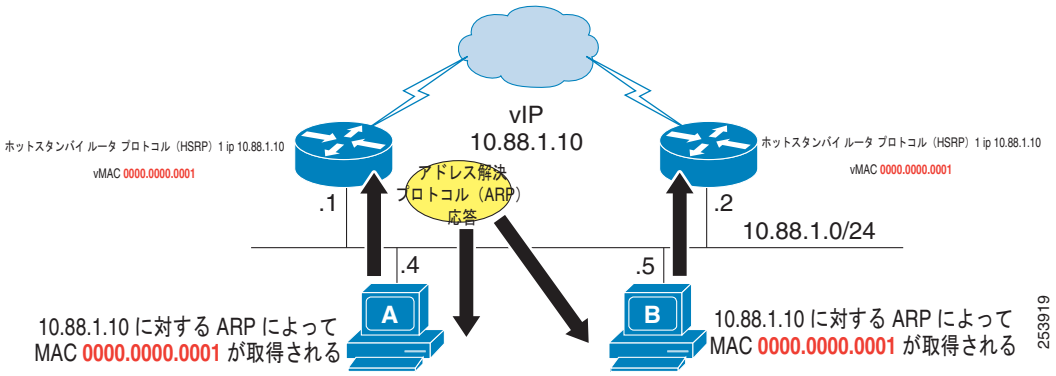
Gateway Load Balancing Protocol（GLBP）

HSRP および VRRP と同様に、シスコの Gateway Load Balancing Protocol（GLBP）は、障害の発生したルータや回線からのデータ トラフィックを保護すると共に、冗長ルータのグループ間のパケット ロード シェアリングを可能にします。デフォルト ゲートウェイの冗長性を提供するために HSRP または VRRP が使用される場合、ピア関係にあるバックアップ メンバーは、処理を引き継ぎ、トラフィックをアクティブに転送するために、発生する障害イベントを待機してアイドル状態となります。

GLBP を開発する以前は、アップリンクをより効率的に利用する方法は実装および管理が困難でした。ある手法では、HSRP および STP/RSTP ルートが、あるピアを目指す偶数の VLAN と別のピアを目指す奇数の VLAN を持つディストリビューション ノード ピア間で交互に使用されました。別の手法では、1 つのインターフェイス上で複数の HSRP グループを使用し、DHCP を使用して複数のデフォルト ゲートウェイ間で交互に使用されました。これらの手法は動作しましたが、設定、保守、または管理の観点から見たときに最適ではありませんでした。

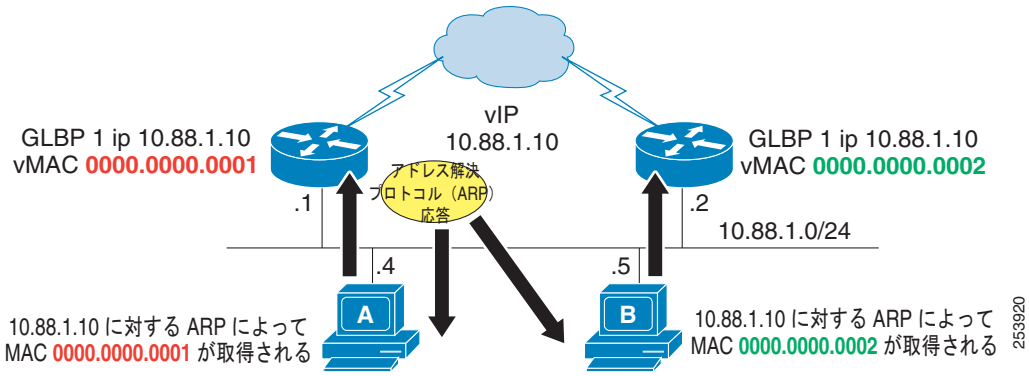
GLBP は HSRP と同じように設定され、機能します。HSRP では、Address Resolution Protocol（ARP; アドレス解決プロトコル）を使用してデフォルト ゲートウェイの物理 MAC アドレスを取得するときに、単一の仮想 MAC アドレスがエンドポイントに指定されます（図 3-5 を参照）。

図 3-5　HSRP では 1 つの仮想 MAC アドレスを使用



2 つの仮想 MAC アドレスが、各 GLBP ピアに 1 つずつ GLBP とともに存在します（図 3-6 を参照）。エンドポイントが ARP を使用してデフォルト ゲートウェイを決定する場合、仮想 MAC アドレスがラウンドロビン方式で照合されます。フェールオーバーとコンバージェンスは、HSRP と同様に動作します。バックアップ ピアは、障害が発生したデバイスの仮想 MAC アドレスを想定して、障害が発生したピアへのトラフィックの転送を開始します。

図 3-6　GLBP では各 GLBP ピアに 1 つずつ、2 つの仮想 MAC アドレスを使用



最終的には、より均等なアップリンクの利用が最小の設定で実現します。副次的な効果として、アップリンクまたはプライマリ ディストリビューション ノードのコンバージェンス イベントがホスト数の半分だけに影響を与え、コンバージェンス イベントの影響を平均 50% 未満にします。

HSRP、VRRP、および GLBP の詳細については、次の Web サイトにある『*Campus Network for High Availability Design Guide*』を参照してください。

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns431/c649/ccmigration_09186a008093b876.pdf

ルーティング プロトコル

高速コンバージェンス、ロード バランシング、および耐障害性を保証するには、ディストリビューション レイヤで、OSPF や EIGRP などのレイヤ 3 ルーティング プロトコルを設定します。コンバージェンス時間を最適化および制御する場合や、複数のパスおよびデバイスにトラフィックを分散させる場合は、ルーティング プロトコル タイマー、パスまたはリンク コスト、およびアドレス サマリーなどのパラメータを使用します。また、**passive-interface** コマンドを使用して、ルーティングに関するネイバー ルータとの隣接関係がアクセス レイヤを介して形成されることを防止することを推奨します。このような隣接関係は、一般には必要ありません。これらの隣接関係があると、余分な CPU オーバーヘッドが作成され、メモリの消費量が増加します。これは、ルーティング プロトコルがこれらの隣接関係をトラッキングするためです。アクセス レイヤ方向のすべてのインターフェイス上で **passive-interface** コマンドを使用すると、ルーティング アップデートがこれらのインターフェイスから送信されることが防止されます。したがって、ネイバー ルータとの隣接関係は形成されません。

キャンパス コア レイヤ

キャンパス LAN のコア レイヤに含まれるネットワーク部分は、ディストリビューション ルータまたはレイヤ 3 スイッチから 1 つまたは複数のハイエンド コア レイヤ 3 スイッチまたはルータまでです。コア レイヤのレイヤ 3 対応 Catalyst スイッチは、多数のキャンパス ディストリビューション レイヤに相互接続性を提供できます。キャンパス コア レイヤ スイッチの詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html で入手可能なマニュアルを参照してください。

コア レイヤにおいても、ハイ アベイラビリティを保証するために、次のタイプの冗長性を確保することが非常に重要です。

- 冗長なリンクまたはケーブル パス

  この冗長性により、ダウンまたは誤作動しているリンクを迂回してトラフィックを再ルーティングできることが保証されます。

- 冗長なデバイス

  この冗長性により、デバイスに障害が発生したときに、その障害デバイスが実行していたタスクをネットワーク内の別のデバイスが引き継げることが保証されます。

- 冗長なデバイス サブシステム

  この冗長性により、デバイス内で複数の電源およびモジュールを使用できることが保証されます。その結果、これらのコンポーネントのいずれかに障害が発生してもデバイスは機能し続けることができます。

Cisco Catalyst 6500 Virtual Switching System（VSS）1440 を使用すると、2 つの Catalyst 6500 スーパーバイザ エンジンを一緒にプールして 1 つのエンジンとして機能させることにより、これらすべての領域で冗長性を確保できます。VSS の詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps9336/index.html

コア レイヤのルーティング プロトコルは、パスの冗長性と高速コンバージェンスにあわせて再度設定および最適化する必要があります。ネットワーク接続はレイヤ 3 でルーティングされる必要があるため、コアに STP を含めないでください。最終的に、コア デバイスとディストリビューション デバイス間の各リンクは、独自の VLAN またはサブネットに属し、30 ビット サブネット マスクを使用して設定される必要があります。

データ センターとサーバ ファーム

一般に、メディア リソース サーバなどの Cisco Unified Communications Manager（Unified CM）クラスタ サーバは、ファイアウォールで保護されたデータ センターまたはサーバ ファーム環境に配置されます。また、カンファレンス ブリッジ、DSP またはトランスコーダ ファーム、メディア ターミネーション ポイントなどの、集中型ゲートウェイと集中型ハードウェア メディア リソースも、データ センターまたはサーバ ファームに配置されることがあります。Cisco Unified Communications Manager（Unified CM）クラスタ サーバおよびメディア リソースに関連したファイアウォールの配置は、ネットワークにおけるセキュリティの設計および実装方法に影響を与える可能性があります。Unified Communications システムに関連したファイアウォール配置の設計ガイドラインについては、「ファイアウォール」（P.4-25）を参照してください。

これらのサーバとリソースは音声ネットワークにおいて重要であるため、すべての Unified CM クラスタ サーバ、集中型音声ゲートウェイ、および集中型ハードウェア リソースは、複数の物理スイッチに分散させ、可能であればキャンパス内の複数の物理ロケーションにも分散させることを推奨します。このようにリソースを分散させると、ハードウェア障害（スイッチやスイッチのライン カードの障害など）が発生しても、少なくともクラスタ内の一部のサーバを使用して、引き続きテレフォニー サービスを提供できることが保証されます。また、一部のゲートウェイとハードウェア リソースを使用して、引き続き公衆網へのアクセスと付加サービスを提供することもできます。物理的に分散させるだけでなく、これらのサーバ、ゲートウェイ、およびハードウェア リソースを別の VLAN またはサブネットに分散させる必要もあります。そのように分散させると、特定の VLAN 上でブロードキャスト ストームまたは DoS 攻撃が発生しても、一部の音声接続およびサービスは中断されずに済みます。

Power over Ethernet（PoE）

PoE（またはインライン パワー）は、標準的なイーサネット Unshielded Twisted-Pair（UTP; シールドなしツイストペア）ケーブルを介して供給される 48 V DC 電源です。IP Phone や、Aironet Wireless Access Points などのインライン Powered Device（PD; 受電装置）は、壁面コンセントを使用する代わりに、インライン パワー対応の Catalyst イーサネット スイッチや他のインライン Power Source Equipment（PSE）によって供給される電力を受けられます。デフォルトでは、インライン パワーは、すべてのインライン パワー対応 Catalyst スイッチ上で有効になっています。

インライン パワー対応のスイッチを Uninterruptible Power Supplies（UPS; 無停電電源装置）と共に配置すると、電源障害の発生中も IP Phone が電力を継続して受けることが保証されます。この電源障害の発生中にテレフォニー ネットワークの残りの部分が使用可能であれば、IP Phone はコールの発信および受信を継続して行うことができます。IP Phone でインライン パワー駆動型イーサネット ポートを使用するには、インライン パワー対応のスイッチをワイヤリング クローゼット内のキャンパス アクセス レイヤに配置する必要があります。この配置により、壁面コンセントが不要になります。

注意　PoE を提供するためにパワー インジェクタまたは電源パッチパネルを使用すると、デバイスによっては損傷することがあります。これは、電力が常にイーサネット ペア線に供給されるためです。PoE スイッチ ポートは、PoE を必要とするデバイスが存在するかどうかを自動的に検出してから、ポートごとに PoE を有効にします。

シスコでは現在、Cisco PoE インライン パワーのほかに、IEEE 802.3af PoE 標準をサポートしています。大部分の Cisco スイッチおよび Cisco Unified IP Phone は、802.3af 標準に準拠しています。802.3af PoE 標準をサポートする Cisco Unified IP Phone については、「エンドポイント機能の要約」（P.18-53）を参照してください。

カテゴリ 3 ケーブリング

カテゴリ 3 ケーブリングを IP コミュニケーションに使用できるのは、次の条件を満たす場合です。

- PC ポートを持ち、そのポートに PC が接続された電話機は、10 Mb 全二重に設定されている必要があります。

  このように設定する場合は、アップストリーム スイッチ ポート、電話機のスイッチ ポートと PC ポート、および PC の NIC ポートを 10 Mb 全二重に固定して設定する必要があります。どのポートも、自動ネゴシエーションには設定しないでください。必要であれば、電話機の PC ポートを 10 Mb 半二重に固定して設定してもかまいません。これにより、PC の NIC が 10 Mb 半二重にネゴシエートするようになります（PC の NIC が自動ネゴシエーションに設定されていることを前提とします）。この設定が受け入れられるのは、電話機とアップストリーム スイッチ ポート間のアップリンクが 10 Mb 全二重に設定されている場合です。

- PC ポートを持たずに 10 Mb スイッチ ポートを持つ電話機は、10 Mb 半二重に自動ネゴシエートできるようになっている必要があります。

  これらの電話機では 10 Mb イーサネットだけがサポートされ、電話機のポートを手動で設定変更することができないため、アップストリーム スイッチ ポートを、自動ネゴシエーションまたは 10 Mb 半二重に設定する必要があります。どちらの場合も、これらの電話機は 10 Mb 半二重にネゴシエートします。

- PC ポートを持つが、そのポートに PC が接続されていない電話機は、10 Mb 半二重にネゴシエートできるようにしてもかまいません。

  これらの電話機をデフォルトのスイッチ ポート設定である自動ネゴシエーションのままにした場合、アップストリーム スイッチ ポートを 10 Mb 半二重に設定すると、これらの電話機は 10Mb 半二重に戻ります。

（注） Cisco Unified IP Phone 7912 については、PC が接続されているときには、カテゴリ 3 ケーブルと共に使用しないでください。これは、この電話機のスイッチ ポートと PC ポートを 10 Mb 全二重にすることができないためです。

IBM タイプ 1A および 2A ケーブリング

IBM Cabling System（ICS）またはトークン リング シールド付きツイストペア タイプ 1A または 2A ケーブリングを IP コミュニケーションに使用できるのは、次の条件を満たす場合です。

- ケーブル長は 100 メートル以下にする必要があります。
- Universal Data Connector（UDC）から RJ-45 イーサネット標準に変換する場合は、インピーダンス整合していないアダプタを使用する必要があります。

（注） トークン リング ケーブルにあるツイストペアは 2 組だけです。したがって、IP Phone へのインライン パワーはサポートされますが、ミッドスパンの給電（Cisco Inline Power と 802.3af を使用する）はペア線を 3 組以上必要とするためサポートされません。

（注） 1000 BASE-T は 4 つのツイストペアが必要になるため、ギガビット イーサネットは IBM 配線システムではサポートされません。Cisco IP Phone 上の 10/100/1000 BASE-T イーサネット インターフェイスと組み合せて IBM 配線システムが使用される場合、サポートされる速度は 10 Mbps と 100 Mbps だけです。

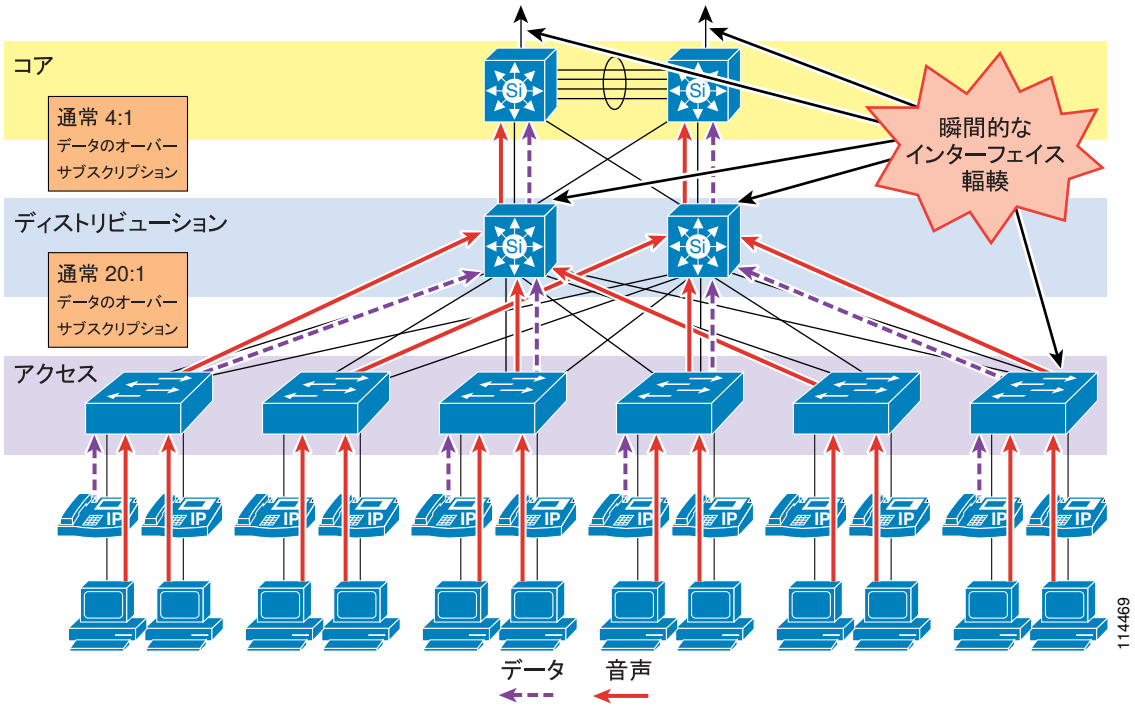
ネットワーク上でデータを伝送しても、ケーブル プラントの品質を十分にテストしたことにならない場合があります。これは、このようなテストでは、準拠に起因しない問題が判明しない場合があるためです。したがって、お客様は、タイプ 1A および 2A ケーブリングの設置がイーサネット標準に準拠していることを確認するために、ケーブル プラントの調査を実施することを推奨します。

LAN の QoS

最近まで、データ トラフィックにはもともと非同期性があること、およびバッファのオーバーフローとパケット損失に耐えるネットワーク デバイスの機能により、企業キャンパスでは、QoS は問題になりませんでした。しかし、音声やデータなどの新しいアプリケーションでは、パケット損失や遅延の影響を受けやすいので、バッファと帯域幅の不足が、企業キャンパスにおける主要な QoS の問題となります。

図 3-7 は、LAN インフラストラクチャで発生する一般的なオーバーサブスクリプションを示しています。

図 3-7　LAN におけるデータ トラフィックのオーバーサブスクリプション



このオーバーサブスクリプションが発生すると、個々のトラフィック量の影響や、複数の独立したトラフィック送信元の累積効果も加わって、出力インターフェイスのバッファが瞬時に満杯になる場合があります。そのため、さらにパケットが出力バッファに入力される場合は、パケットがドロップします。キャンパス スイッチはハードウェアベースのバッファを使用していますが、バッファはインターフェイス速度の点でルータの WAN インターフェイスよりもはるかに遅いため、存続期間の短いトラフィック バーストであっても、バッファのオーバーフローとパケットのドロップが発生する可能性が高くなります。

ファイル共有などのアプリケーション（ピアツーピアとサーバベースの両方）、リモート ネットワーク上のストレージ、ネットワークベースのバックアップ ソフトウェア、およびサイズの大きな添付ファイルを持つ電子メールによって、ネットワークの輻輳がより頻繁に発生したり、より長期間発生したり

する場合があります。最近のワーム攻撃の弊害に、膨大な量のネットワーク トラフィック（ユニキャスト ベースとブロードキャストストーム ベースの両方）があります。この攻撃により、ネットワークの輻輳が増加します。バッファの管理ポリシーが適用されていない場合は、すべてのトラフィックにおいて、LAN の損失、遅延、およびジッタ特性が影響を受けることがあります。

また、冗長なネットワーク要素の障害による影響も考慮する必要があります。この障害により、トポロジ変更が発生します。たとえば、ディストリビューション スイッチに障害が発生した場合は、すべてのトラフィック フローが残りのディストリビューション スイッチを介して再度確立されます。障害の発生前にロード バランシング設計によって 2 つのサイト間で負荷が共有されていても、障害の発生後にすべてのフローが単一のスイッチに集中すると、出力バッファが、通常では発生しない状況に陥る可能性があります。

音声などのアプリケーションの場合、このパケット損失と遅延は、重大な音声品質の低下を招きます。したがって、これらのバッファを管理し、パケットの損失、遅延、および遅延変動（ジッタ）を最小限に抑えるために、QoS ツールが必要です。

ネットワーク全体でトラフィックを管理し、音声品質を保証するには、次のタイプの QoS ツールが必要です。

- トラフィック分類

  分類では、ネットワークの Class of Service（CoS; サービス クラス）に関する要件を示す特定のプライオリティがパケットにマークされます。このパケット マーキングが信頼される地点とされない地点の間は、信頼性境界と見なされます。信頼性は、一般に、音声デバイス（電話機）までは拡張されますが、データ デバイス（PC）には拡張されません。

- キューイングまたはスケジューリング

  インターフェイス キューイングまたはスケジューリングでは、ネットワーク全体で処理を高速化するため、パケットが分類に基づいて複数のキューのいずれかに割り当てられます。

- 帯域幅のプロビジョニング

  プロビジョニングでは、すべてのアプリケーションおよび要素のオーバーヘッドに必要な帯域幅が正確に計算されます。

次の項では、これらの QoS メカニズムをキャンパス環境で使用する方法について説明します。

- 「トラフィック分類」（P.3-16）
- 「インターフェイス キューイング」（P.3-18）
- 「帯域幅のプロビジョニング」（P.3-19）
- 「QoS が使用されない場合の IP コミュニケーションの障害」（P.3-19）

トラフィック分類

可能な限りネットワーク エッジの近くでトラフィックを分類したり、マークすることは、常に Cisco ネットワーク デザイン アーキテクチャの必要不可欠となる部分でした。トラフィック分類は、キャンパス スイッチおよび WAN インターフェイス内で使用される各種キューイング体系にアクセスするための基本的基準です。Cisco IP Phone は、音声制御シグナリングと音声 RTP ストリームを送信元でマークします。その際は、表 3-3 に示されている値に従います。IP Phone は、このようにトラフィック フローを分類可能であり、実際に分類する必要があります。

表 3-3 は、LAN インフラストラクチャのトラフィックを分類する場合の要件をリストしています。

表 3-3　各種タイプのネットワーク トラフィックのトラフィック分類ガイドライン

	レイヤ 3 分類			レイヤ 2 分類
アプリケーション	タイプ オブ サービス（ToS） IP Precedence（IPP）	Per-Hop Behavior（PHB）	Differentiated Services Code Point（DSCP）	サービス クラス（CoS）
ルーティング	6	CS6	48	6
音声 Real-Time Transport Protocol（RTP）	5	EF	46	5
ビデオ会議	4	AF41	34	4
ストリーミング ビデオ	4	CS4	32	4
コール シグナリング[1]	3	CS3（現行） AF31（以前）	24（現行） 26（以前）	3
トランザクション データ	2	AF21	18	2
ネットワーク管理	2	CS2	16	2
Scavenger	1	CS1	8	1
ベストエフォート型	0	0	0	0

1. 呼制御シグナリング トラフィック用の推奨 DSCP/PHB マーキングは、26/AF31 から 24/CS3 に変更されています。シスコではこの変更を反映するようにマーキングを移行しましたが、一部の製品は、引き続きシグナリング トラフィックを 26/AF31 としてマークします。したがって、当面は、コール シグナリング用に AF31 と CS3 の両方を予約することを推奨します。

トラフィック分類の詳細については、次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

http://www.cisco.com/go/designzone

ビデオ テレフォニーのトラフィック分類

IP ビデオ テレフォニーに関係する主なクラスは、次のとおりです。

- 音声

  音声は、CoS 5（IP Precedence 5、PHB EF、または DSCP 46）に分類されます。

- ビデオ会議

  ビデオ会議は、CoS 4（IP Precedence 4、PHB AF41、または DSCP 34）に分類されます。

- コール シグナリング

  音声およびビデオ会議のコール シグナリングは、CoS 3（IP Precedence 3、PHB CS3、または DSCP 24）に分類されるようになりましたが、以前は PHB AF31 または DSCP 26 に分類されていました。

Cisco Unified Communications ネットワークでは、これらの分類をベスト プラクティスとして強く推奨します。

ビデオ コールと音声専用コール間の QoS マーキングの相違点

コールの音声コンポーネントは、進行中のコールのタイプに応じて、2 つのいずれかに分類できます。音声だけの通話呼のメディアは、CoS 5（IP Precedence 5 または PHB EF）に分類されますが、ビデオ会議の音声チャネルのメディアは CoS 4（IP Precedence 4 または PHB AF41）に分類されます。すべ

ての Cisco IP Video Telephony 製品は、Cisco Corporate QoS Baseline 標準に準拠し、ビデオ コールのオーディオ チャネルとビデオ チャネルの両方が CoS 4（IP Precedence 4 または PHB AF41）にマークされている必要があります。この推奨事項には次の理由がありますが、これら以外にもあります。

- オーディオ チャネルとビデオ チャネルのリップシンクを維持する。
- オーディオだけのコールとビデオ コールに個別のクラスを提供する。

シグナリング クラスは、すべての音声シグナリング プロトコル（SCCP、MGCP など）、およびビデオ シグナリング プロトコル（SCCP、H.225、RAS、CAST など）に適用されます。これらのプロトコルについては、「ソフトウェアベースのエンドポイント」（P.18-41）の項で詳しく説明します。

推奨クラスを使用する場合、最初の手順は、パケットを分類する場所（トラフィックの QoS 分類でトラフィックを最初にマークするデバイス）の決定です。トラフィックをマークまたは分類する場所は、基本的には 2 箇所あります。

- 発信元エンドポイント：分類はアップストリーム スイッチおよびルータで信頼されます。
- スイッチまたはルータ：エンドポイントにパケットを分類する機能がない場合、または正しく分類されない場合。

Trusted Relay Point（TRP）を使用した QoS の強制

Trusted Relay Point (TRP) は、エンドポイントからのメディア フローの DSCP 値の強制および再マーキングに使用できます。この機能により、QoS がローカルに変更されている可能性がある、ソフトフォンなどのエンドポイントからのメディアに QoS を強制的に適用できます。この場合、メディアの QoS 値はローカルに変更されている可能性があります。

TRP は、既存の Cisco IOS Media Termination Point（MTP）機能に基づくメディア リソースです。

エンドポイントを「信頼できるリレーポイントを使用（Use Trusted Relay Point)」に設定し、すべてのコールに対して TRP を呼び出すことができます。

QoS の強制では、TRP は Unified CM のサービス パラメータでメディア用に設定された QoS 値を使用して、エンドポイントからのメディア ストリームで QoS 値を再マーキングし、強制的に適用します。

TRP 機能は、Cisco IOS MTP とトランスコーディング リソースによってサポートされます（Unified CM を使用して、MTP またはトランスコーディング リソースで [Enable TRP] チェックボックスをオンにして、TRP 機能をアクティブにします)。

インターフェイス キューイング

レイヤ 2（CoS）とレイヤ 3（DSCP または PHB）でパケットを適切なタグでマークしたら、この分類に基づいてトラフィックのスケジューリングまたはキューイングを行うようにネットワークを設定することが重要です。この設定により、各クラスのトラフィックに対して、必要なサービスがネットワークから提供されます。キャンパス スイッチ上で QoS を使用可能にすることにより、すべての音声トラフィックを個別のキューを使用するように設定できます。この設定により、インターフェイス バッファが即時に満杯になるときでも、音声パケットがドロップする可能性を事実上なくすことができます。

ネットワーク管理ツールが、キャンパス ネットワークが輻輳していないことを示す場合がありますが、それでも音声品質を保証するためには、QoS ツールが必要です。ネットワーク管理ツールは、サンプルの期間全体の平均的な輻輳しか示しません。この平均値は便利ですが、キャンパス インターフェイス上の輻輳のピークを示しません。

キャンパス内の送信インターフェイス バッファは、ネットワーク トラフィック自体にバースト性があるため、短い時間間隔で散発的に輻輳する傾向があります。輻輳が起きると、その送信インターフェイスを宛先とするすべてのパケットがドロップされます。音声トラフィックのドロップを防止する唯一の方法は、キャンパス スイッチ上で複数のキューを設定することです。このため、ポートごとに 2 つ以上の出力キューを持ち、レイヤ 2、レイヤ 3、またはその両方の QoS 分類に基づいてこれらのキュー

にパケットを送信する機能を持つスイッチを常に使用することを推奨します。大部分の Cisco Catalyst スイッチは、ポートごとに 2 つ以上の出力キューをサポートしています。Cisco Catalyst スイッチのインターフェイス キューイング機能の詳細については、http://www.cisco.com/en/US/products/hw/switches/index.html にあるマニュアルを参照してください。

帯域幅のプロビジョニング

キャンパス LAN では、帯域幅プロビジョニングの推奨事項は、「*プロビジョニングは多めに、サブスクリプションは少なめに*」という標語に集約できます。この標語は、使用可能な帯域幅は常に負荷よりも相当量広くし、LAN リンク上に定常的な輻輳がないように、LAN インフラストラクチャを慎重に設計するという意味です。

統合されたネットワークに流れ込む音声トラフィックが増加することは、ネットワーク トラフィックの負荷全体が大幅に増加することを意味するわけではありません。したがって、帯域幅のプロビジョニングを行う場合は、常に、データ トラフィック要件の要求に従います。この設計目標は、テレフォニー シグナリングまたはメディア フローによって通過するデータ トラフィックの大規模な輻輳がすべてのリンク上で発生しないようにすることにあります。単一の G.711 音声コールの帯域幅要件（約 86 Kbps）とファストイーサネット リンクそのものの帯域幅（100 Mbps）を比較してわかるのは、音声は LAN 内でネットワークの輻輳を引き起こすトラフィックのソースではなく、むしろ LAN ネットワークの輻輳から保護されるトラフィック フローであるということです。

QoS が使用されない場合の IP コミュニケーションの障害

QoS が配置されていないと、パケット ドロップや大幅な遅延およびジッタが発生して、テレフォニー サービスの障害を引き起こすことがあります。メディア パケットにドロップ、遅延、およびジッタが発生すると、クリック音が聞こえる、音声が異常になる、無音状態が長期間続く、およびエコーが聞こえるなど、ユーザが知覚できる影響が現れます。

シグナリング パケットが同様の状況になった場合は、ユーザ入力に対する反応が遅い（ダイヤル トーンの遅延など）、応答しても呼出音が続く、および最初のダイヤルが無効になった（したがって電話を切ってリダイヤルする必要がある）とユーザが思い込んで二重に番号をダイヤルすることなど、ユーザが知覚できる障害が発生します。さらに極端なケースとしては、エンドポイントが再初期化される、コールが終了する、および拠点で SRST 機能が誤動作する（ゲートウェイ コールの中断を引き起こす）ことなどが挙げられます。

これらの影響は、すべての配置モデルに現れます。ただし、単一サイト（キャンパス）配置では、リンクの中断が続くことによってこのような状況が発生する可能性は低くなります。これは、一般に LAN 環境にはより大きな帯域幅が配置される（最小リンクは 100 Mbps）ので、残りの帯域幅の一部を IP コミュニケーション システムに使用できるためです。

WAN ベースの配置モデルでは、トラフィックの輻輳によって、リンクの中断が続いたり、より高い頻度で発生したりする可能性が高くなります。これは、使用可能な帯域幅が LAN よりもはるかに小さい（一般に 2 Mbps 未満）ためです。そのため、リンクがより簡単に飽和します。リンクの中断は、エンドポイントと Unified CM サーバ間のシグナリング トラフィックも遅延またはドロップする可能性があるので、音声メディアがパケット ネットワークを通過するかどうかに関係なく、ユーザに大きな影響を与える場合があります。

Cisco UCS B シリーズ ブレード サーバを使用した仮想 Unified Communications に関する QoS 設計上の考慮事項

仮想化された Unified Communications ソリューションでは、Cisco Unified Communications 製品を、サポート対象のハイパーバイザ、サーバ、およびストレージ製品の選択セット上で仮想マシンとして実行できます。仮想 Unified Communications ソリューションの最も重要なコンポーネントは、Cisco Unified Computing System（UCS）プラットフォームとハイパーバイザ仮想化テクノロジーです。仮想化された Unified Communications の設計には、QoS に関して、次のような特別な考慮事項があります。Cisco Unified Computing System（UCS）アーキテクチャ、アプリケーション仮想化のハイパーバイザ テクノロジー、および Storage Area Networking（SAN; ストレージ エリア ネットワーキング）の概念の詳細については、「仮想サーバでの Unified Communications の配置」（P.5-59）を参照してください。

仮想化された環境では、Cisco Unified Communications Manager（Unified CM）のような Unified Communications アプリケーションが、仮想マシンとして VMware 上で実行されます。これらの Unified Communications 仮想マシンは、Media Convergence Server（MCS）配置のハードウェアベースのイーサネット スイッチではなく、仮想ソフトウェア スイッチに接続されます。次のタイプの仮想ソフトウェア スイッチを使用できます。

- ローカルの VMware vSwitch

  VMware ESXi ハイパーバイザのすべてのエディションで使用可能であり、VMware ライセンス方式の種類に依存しません。仮想ソフトウェア スイッチングは、仮想マシンが実行しているローカルの物理ブレード サーバに限定されます。

- 分散型の VMware vSwitch

  VMware ESXi ハイパーバイザの Enterprise Plus Edition に限り使用可能です。分散仮想ソフトウェア スイッチングは、複数の物理ブレードにまたがることができ、ソフトウェア スイッチの管理を簡素化します。

- Cisco Nexus 1000V スイッチ

  シスコには、Nexus 1000 仮想（1000V）スイッチと呼ばれるソフトウェア スイッチがあります。Cisco Nexus 1000V には、VMware ESXi の Enterprise Plus Edition が必要です。これは、複数の VMware ホストおよび仮想マシンで認識可能な分散仮想スイッチです。Cisco Nexus 1000V シリーズは、ポリシーベースの仮想マシン接続、モバイルの仮想マシン セキュリティ、拡張 QoS、およびネットワーク ポリシーを提供します。

仮想接続の観点から見ると、各仮想マシンは、ブレード サーバに配置されている上記の仮想スイッチのいずれかに接続できます。ブレード サーバは、UCS シャーシ内のファブリック エクステンダから UCS ファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズなど）を経由して、ネットワークの残りの部分に物理的に接続します。UCS ファブリック インターコネクト スイッチは、お客様の 1 Gb または 10 Gb イーサネット LAN および FC SAN と物理的配線が接続される場所です。

トラフィック フローの観点から見ると、仮想マシンからのトラフィックは、最初にソフトウェア仮想スイッチ（VMware vSwitch、VMware の分散 vSwitch、または Cisco Nexus 1000V スイッチなど）に転送されます。続いて、仮想スイッチは、ブレード サーバのネットワーク アダプタおよびファブリック エクステンダを介して、トラフィックを物理的な UCS ファブリック インターコネクト スイッチ（UCS 6100 シリーズ）に送信します。UCS ファブリック インターコネクト スイッチは、IP およびファイバ チャネル SAN トラフィックの両方を単線の Fiber Channel over Ethernet（FCoE）を介して伝送します。UCS ファブリック インターコネクト スイッチは IP トラフィックを IP スイッチ（Cisco Catalyst または Nexus シリーズ スイッチ）に送信し、IP スイッチは SAN トラフィックをファイバ チャネル SAN スイッチ（Cisco MDS シリーズ スイッチなど）に送信します。

標準的なスイッチング要素の QoS 動作

デフォルトでは、UCS 6100 シリーズのファブリック インターコネクト スイッチ内で、SAN スイッチに送信されるすべての Fiber Channel（FC; ファイバ チャネル）に対して優先度の QoS クラスが自動的に作成されます。この FC QoS クラスにドロップ ポリシーはなく、すべての FC トラフィックに 3 のレイヤ 2 CoS 値が付けられます。デフォルトでは、音声シグナリングおよびメディア トラフィックを含む他のすべてのトラフィック（イーサネットおよび IP）が、Best Effort QoS クラスに分類されます。

VMware のローカル vSwitch、VMware の分散 vSwitch、および UCS 6100 シリーズ スイッチでは、L3 DSCP 値を L2 CoS 値にマッピングできません。トラフィックは、L2 CoS だけに基づいて、UCS 6100 スイッチ内で優先順位を付けたり解除したりできます。

（注）　Unified Communications アプリケーションは、L3 DSCP 値だけを付けます（音声シグナリングに対する CS3 など）。ただし、ブレード サーバのネットワーク アダプタから発信されたすべてのトラフィックに、単一の L2 CoS 値を付けることができます。

Nexus 1000V ソフトウェア スイッチには、Catalyst シリーズ スイッチなどの従来のシスコ製物理スイッチのように、L3 DSCP 値を L2 CoS 値に、およびその逆にマッピングする機能があります。そのため、Unified Communications トラフィックが仮想マシンを離れて Nexus 1000V スイッチに到達したときに、その L3 DSCP 値を対応する L2 CoS 値にマッピングできます。続いて、UCS 6100 スイッチ内で、L2 CoS 値に基づいてこのトラフィックに優先順位を付けたり解除したりできます。

たとえば、CS3 の値が L3 DSCP の音声シグナリング トラフィックは、Nexus 1000V によって 3 の L2 CoS 値にマップされます。すべての Fibre Channel over Ethernet（FCoE）トラフィックは、Cisco UCS によって 3 の L2 CoS 値にマークされます。音声シグナリング トラフィックと FCoE トラフィックが Cisco UCS 6100 ファブリック インターコネクト スイッチに入力された場合は、どちらも 3 の CoS 値を伝送します。この状況では、音声シグナリング トラフィックが、ファイバ チャネル プライオリティ クラスを使用してキューとスケジューリングを共有することによって、無損失動作が実現します（UCS 6100 ファブリック インターコネクト スイッチ内の CoS 3 のファイバ チャネル プライオリティ クラスは、そのクラスが他のタイプのトラフィックと共有できないことを意味しているわけではありません）。

一方、FCoE トラフィックの L2 CoS 値はデフォルト値の 3 から別の値に変更することができ、CoS 3 は音声シグナリング トラフィック専用として保存できます。ただし、FCoE CoS の値が 3 に設定されなかった場合に一部の Converged Network Adapter（CNA; 統合型ネットワーク アダプタ）で問題が発生するため、このアプローチは推奨できません。

輻輳シナリオ

物理的なサーバ設計では、ハード ドライブは MCS サーバにローカルに接続され、SCSI トラフィックがイーサネット IP トラフィックと競合することはありません。

UCS B シリーズ システムを使用する仮想 Unified Communications の設計は、従来の MCS ベースの設計とは異なります。仮想 Unified Communications の設計では、ハード ドライブがリモートで、FC SAN を介してアクセスされるため、FC SAN トラフィックが帯域幅を得るために UCS 6100 シリーズ スイッチ内でイーサネット IP トラフィックと競合する可能性があります。UCS 6100 スイッチ内に FC トラフィックのドロップ ポリシーがないため、この結果として、音声関連の IP トラフィック（シグナリングおよびメディア）がドロップされる可能性があります。ただし、UCS 6100 スイッチでは高キャパシティのスイッチング ファブリックが提供されており、さらにサーバ ブレードごとの使用可能な帯域幅が一般的な Unified Communications アプリケーションの最大トラフィック要件を大幅に上回っているため、この輻輳またはオーバーサブスクリプションのシナリオが発生する可能性は非常に低くなります。

設計に関する推奨事項

Nexus 1000V は、仮想化されたデータ センターには不可欠で他の仮想スイッチ実装では使用できない拡張 QoS およびその他の機能（ACL、DHCP スヌーピング、IP ソース ガード、SPAN など）を提供します。Cisco Unified Communications アプリケーションを UCS B シリーズ システムで稼動している他の多くの仮想マシンとともに配置するような大規模データ センターの実装では、L3 DSCP 値を L2 CoS 値にマッピングする機能を有効にして、Nexus 1000V スイッチを使用することを推奨します。その他の Unified Communications 配置の場合、Nexus 1000V を使用するかどうかの決定は、UCS アーキテクチャ内で Unified Communications アプリケーションが使用できる帯域幅に応じて、ケースバイケースで変わります。輻輳シナリオが発生する可能性がある場合は、Nexus 1000V スイッチを配置する必要があります。

すべての仮想スイッチに配置できる代替ソリューションは、すべてのトラフィックに **Platinum**（CoS=5、ドロップ ポリシーなし）の QoS ポリシーを設定するように、Unified Communications サーバ ブレード上のすべての物理ネットワーク アダプタを設定することです。同じ UCS システムまたはシャーシで稼動している他のアプリケーションはすべて、QoS ポリシーを**ベストエフォート**に設定する必要があります。このアプローチのデメリットは、すべての非音声トラフィック（バックアップ、CDR、ログ、Web トラフィックなど）を含む仮想 Unified Communications アプリケーションのすべてのトラフィック タイプで、CoS 値が Platinum に設定されることです。このソリューションは最適ではありませんが、Unified Communications アプリケーションのトラフィックの優先順位を、FC SAN 行きのトラフィックの優先順位まで上げ、これによってトラフィック ドロップの可能性を減らします。

ネットワーク サービス

IP Communications システムの配置には、構造化されて可用性と回復力が高いネットワーク インフラストラクチャの調和の取れた設計、および Domain Name System（DNS; ドメイン ネーム システム）、DHCP（Dynamic Host Configuration Protocol）、TFTP（Trivial File Transfer Protocol）、Network Time Protocol（NTP; ネットワーク タイム プロトコル）を含むネットワーク サービスの統合セットが必要です。

ドメイン ネーム システム（DNS）

DNS を使用すると、ホスト名およびネットワーク サービスをネットワーク（複数可）内の IP アドレスにマッピングできます。ネットワーク内に配置された DNS サーバは、ネットワーク サービスをホスト名にマッピングし、次にホスト名を IP アドレスにマッピングするデータベースを備えています。ネットワーク上のデバイスは、DNS サーバに照会して、ネットワークにある他のデバイスの IP アドレスを受信できます。そのため、ネットワーク デバイス間の通信が容易になります。

DNS などの 1 つのネットワークサービスに完全に依存することは、重要な Unified Communications システムを配置するときに、リスク要素になることがあります。DNS サーバが使用不能になった場合、ネットワーク デバイスがそのサーバを利用してホスト名から IP アドレスへのマッピングを取得しているときは、通信に障害が発生することがあります。このため、ハイ アベイラビリティが要求されるネットワークでは、Unified CM と Unified Communications エンドポイント間の通信は、DNS 名前解決に依存しないことを推奨します。

標準配置では、Unified CM、ゲートウェイ、およびエンドポイント デバイスを設定して、ホスト名ではなく IP アドレスを使用することを推奨します。エンドポイント デバイス設定では、DNS サーバのアドレス、ホスト名、およびドメイン名などの DNS パラメータを設定することは推奨できません。初めて Unified CM クラスタにパブリッシャ ノードをインストールするとき、パブリッシャは、システムに提供したホスト名によってサーバ テーブルで参照されます。その後のサブスクライバのインストールおよび設定、またはエンドポイントの定義の前に、このサーバ エントリをパブリッシャのホスト名ではなく IP アドレスに変更する必要があります。クラスタに追加する各サブスクライバは、ホスト名で

はなく IP アドレスで、同じサーバ テーブルに定義する必要があります。各サブスクライバは、1 デバイスずつこのサーバ テーブルに追加する必要があります。新しいサブスクライバをインストールするときに定義する場合を除き、存在しないサブスクライバは定義しないでください。

パブリッシャおよびサブスクライバをインストールするときは、システム管理の目的で特に DNS が必要な場合を除き、DNS を有効にするオプションを選択しないことを推奨します。DNS を有効にする場合も、IP Communications エンドポイント、ゲートウェイ、および Unified CM サーバの設定では、DNS 名を使用しないことを強く推奨します。クラスタのサーバで DNS を有効にした場合でも、そのクラスタ外のデバイスとの通信にだけ使用して、クラスタ内サーバ間通信には使用しないでください。

Cisco Unified CM 5.0 以降のリリースでは、HOSTS ファイルまたは LHOSTS ファイルを手動で設定できません。HOSTS テーブルのローカル バージョンが各クラスタのパブリッシャによって自動的に構築され、セキュア通信チャネルを介してすべてのサブスクライバ ノードに配布されます。セキュアなクラスタ内通信には、このローカル テーブルが使用されます。テーブルには、Unified CM サーバ以外のエンドポイントのアドレスまたは名前は含まれていません。LMHOSTS ファイルは存在せず、Cisco Unified CM 5.0 以降のリリースでは使用されません。

DNS を使用した Unified CM の配置

場合によっては、DNS を設定および使用することが避けられないことがあります。たとえば、IP Communications ネットワーク内での IP Phone と Unified CM 間の通信に Network Address Translation（NAT; ネットワーク アドレス変換）が必要な場合、NAT 変換後のアドレスがネットワーク ホスト デバイスに正しくマッピングされることを保証するには、DNS が必要です。同様に、ホスト名をセカンダリ バックアップ サイトの IP アドレスにマッピングすることで、障害発生時にネットワークのフェールオーバーが正常に行われることを保証するには、一部の IP テレフォニー ディザスタ リカバリ ネットワーク設定で DNS を利用する必要があります。

このどちらかの状況で DNS の設定が必要になった場合は、DNS サーバを地理的に冗長な方式で配置する必要があります。この配置により、一方の DNS サーバに障害が発生しても、IP テレフォニー デバイス間のネットワーク通信が妨げられることはありません。DNS サーバを冗長にすると、一方の DNS サーバで障害が発生しても、引き続き、DNS を利用してネットワーク上で通信するデバイスが、バックアップまたはセカンダリ DNS サーバから、ホスト名から IP アドレスへのマッピングを受信できることが保証されます。

（注）　ローカルの HOSTS ファイルまたは DNS 照会によるクラスタ内のホスト名解決が実行されるのは、サブシステムの初期化時（サーバのブートアップ時）だけです。結果として、クラスタ内のサーバが、HOSTS ファイルまたは DNS サーバ上で変更された DNS 名を解決できるようにするには、クラスタ内のすべてのサーバ上で Cisco CallManager サービスを再起動する必要があります。

Unified CM は DNS を使用して次を実行できます。

- 簡素化されたシステム管理を提供する
- 完全修飾ドメイン名（FQDN）をトランク宛先の IP アドレスに解決する
- 完全修飾ドメイン名をドメイン名に基づく SIP ルート パターンの IP アドレスに解決する
- サービス（SRV）レコードをホスト名に解決し、SIP トランク宛先の IP アドレスに解決する

DNS を使用する場合、各 Unified CM クラスタを、より大きな組織の DNS ドメインの有効なサブドメインのメンバーとして定義し、各 Cisco MCS サーバ上に DNS ドメインを定義し、各 MCS サーバ上にプライマリおよびセカンダリの DNS サーバのアドレスを定義することを推奨します。

表 3-4 に、DNS サーバが Unified CM 環境で A レコード（ホスト名から IP アドレスへの解決）、Cname レコード（エイリアス）、および SRV レコード（冗長性とロード バランシング用のサービス レコード）を使用できる例を示します。

表 3-4　Unified CM における DNS の使用例

ホスト名	タイプ	TTL	データ
CUCM-Admin.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.1
CUCM1.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.1
CUCM2.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.2
CUCM3.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.3
CUCM4.cluster1.cisco.com	ホスト（A）	デフォルト	182.10.10.4
TFTP-server1.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.11
TFTP-server2.cluster1.cisco.com	ホスト（A）	12 時間	182.10.10.12
www.CUCM-Admin.cisco.com	エイリアス（CNAME）	デフォルト	CUCM-Admin.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM1.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM2.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM3.cluster1.cisco.com
_sip._tcp.cluster1.cisco.com	サービス（SRV）	デフォルト	CUCM4.cluster1.cisco.com

Dynamic Host Configuration Protocol（DHCP）

DHCP は、ネットワーク上のホストが、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、および TFTP サーバ アドレスなどの初期設定情報を取得するために使用します。DHCP により、各ホストに IP アドレスやその他の設定情報を手動で設定する管理負担が軽減されます。また、DHCP により、デバイスをサブネット間で移動したときに、ネットワーク設定が自動的に再設定されます。設定情報はネットワーク内にある DHCP サーバから提供されます。このとき、DHCP サーバは、DHCP 対応のクライアントから送信される DHCP 要求に応答します。

これらのデバイスの配置を簡素化するには、DHCP を使用するように IP Communications エンドポイントを設定する必要があります。任意の RFC 2131 準拠 DHCP サーバを使用して、IP Communications ネットワーク デバイスに設定情報を提供できます。既存のデータ専用ネットワークに IP テレフォニー デバイスを配置する場合、作業としては、この新しい音声デバイスに対応する DHCP 音声スコープを既存の DHCP サーバに追加するだけで済みます。IP テレフォニー デバイスは、DHCP サーバを利用して IP 設定情報を取得するように設定されているため、DHCP サーバは冗長な方式で配置する必要があります。テレフォニー ネットワークには、2 つ以上の DHCP サーバを配置する必要があります。この配置により、いずれかのサーバに障害が発生しても、他のサーバが引き続き DHCP クライアント要求に応答できます。また、DHCP サーバに、ネットワーク内の DHCP に依存するクライアントすべてを処理するのに十分な IP サブネット アドレスが設定されていることを確認する必要があります。

DHCP オプション 150

IP テレフォニー エンドポイントでは、DHCP オプション 150 を利用することで、TFTP を実行するサーバから入手可能なテレフォニー設定情報の送信元を特定するように設定できます。

単一の TFTP サーバがすべての配置済みエンドポイントにサービスを提供するという最も単純な設定では、オプション 150 は、システムの指定 TFTP サーバを指す単一の IP アドレスとして配布されます。2 つの TFTP サーバが同じクラスタ内にある配置の場合、DHCP スコープは、オプション 150 で 2 つの IP アドレスを配布することもできます。プライマリ TFTP サーバにアクセスできなくなった場合、電話機は 2 つめのアドレスを使用します。その結果、冗長性が確保されます。TFTP サーバ間で冗長性とロード シェアリングの両方を実現するには、DHCP スコープの半分において 2 つの TFTP サーバ アドレスが逆の順序になるように、オプション 150 を設定します。

（注）　プライマリ TFTP サーバが使用可能でも、要求されたファイルを電話機に付与できない場合（たとえば、要求元の電話機がそのクラスタ上に設定されていない場合）、その電話機はセカンダリ TFTP サーバへのアクセスを試みません。

オプション 150 には直接 IP アドレスを使用する（つまり、DNS サービスを利用しない）ことを強く推奨します。これは、このように設定することで、電話機のブートアップおよび登録プロセス中に DNS サービスの可用性に依存しなくなるためです。

（注）　IP Phone はオプション 150 で最大 2 つの TFTP サーバをサポートしますが、Unified CM クラスタには 3 つ以上の TFTP サーバを設定できます。たとえば、Unified CM システムが 3 つの別々のサイトで WAN を介してクラスタリングされている場合は、3 つの TFTP サーバを（サイトごとに 1 つ）配置できます。次に、オプション 150 内にそのサイトの TFTP サーバを含む DHCP スコープを、各サイト内の電話機に付与できます。このように設定すると、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離される（1 つのサイトの障害が別のサイトの TFTP サービスに影響しない）ことが保証されます。

電源復帰後の電話機による DHCP オペレーション

電話機の電源が切断され、DHCP サーバがオフラインになっている間に復旧した場合、電話機は DHCP を使用して IP アドレス指定情報を取得しようとします（通常動作）。DHCP サーバからの応答がない場合、電話機は以前に受信した DHCP 情報を再利用して Unified CM に登録します。

DHCP のリース期間

DHCP のリース期間は、ネットワーク環境に応じて設定します。PC とテレフォニー デバイスが長期間にわたって同じ場所にある、ほとんど変化のないネットワークでは、DHCP のリース期間を長くする（たとえば、1 週間にする）ことを推奨します。リース期間を短くすると、DHCP 設定の更新頻度が高くなるため、ネットワーク上の DHCP トラフィック量が増加します。逆に、ラップトップやワイヤレス テレフォニー デバイスなどのモバイル デバイスを多数含むネットワークでは、DHCP のリース期間を短くして（たとえば、1 日間にして）、DHCP で管理するサブネット アドレスが枯渇することを防止する必要があります。モバイル デバイスは、一般に、IP アドレスを短期間使用し、その後は DHCP の更新や新しいアドレスを長期間要求しない場合があります。リース期間を長くすると、この IP アドレスは一定期間拘束されるため、使用されなくなった場合でも再割り当てされなくなります。

Cisco Unified IP Phone は、DHCP サーバのスコープ設定で指定された、DHCP のリース期間の条件に従います。DHCP サーバが最後に正常に応答してからリース期間の半分が経過すると、IP Phone はリースの更新を要求します。この DHCP クライアント要求が DHCP サーバによって応答されると、IP Phone は、次のリース期間にわたって IP スコープ（つまり、IP アドレス、デフォルト ゲートウェイ、サブネット マスク、DNS サーバ（オプション）、および TFTP サーバ（オプション））を継続使用できるようになります。DHCP サーバが使用不能になると、IP Phone はその DHCP リースを更新できません。さらに、リースが期限切れになるとすぐに、IP Phone はその IP 設定を開放するため、Unified CM から登録解除（アンレジスタ）されます。この状態は、DHCP サーバが別の有効なスコープを付与するまで継続されます。

集中型コール処理配置では、リモート サイトが中央の DHCP サーバを使用するように設定されている場合（Cisco IOS の IP ヘルパー アドレスなどの DHCP リレー エージェントを利用して）、および中央サイトへの接続が切断された場合、支店内の IP Phone はその DHCP スコープのリースを更新できなくなります。この場合、支店の IP Phone では、その DHCP のリースが期限切れになる危険性があります。その結果、その IP アドレスが使用できなくなり、サービスが中断されます。電話機はリース期間の半分が経過した時点でそのリースの更新を試みるという事実を考えると、DHCP サーバが到達不能になってからリース期間の半分が経過するとすぐに、DHCP のリースが期限切れになる可能性があり

ます。たとえば、DHCP スコープが 4 日間に設定されている場合、WAN の障害によって支店内の電話機が DHCP サーバを使用できなくなったときは、その電話機はリース期間の半分（この場合は 2 日間）が経過した時点でリースを更新できなくなります。IP Phone は、WAN に障害が発生してから最短で 2 日後に機能を停止する可能性があります。ただし、その時点までに WAN が復旧して、DHCP サーバが使用可能になった場合は除きます。WAN の接続障害が続くと、WAN に障害が発生してから遅くとも 4 日後には、すべての電話機の DHCP スコープが期限切れになります。

次のいずれかの方法によって、この状況を緩和できます。

- DHCP スコープのリース期間を長くする（たとえば、8 日間以上にします）

  この方法を使用すると、システム管理者は、少なくともリース期間の半分の時間を費やして、DHCP の到達不能に関するすべての問題に対処できます。また、リース期間が長ければ、リースの更新に関連するネットワーク トラフィックの頻度が減少します。

- 共存 DHCP サーバの機能を設定する（たとえば、支店の Cisco IOS ルータ上で DHCP サーバ機能を実行します）

  このアプローチは、WAN 接続の中断の影響を受けません。このアプローチを使用すると、IP アドレスの管理が分散されるため、各拠点で設定を更新する作業が発生します（詳細については、「DHCP のネットワーク配置」（P.3-26）を参照してください）。

（注）　「*共存*」という用語は、同じ物理的な場所にある複数のデバイスを指します。これらのデバイスの間に WAN または MAN 接続はありません。

DHCP のネットワーク配置

IP テレフォニー ネットワーク内に DHCP 機能を配置するためのオプションには、次の 2 つがあります。

- 中央の DHCP サーバ

  一般に、単一サイトのキャンパス IP テレフォニー配置の場合は、DHCP サーバをキャンパス内の中央ロケーションに設置する必要があります。前にも説明したように、冗長な DHCP サーバを配置する必要があります。集中型マルチサイト Unified CM 配置の場合と同様に、IP テレフォニー配置にもリモートの拠点テレフォニー サイトを含める場合は、中央サーバを使用して、リモート サイト内のデバイスに DHCP サービスを提供できます。このタイプの配置では、支店ルータのインターフェイス上で **ip helper-address** を設定する必要があります。冗長な DHCP サーバを中央サイトに配置する場合は、両方のサーバの IP アドレスを **ip helper-address** として設定する必要があることに留意してください。また、支店側のテレフォニー デバイスが中央の DHCP サーバを利用する場合、2 つのサイト間で WAN リンクに障害が発生すると、支店サイトのデバイスは、DHCP 要求を送信することも、DHCP 応答を受信することもできなくなります。

（注）　デフォルトでは、**service dhcp** は Cisco IOS デバイス上で有効になっていますが、設定には表示されません。このサービスを支店ルータ上で無効にしないでください。無効にすると、デバイス上で DHCP リレー エージェントが無効になり、**ip helper-address** コンフィギュレーション コマンドが動作しなくなります。

- 中央の DHCP サーバとリモート サイトの Cisco IOS DHCP サーバ

  集中型マルチサイト Unified CM 配置で使用する DHCP を設定する場合は、中央の DHCP サーバを使用して、中央にあるデバイスに DHCP サービスを提供できます。リモート デバイスは、ローカルに設置されたサーバから、またはリモート サイトにある Cisco IOS ルータから、DHCP サー

ビスを受信できます。このタイプの配置では、WAN に障害が発生しても、リモートのテレフォニー デバイスから DHCP サービスを使用できることが保証されます。例 3-1 は、Cisco IOS DHCP サーバの基本的なコンフィギュレーション コマンドを示しています。

例 3-1　Cisco IOS DHCP サーバのコンフィギュレーション コマンド

```
! Activate DHCP Service on the IOS Device

service dhcp

! Specify any IP Address or IP Address Range to be excluded from the DHCP pool

ip dhcp excluded-address <ip-address>|<ip-address-low> <ip-address-high>

! Specify the name of this specific DHCP pool, the subnet and mask for this
! pool, the default gateway and up to four TFTP

ip dhcp pool <dhcp-pool name>
   network <ip-subnet> <mask>
   default-router <default-gateway-ip>
   option 150 ip <tftp-server-ip-1> ...

! Note: IP phones use only the first two addresses supplied in the option 150
! field even if more than two are configured.
```

Unified CM DHCP サーバ（スタンドアロン サーバと共存サーバの比較）

ほとんどのネットワーク インフラストラクチャで、通常、DHCP サーバは専用のマシンで、そのネットワークで使用する DNS サービスと Windows Internet Naming Service（WINS）サービスを組み合せて実行します。場合によっては、クラスタに登録されているデバイスが 1000 以下の小規模な Unified CM の配置では、DHCP サーバを Unified CM サーバで実行して、これらのデバイスをサポートできます。ただし、Unified CM 上で実行する他の重要なサービスとの CPU 競合などの考えられるリソースの競合を回避するために、DHCP サーバの機能を専用サーバに移動することを推奨します。クラスタに 1000 を超えるデバイスが登録されている場合は、DHCP を Unified CM サーバでは*実行しない*で、専用のスタンドアロン サーバで実行する必要があります。

（注）　「*共存*」という用語は、同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態を指します。

トリビアル ファイル転送プロトコル（TFTP）

Cisco Unified CM システムにおいて、IP Phone などのエンドポイントは、TFTP プロセスを利用して設定ファイル、ソフトウェア イメージ、およびその他のエンドポイント固有の情報を取得します。シスコの TFTP サービスは、1 つ以上の Unified CM サーバで実行できるファイル サービス システムです。このサービスは、設定ファイルを構築し、ファームウェア ファイル、リンガー ファイル、デバイス コンフィギュレーション ファイルなどをエンドポイントに提供します。

TFTP ファイル システムは、次のような複数のファイル タイプを保持できます。

- 電話機設定ファイル
- 電話機ファームウェア ファイル
- Certificate Trust List（CTL）ファイル
- Identity Trust List（ITL）ファイル

- トーン ローカリゼーション ファイル
- ユーザ インターフェイス（UI）ローカリゼーションおよび辞書ファイル
- リンガー ファイル
- ソフトキー ファイル
- SIP 電話機のダイヤル プラン ファイル

TFTP サーバは、変更できないタイプ（電話機のファームウェア ファイルなど）と変更できるタイプ（設定ファイルなど）の 2 つのタイプのファイルを管理し、提供します。

一般的な設定ファイルには、デバイス（SCCP または SIP 電話機など）の Unified CM の優先順位順に並べられたリスト、デバイスがこれらの Unified CM に接続する TCP ポート、および実行可能なロード識別子があります。選択したデバイスの設定ファイルには、メッセージのロケール情報と URL、ディレクトリ、サービス、および電話機の情報ボタンなどが含まれています。

デバイスの設定が変更されると、TFTP サーバは Unified CM データベースから関連する情報をプルして、設定ファイルを再構築します。その後、電話機をリセットすると、新しいファイルが電話機にダウンロードされます。たとえば、1 台の電話機の設定ファイルが変更された場合（エクステンション モビリティのログインまたはログアウト時など）、そのファイルだけが再構築されて、電話機にダウンロードされます。ただし、デバイス プールの設定の詳細が変更された場合（プライマリ Unified CM サーバが変更された場合など）、このデバイス プール内のすべてのデバイスに対して、設定ファイルを再構築し、ダウンロードする必要があります。多数のデバイスが含まれているデバイス プールでは、このファイル再構築プロセスがサーバのパフォーマンスに影響を及ぼす可能性があります。

（注） Cisco Unified CM 6.1 よりも前のリリースでは、TFTP サーバは、変更されたファイルを再構築するために、パブリッシャのデータベースから情報をプルしました。Unified CM 6.1 以降のリリースでは、TFTP サーバは、共存するサブスクライバ サーバ上のデータベースからローカル データベースの読み取りを実行できます。ローカル データベースの読み取りは、パブリッシャが使用できない場合にユーザ方向機能を保持するなどの利点を提供するだけではなく、WAN を介したクラスタリングを通じて、複数の TFTP サーバの分散を可能にします（WAN を介したクラスタリングと同じ遅延規則が、登録済み電話機を持つサーバに関して TFTP サーバに適用されます）。この設定により、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離されることが保証されます。

デバイスが TFTP サーバに設定ファイルを要求すると、TFTP サーバは、内部キャッシュ、ディスク、さらには代替 Cisco ファイル サーバ（指定されている場合）内の設定ファイルを検索します。TFTP サーバが設定ファイルを検出すると、デバイスにそのファイルを送信します。設定ファイルに Unified CM 名が含まれている場合、デバイスは DNS を使用して名前を解決し、Unified CM に接続できます。デバイスが IP アドレスまたは名前を受信しない場合、TFTP サーバの名前または IP アドレスを使用して登録接続を試行します。TFTP サーバが設定ファイルを検出できない場合、「ファイルが見つかりませんでした」というメッセージをデバイスに送信します。

TFTP サーバが設定ファイルを再構築している最中、または要求の最大数を処理している最中に設定ファイルを要求したデバイスは、後で設定ファイルを要求するようにデバイスに指示するメッセージを TFTP サーバから受信します。Maximum Serving Count サービス パラメータは、TFTP サーバが同時に処理できる要求の最大数を指定し、設定できます（デフォルト値 = 500 の要求）。同じサーバ上で、TFTP サービスが他の Cisco CallManager サービスと一緒に実行されている場合、デフォルト値を使用します。専用 TFTP サーバでは、Maximum Serving Count として、シングル プロセッサ システムの場合 1500、デュアル プロセッサ システムの場合 3000 の推奨値を使用します。

Cisco Unified IP Phone 8900 シリーズおよび 9900 シリーズは、TFTP よりも大幅に高速な HTTP プロトコル（ポート 6970）を使用して TFTP 設定ファイルを要求します。

TFTP 動作の例

エンドポイントをリブートするたびに、エンドポイントは（TFTP を介して）設定ファイルを要求します。設定ファイルの名前は要求するエンドポイントの MAC アドレスに基づいています（たとえば、MAC アドレスが ABCDEF123456 の Cisco Unified IP Phone 7961 の場合、ファイル名は SEPABCDEF123456.cnf.xml となります）。受信した設定ファイルには、電話機で実行するソフトウェアのバージョンと、電話機の登録に使用する Cisco Unified CM サーバのリストが格納されています。エンドポイントは、必要な設定情報を取得し、動作可能にするために TFTP を介して、リンガー ファイル、ソフトキー テンプレート、およびその他のファイルをダウンロードすることもできます。

設定ファイルに、電話機が現在使用しているバージョン番号と異なるバージョン番号のソフトウェア ファイルが含まれている場合、電話機は TFTP サーバから新しいソフトウェア ファイルもダウンロードして、アップグレードします。エンドポイントがソフトウェアをアップグレードするためにダウンロードする必要があるファイルの数は、エンドポイントのタイプと、電話機の現在のソフトウェアと新しいソフトウェアの差分によって異なります。たとえば、Cisco Unified IP Phones 7961、7970、および 7971 は、最悪のケースのソフトウェア アップグレードで 5 つのソフトウェア ファイルをダウンロードします。

TFTP ファイル転送時間

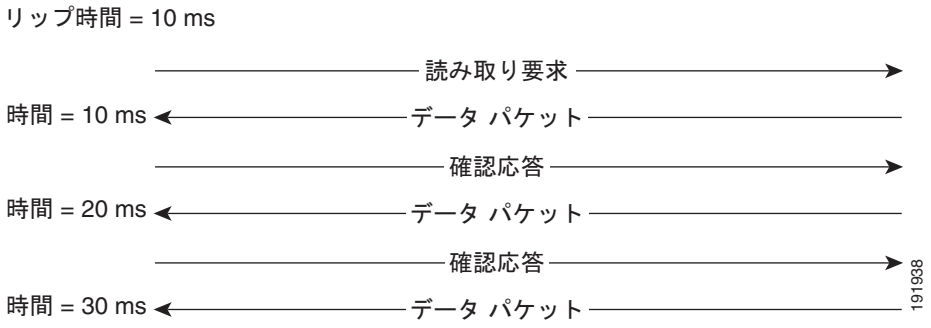
エンドポイントがファイルを要求するたびに、新しい TFTP 転送セッションが確立します。集中型コール処理配置の場合、これらの各転送が完了する時間は、エンドポイントを起動し、動作可能にするためにかかる時間と定期保守時にエンドポイントをアップグレードするためにかかる時間に影響を与えます。TFTP 転送時間は、これらの最終状態に影響を与える唯一の要因ではありませんが、重要なコンポーネントです。

TFTP を介して各ファイルの転送を完了する時間は、ファイル サイズ、再送信が必要な TFTP パケットの割合、およびネットワーク遅延またはラウンドトリップ時間の関数として予測可能です。

一目見ただけでは、ネットワーク帯域幅は前述のステートメントから欠落しているように見えますが、実際には再送信が必要な TFTP パケットの割合を介して含まれています。これは、ファイル転送をサポートするのに十分なネットワーク帯域幅がない場合、パケットはネットワーク インターフェイス キューイング アルゴリズムによってドロップされ、再送信する必要があるためです。

TFTP は User Datagram Protocol（UDP; ユーザ データグラム プロトコル）上で動作します。Transmission Control Protocol（TCP; 伝送制御プロトコル）とは異なり、UDP は信頼性の高いプロトコルではありません。つまり、UDP は本質的にパケット損失を検出する機能を備えていません。言うまでもなく、ファイル転送におけるパケット損失の検出は重要であるため、RFC 1350 は TFTP をロックステップ プロトコルとして規定しています。つまり、TFTP 送信側は 1 つのパケットを送信し、次のパケットを送信する前に応答を待ちます（図 3-8 を参照）。

図 3-8　TFTP パケット転送シーケンスの例

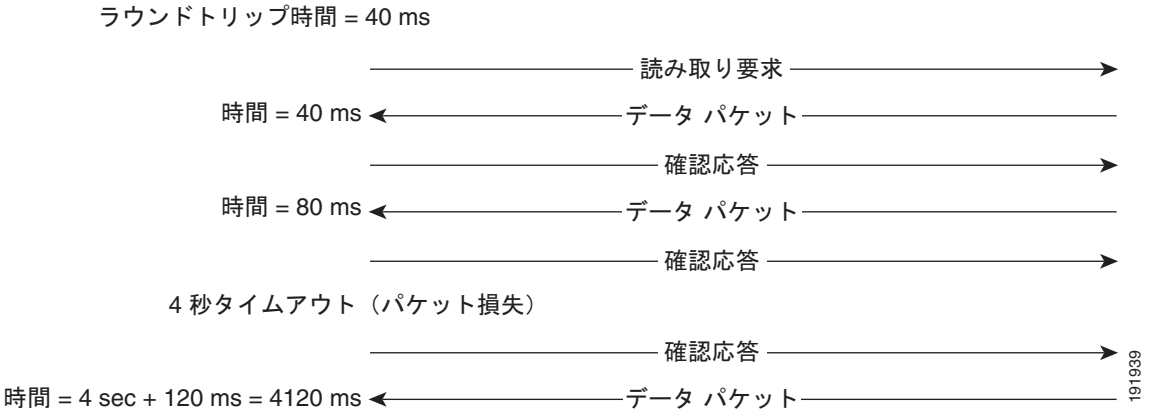


応答がタイムアウト時間（デフォルトでは 4 秒）内に受信されない場合、送信側はデータ パケットまたは確認応答を再送信します。5 回送信されても応答がない場合、TFTP セッションは失敗します。タイムアウト時間は常に同じであり、TCP タイムアウトのように適応できないので、パケット損失は、転送セッションを完了するのにかかる時間を大幅に増加させる可能性があります。

各データ パケット間の遅延は、最短でも、ネットワークのラウンドトリップ時間と同じなので、ネットワーク遅延は TFTP セッションで実現できる最大スループットの係数にもなります。

図 3-9 では、ラウンドトリップ時間が 40 ms に増加し、1 つのパケットが送信中に失われています。エラー率が 12% と高い率である一方、セッションを完了する時間が 30 ms（図 3-8 を参照）から 4160 ms（図 3-9 を参照）に増加しているので、TFTP の遅延とパケット損失の効果が簡単にわかります。

図 3-9　TFTP セッション完了時間におけるパケット損失の効果



次の公式を使用して、TFTP ファイル転送が完了するのにかかる時間を計算します。

FileTransferTime = FileSize * [(RTT + ERR * Timeout) / 512000]

定義：

FileTransferTime は秒単位です。

FileSize はバイト単位です。

RTT はラウンドトリップ時間（ミリ秒単位）です。

ERR はエラー率または失われたパケットの比率です。

Timeout はミリ秒単位です。

512000 =（TFTP パケット サイズ）*（1000 ミリ秒/秒）=
（512 バイト）*（1000 ミリ秒/秒）

表 3-5 と表 3-6 は、この公式を使用して、各種エンドポイント デバイス タイプ、プロトコル、およびネットワーク遅延用のソフトウェア ファイルの転送時間を計算した例を示しています。

表 3-5　SCCP デバイスの TFTP ファイル転送時間

デバイス タイプ（Cisco Unified IP Phone）	ファームウェア サイズ（バイト、100,000 未満の値は切り上げ）	転送完了時間（エラー率 1%）				
		RTT 40 ms	RTT 80 ms	RTT 120 ms	RTT 160 ms	RTT 200 ms
7985	15,000,000	39 分 3 秒	58 分 35 秒	78 分 7 秒	97 分 39 秒	117 分 11 秒
7921	9,700,000	25 分 15 秒	37 分 53 秒	50 分 31 秒	63 分 9 秒	75 分 46 秒
7975	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7970 または 7971	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7965 または 7945	6,300,000	16 分 24 秒	24 分 36 秒	32 分 48 秒	41 分 0 秒	49 分 13 秒
7962 または 7942	6,200,000	16 分 8 秒	24 分 13 秒	32 分 17 秒	40 分 21 秒	48 分 26 秒
7941 または 7961	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7931	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7911 または 7906	6,100,000	15 分 53 秒	23 分 49 秒	31 分 46 秒	39 分 42 秒	47 分 39 秒
7935	2,100,000	5 分 28 秒	8 分 12 秒	10 分 56 秒	13 分 40 秒	16 分 24 秒
7920	1,200,000	3 分 7 秒	4 分 41 秒	6 分 15 秒	7 分 48 秒	9 分 22 秒
7936	1,800,000	4 分 41 秒	7 分 1 秒	9 分 22 秒	11 分 43 秒	14 分 3 秒
7940 または 7960	900,000	2 分 20 秒	3 分 30 秒	4 分 41 秒	5 分 51 秒	7 分 1 秒
7910	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7912	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7905	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7902	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒

表 3-6　SIP デバイスの TFTP ファイル転送時間

デバイス タイプ（Cisco Unified IP Phone）	ファームウェア サイズ（バイト、100,000 未満の値は切り上げ）	転送完了時間（エラー率 1%）				
		RTT 40 ms	RTT 80 ms	RTT 120 ms	RTT 160 ms	RTT 200 ms
7975	6,600,000	17 分 11 秒	25 分 46 秒	34 分 22 秒	42 分 58 秒	51 分 33 秒
7970 または 7971	6,700,000	17 分 26 秒	26 分 10 秒	34 分 53 秒	43 分 37 秒	52 分 20 秒
7965 または 7945	6,600,000	17 分 11 秒	25 分 46 秒	34 分 22 秒	42 分 58 秒	51 分 33 秒
7962 または 7942	6,500,000	16 分 55 秒	25 分 23 秒	33 分 51 秒	42 分 19 秒	50 分 46 秒
7941 または 7961	6,500,000	16 分 55 秒	25 分 23 秒	33 分 51 秒	42 分 19 秒	50 分 46 秒
7911 または 7906	6,400,000	16 分 40 秒	25 分 0 秒	33 分 20 秒	41 分 40 秒	50 分 0 秒
7940 または 7960	900,000	2 分 20 秒	3 分 30 秒	4 分 41 秒	5 分 51 秒	7 分 1 秒
7912	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒
7905	400,000	1 分 2 秒	1 分 33 秒	2 分 5 秒	2 分 36 秒	3 分 7 秒

表 3-5 と表 3-6 の値は、必要なファームウェア ファイルを電話機にダウンロードするおおよその時間です。これは、電話機を新しいファームウェアにアップグレードし、動作可能になるまでにかかる時間の推定値では*ありません*。

Cisco Unified IP Phone ファームウェア リリース 7.*x* には、新しいファイルのダウンロード時に 10 分のタイムアウトが用意されています。この時間内に転送が完了しない場合、後で転送が正常に完了する場合であっても、電話機はダウンロードを破棄します。この問題が発生した場合は、ローカルの TFTP サーバを使用して、電話機を 8.*x* ファームウェア リリースにアップグレードすることを推奨します。このリリースには、61 分のタイムアウト値が用意されています。

ネットワーク遅延とパケット損失は TFTP 転送時間に上記のような影響を与えるので、ローカルの TFTP サーバは便利です。このローカルの TFTP サーバは、WAN を介したクラスタを使用する配置における Unified CM サブスクライバか、または Cisco サービス統合型ルータ（ISR）などで実行する代替のローカル TFTP Load Server です。最新のエンドポイント（より大きなファームウェア ファイルを必要とする）は、Load Server アドレスを使用して設定できます。これにより、エンドポイントは、中央の TFTP サーバから比較的小さい設定ファイルをダウンロードする一方で、ローカルの TFTP サーバ（Unified CM クラスタの一部ではない）を使用してより大きなソフトウェア ファイルをダウンロードできます。代替のローカル TFTP Load Server をサポートしている Cisco IP Phone の詳細については、「エンドポイント機能の要約」（P.18-53）を参照してください。

（注）　起動時に各電話機で実行される正確な処理と、ダウンロードされるファイルのサイズは、電話機のモデル、電話機に設定されているシグナリング タイプ（SCCP、MGCP、または SIP）、および電話機の以前の状態によって異なります。要求されるファイルは異なりますが、各電話機で実行される一般的なプロセスは同じで、すべての場合で TFTP を使用して適切なファイルが要求され、配送されます。TFTP サーバの配置に関する一般的な推奨事項が、プロトコルや配置する電話機モデルによって変わることはありません。

TFTP サーバの冗長性

オプション 150 を使用すると、最大 2 つの IP アドレスを DHCP スコープの一部として電話機に配布できます。電話機はリスト内の最初のアドレスを試行し、最初の TFTP サーバとの通信を確立できなければ、その次のアドレスを試行します。このアドレス リストには冗長性メカニズムがあるため、電話機は、そのプライマリ TFTP サーバに障害が発生しても、別のサーバから TFTP サービスを取得できます。

TFTP のロード シェアリング

TFTP サーバの順序が異なるリストを別のサブネットに付与して、ロード バランシングを実現することを推奨します。次の例を参考にしてください。

- サブネット 10.1.1.0/24：オプション 150：TFTP1_Primary、TFTP1_Secondary
- サブネット 10.1.2.0/24：オプション 150：TFTP1_Secondary、TFTP1_Primary

通常の動作では、10.1.1.0/24 の電話機は TFTP1_Primary に TFTP サービスを要求し、サブネット 10.1.2.0/24 の電話機は TFTP1_Secondary に TFTP サービスを要求します。TFTP1_Primary に障害が発生した場合、両方のサブネットからの電話機が TFTP1_Secondary に TFTP サービスを要求します。

ロード バランシングは、単一の TFTP サーバがホットスポットになること、つまり、複数のクラスタの電話機すべてが同じサーバを利用してサービスを取得しようとすることを回避します。TFTP ロード バランシングは、Unified CM のアップグレード時など、電話機のソフトウェア ロードが転送される場合に特に重要です。これは、転送されるファイルのサイズと数が増えることで、TFTP サーバにかかる負荷が大きくなるためです。

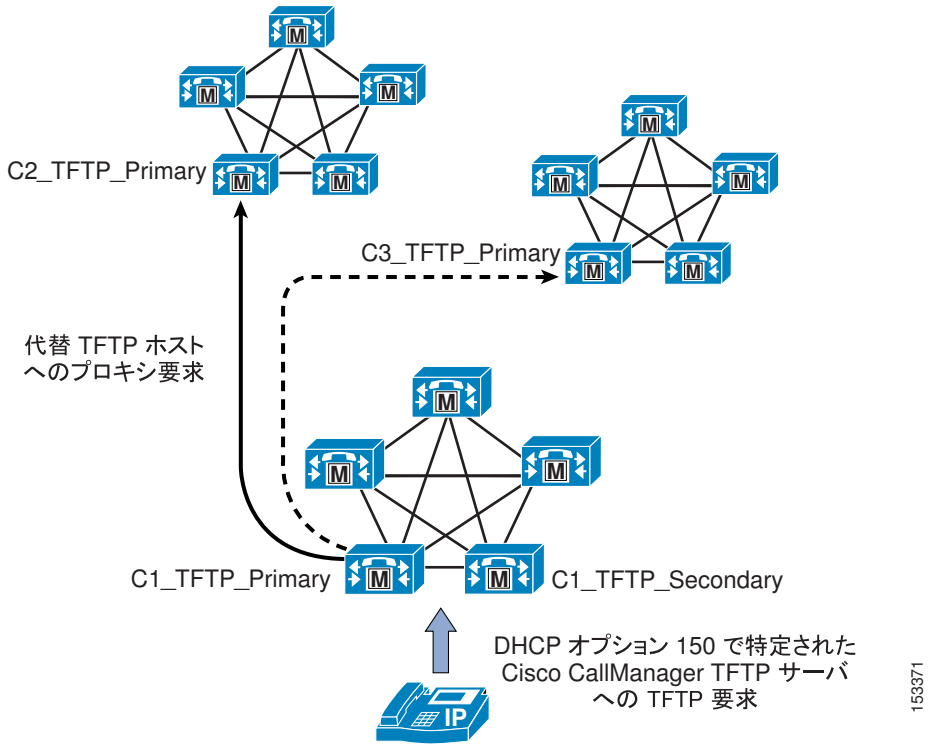
中央集中型 TFTP サービス

マルチクラスタ システムでは、単一のサブネットまたは VLAN に複数のクラスタの電話機を含めることができます。この場合、サブネットまたは VLAN 内のすべての電話機に提供されるアドレスの TFTP サーバは、電話機が属するクラスタに関係なく、各電話機から送信されるファイル転送要求に応答する必要があります。中央集中型 TFTP 配置では、1 つのクラスタに関連付けられている TFTP サーバのセットが、マルチクラスタ システムのすべての電話機に TFTP サービスを提供する必要があります。

このファイル アクセスの単一ポイントを提供するために、各クラスタの TFTP サーバは、中央のプロキシ TFTP サーバ経由でファイルを提供できる必要があります。Cisco Unified CM 5.0 では、中央の TFTP サーバに各クラスタの TFTP サーバをポイントするリダイレクト ロケーションのセットを設定することによって、このプロキシ設定を行います。この設定では、他のクラスタごとに 1 つずつ、中央の TFTP サーバの代替ファイル ロケーションの HOST リダイレクト ステートメントを使用します。中央集中型クラスタの各冗長 TFTP サーバは、各子クラスタの冗長サーバの 1 つをポイントする必要があります。中央集中型サーバが子クラスタの両方の冗長サーバをポイントする必要はありません。各クラスタ内でのファイルの再配布および中央クラスタの冗長サーバ間での電話機のフェールオーバー メカニズムには、高い耐障害性があるからです。

図 3-10 に、このプロセスの動作例を示します。Cluster 3 に登録されている電話機からの要求は、Cluster 1 で設定されている中央集中型 TFTP サーバ（C1_TFTP_Primary）に転送されます。このサーバは、次に、電話機が要求したファイルのコピーによる最初の応答があるまで、設定済みの代替 TFTP サーバのそれぞれに対して照会します。中央集中型セカンダリ TFTP サーバ（C1_TFTP_Secondary）への要求は、要求されたファイルが見つかるか、すべてのサーバから要求されたファイルが存在しないという応答があるまで、プロキシによって別のクラスタのセカンダリ TFTP サーバに送信されます。

図 3-10　　中央集中型 TFTP サーバ



リリースの異なる Unified CM を実行するサーバが含まれる混在環境の中央集中型 TFTP

以前の Unified CM リリースから Unified CM 5.0 以降のリリースに移行するときに、大規模な中央集中型 TFTP 環境では、混合モードでの運用が必要になることがよくあります。Unified CM 5.0 以前では、中央集中型 TFTP サーバは子サーバにファイルを要求せず、すべての子クラスタの TFTP ディレクトリをリモートで中央サーバにマウントし、すべてのローカル ディレクトリとリモート ディレクトリで要求されたファイルを検索していました。移行期間中は、両方のモード（Unified CM 5.0 以前で使用する *リモート マウント*と、Unified CM 5.0 以降のリリースで使用する *プロキシ要求*の混合モード）で動作できる中央集中型 TFTP サーバを提供する必要があります。Unified CM 5.0 以降のリリースに対応するサーバは、混在環境でのファイル システムのリモート マウントをサポートしないため、Cisco Unified CM 4.1(3)SR3a 以降の Windows OS ベースの Unified CM リリースを混合モードの中央集中型 TFTP クラスタとして配置する必要があります。

（注）　Cisco Unified CM Release 4.1(3)SR3a（およびそれ以降の Windows OS プラットフォーム対応の Unified CM リリース）には、混合モードの中央集中型 TFTP 設計をサポートする cTFTP サーバ デーモンへのアップグレードが含まれています。これらのリリースでは、中央集中型 TFTP サーバがリモート マウントとプロキシ要求の両方を、他のクラスタ内の代替 TFTP ファイル サーバに到達する方法としてサポートします。

混合モードの TFTP サーバを設定する場合、HOST プロキシ要求によって Unified CM 5.0 以降のリリースに対応するサーバを指定し、リモート マウント設定プロセスを使用して Unified CM 4.1(3)SR3a 以前の任意のサーバを指定する必要があります。例 3-2 を参照してください（リモート マウント設定の詳細については、次を参照してください）。混合モードをサポートする任意の子クラスタは、リモート マウントとプロキシ クラスタのどちらにも設定できます。

中央集中型 TFTP 設定では、メイン TFTP サーバは、最高のバージョンの Cisco Unified Communications Manager を実行するクラスタ内に存在する必要があります。たとえば、互換性がある Cisco Unified CM 4.*x*（混合モード）クラスタと Unified CM 7.0 クラスタ間で中央集中型 TFTP サーバを使用している場合、中央 TFTP サーバは Cisco Unified CM 7.0 クラスタ内に存在する必要があります。

中央集中型 TFTP サーバが低いバージョンの Cisco Unified Communications Manager を実行するクラスタ内に存在する場合、すべての電話機が、この中央集中型 TFTP サーバから提供されるロケール ファイルを使用します。これらの古いロケール ファイルには、新しくローカライズされた語句がメイン クラスタの TFTP サーバから提供されるロケール ファイルに含まれていないため、高いバージョンの Cisco Unified CM を実行するクラスタに登録された電話機の表示問題を引き起こす可能性があります。

例 3-2　混合モードの TFTP の設定

Unified CM TFTP サーバの [Service Parameters] > [TFTP Server] > [Cisco TFTP (Active) Parameters] で、次のように設定します。

- Parameter Name = パラメータ値
- Alternate Cisco File Server = HOST://10.10.10.1
- Alternate Cisco File Server = C:¥Program Files¥Cisco¥TFTPpath¥TFTP2

リモート マウントの代替 Cisco ファイル サーバ設定の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications SRND Based on Cisco Unified CallManager 4.x*』を参照してください。

http://www.cisco.com/go/ucsrnd

ネットワーク タイム プロトコル（NTP）

NTP を使用すると、ネットワーク デバイスは、そのクロックをネットワーク タイム サーバまたはネットワーク対応のクロックと同期させることができます。NTP は、ネットワーク内のすべてのデバイスが同じ時刻に設定されていることを保証するうえで重要です。テレフォニー ネットワークのトラブルシューティングまたは管理を行う場合は、ネットワーク全体でデバイス上にあるすべてのエラー ログ、セキュリティ ログ、トレース、およびシステム レポート内のタイムスタンプを同期させることが極めて重要です。この同期により、管理者は、ネットワークのアクティビティと動作を、共通の時系列に基づいて再現できます。課金記録とコール詳細レコード（CDR）でも、正確な同期時刻が必要になります。

Unified CM の NTP 時刻同期

時刻同期は、Unified CM サーバにおいて特に重要です。CDR レコードが正確で、ログ ファイルの同期が取れていることを保証するだけではなく、クラスタ内で将来的に IPSec 機能を有効にしたり、外部エンティティと通信したりするには、正確な時刻源が必要です。

Unified CM は、クラスタ内のすべてのサブスクライバの NTP 時刻を自動的にパブリッシャと同期します。インストール時に、各サブスクライバは自動的に、パブリッシャで実行されている NTP サーバをポイントするように設定されます。パブリッシャはマスター サーバと見なされ、外部サーバと同期するように設定されている場合を除き、内部ハードウェア クロックを基にクラスタに時刻を提供します。クラスタの時刻と外部時刻源を確実に同期させるために、パブリッシャは Stratum-1、Stratum-2、または Stratum-3 NTP サーバをポイントするように設定することを強く推奨します。

Unified CM を Cisco IOS または Linux ベースの NTP サーバと同期させることを推奨します。Windows Time Services を NTP サーバとして使用することは推奨できず、サポート対象にもなっていません。Windows Time Services は、多くの場合、Simple Network Time Protocol（SNTP; 簡易ネットワーク タイム プロトコル）を使用していますが、Linux ベースの CM は SNTP とは正常に同期できないためです。

互換性、精度、およびネットワーク ジッタの問題を回避するために、プライマリ ノードに指定する外部 NTP サーバは、NTP v4（バージョン 4）にしてください。IPv6 アドレッシングを使用している場合は、外部 NTP サーバは、NTP v4 *でなければなりません*。

（注）　NTP.conf ファイルの手動設定はできなくなりました。このファイルに対して行った変更は、自動的にシステム設定で置き換えられます。

Cisco Unified Communications 環境における NTP 時刻同期に関する追加情報については、次の Web サイトで入手可能なホワイト ペーパー『*Cisco IP Telephony Clock Synchronization: Best Practices*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_white_paper0900aecd8037fdb5.shtml

Cisco IOS と CatOS の NTP 時刻同期

時刻同期は、ネットワーク内の他のデバイスにも重要です。Cisco IOS ルータと Catalyst スイッチは、NTP を介してそれぞれの時刻をその他のネットワーク デバイスと同期させるように設定する必要があります。この設定は、デバッグ メッセージ、syslog メッセージ、およびコンソール ログ メッセージにタイムスタンプが適切に付加されることを保証するうえで重要です。ネットワーク全体でデバイスに発生するイベントの明確な時間記録が得られれば、テレフォニー ネットワークの問題に関するトラブルシューティングが簡素化されます。

例 3-3 は、Cisco IOS および CatOS デバイスに対する NTP 時刻同期の設定を示しています。

例 3-3　　Cisco IOS と CatOS の NTP 設定

Cisco IOS の設定：

```
ntp server 64.100.21.254
```

CatOS の設定：

```
set ntp server 64.100.21.254
set ntp client enable
```

ルータとスイッチの NTP 時刻同期が適切に行われるよう保証するには、**clock timezone** コマンド（Cisco IOS の場合）、**set timezone** コマンド（CatOS の場合）、またはその両方を使用して、時間帯を設定することが必要になる場合があります。

WAN インフラストラクチャ

統合されたネットワーク上で Unified Communications を正常に動作させるには、WAN インフラストラクチャを適切に設計することも極めて重要です。インフラストラクチャを適切に設計するには、基本的な設定と設計に関するベスト プラクティスに従って、できるだけ可用性の高い、スループットを保証できる WAN を配置する必要があります。さらに、WAN インフラストラクチャを適切に設計するには、すべての WAN リンク上にエンドツーエンド QoS を配置する必要もあります。次の項では、これらの要件について説明します。

- 「WAN の設計と設定」（P.3-36）
- 「WAN の QoS」（P.3-40）
- 「リソース予約プロトコル（RSVP）」（P.11-18）
- 「帯域幅のプロビジョニング」（P.3-47）

WAN の設計と設定

WAN を適切に設計するには、耐障害性のあるネットワーク リンクを構築し、このリンクが使用不能になる可能性を考える必要があります。耐障害性のある冗長なネットワークを構築するには、慎重に WAN トポロジを選択し、必要な帯域幅をプロビジョニングし、ネットワーク トポロジ内の別のレイヤと同じように WAN インフラストラクチャにアプローチします。次の項では、必要なインフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「配置上の考慮事項」（P.3-36）
- 「保証帯域幅」（P.3-38）
- 「ベストエフォート型の帯域幅」（P.3-39）

配置上の考慮事項

音声ネットワークの WAN 配置では、ハブアンドスポーク、フル メッシュ構造、または部分メッシュ構造のトポロジを使用できます。ハブアンドスポーク トポロジは、1 つの中央ハブ サイトと、中央ハブ サイトに接続された複数のリモート スポーク サイトで構成されます。このシナリオでは、各リモート（スポーク）サイトは、中央（ハブ）サイトから 1 WAN リンク ホップ離れており、他のすべてのスポーク サイトから 2 WAN リンク ホップ離れています。メッシュ構造のトポロジには複数の WAN リンクが含まれ、サイト間のホップ数は任意です。このシナリオでは、同じサイトに対して複数の異なるパ

スがあり、別のサイトと異なるリンクで通信が行われるサイトがあります。最も単純な例として、他の 2 つのサイトとの WAN リンクを持つ 3 つのサイトが三角形を形成している例があります。この場合、あるサイトから別のサイトへのパスは 2 つあります。

トポロジ非対応コール アドミッション制御を行うには、WAN をハブアンドスポークにするか、MPLS VPN の場合はスポークレス ハブにする必要があります。このトポロジにすると、Unified CM のロケーションまたはゲートキーパーによって提供されるコール アドミッション制御によって、WAN にある任意の 2 つのサイト間で使用可能な帯域幅が正常にトラッキングされます。また、WAN リンクを介して複数のハブアンドスポーク配置を相互接続することもできます。

トポロジ対応コール アドミッション制御は、ハブアンドスポークと任意の WAN トポロジの両方で使用できます。このコール アドミッション制御の形式には、リソース予約プロトコル（RSVP）をサポートする WAN インフラストラクチャの部分が必要です。詳細については、「リソース予約プロトコル（RSVP）」（P.11-18）および「コール アドミッション制御」（P.11-1）を参照してください。

集中型および分散型マルチサイト配置モデルや、これらの配置モデルに対する Multiprotocol Label Switching（MPLS）の影響に関する詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

可能であれば、WAN リンクを冗長にして、より高いレベルの耐障害性を実現する必要があります。冗長な WAN リンクを、別のサービス プロバイダーから入手するか、またはネットワーク内の物理的に異なる入力/出力点に配置すると、単一のリンクに障害が発生してもバックアップの帯域幅および接続性を利用できることが保証されます。障害のないシナリオでは、この冗長リンクを使用して、追加の帯域幅を利用し、WAN 内の複数のパスと機器を介してフローごとにトラフィックのロード バランシングを行うことができます。トポロジ非対応コール アドミッション制御では、サイト間で使用できる帯域幅を減少させる障害が発生した場合に、コール アドミッション制御メカニズムがこれらの障害または帯域幅の減少の影響を受けないように、通常、冗長パスを多めにプロビジョニングし、少なめにサブスクライブする必要があります。トポロジ対応コール アドミッション制御では、トポロジの変更の多くを動的に調整でき、使用可能な合計帯域幅を効率的に使用できます。

音声とデータは、LAN で収束される場合とまったく同じように、WAN でも収束される必要があります。QoS プロビジョニングおよびキューイング メカニズムは、一般に、WAN 環境において音声とデータを同じ WAN リンク上で相互運用できることを保証するために使用されます。音声とデータを分離して別々のリンク上で転送すると、多くの場合において問題になることがあります。これは、1 つのリンクで障害が発生すると、一般に、すべてのトラフィックが単一リンクに集中するためです。その結果、トラフィックの各タイプでスループットが減少し、ほとんどの場合において音声品質が低下します。さらに、ネットワーク リンクまたはデバイスを別々に保守すると、最善を尽くしても、トラブルシューティングや管理が困難になります。

WAN リンクでは、障害が発生する可能性や、オーバーサブスクリプションになる可能性があるため、WAN のもう一方の側にあるサイトには、必要に応じて非集中型のリソースを配置することを推奨します。特に、メディア リソース、DHCP サーバ、および音声ゲートウェイのほか、Survivable Remote Site Telephony（SRST）や Cisco Unified Communications Manager Express（Unified CME）などのコール処理アプリケーションは、適宜、サイトの規模やそのサイトにおけるこれらの機能の重要性に応じて、中央以外のサイトに配置される必要があります。音声アプリケーションおよびデバイスを非集中化すると、ネットワーク配置がより複雑になり、企業全体でこれらのリソースを管理する作業もより複雑になり、さらにネットワーク ソリューションの総コストが増加する可能性があることに留意してください。ただし、WAN リンク障害の発生中にリソースが使用可能になるという事実により、これらの要因は軽減される場合もあります。

WAN 環境に音声を配置する場合は、WAN リンクを通過するすべての音声コールに対して低帯域幅の G.729 コーデックを使用することを推奨します。これは、この方法によって、このような低速リンク上で帯域幅が節約されるためです。さらに、MoH などのメディア リソースは、可能であればマルチキャスト トランスポート メカニズムを使用するように設定される必要があります。これは、この方法によって、さらに帯域幅が節約されるためです。

音声に対する QoS 保証のないベストエフォート ネットワークを介してコールが行われる場合は、Internet Low Bit Rate Codec（iLBC）を使用することを検討してください。これにより、フレームが失われる可能性のあるネットワークで、品位のある音声品質の低下と適切なエラー復元特性が可能になります。コーデック タイプとサンプル サイズに基づく帯域幅使用量の詳細については、表 3-9 を参照してください。

IP 音声ネットワークの遅延

International Telecommunication Union（ITU; 国際電気通信連合）の G.114 勧告には、音声ネットワークにおける片方向の遅延は 150 ミリ秒以下でなければならないと明記されています。ネットワーク内に低速 WAN リンクを実装する場合は、この要件に留意することが重要です。片方向の遅延がこの 150 ミリ秒の勧告を超えないように、WAN リンクのトポロジ、テクノロジー、および物理的な距離を考慮する必要があります。片方向の遅延が 150 ミリ秒を超える VoIP ネットワークの実装は、音声コールの品質だけでなく、コールのセットアップ時間およびメディアのカットスルー時間にかかわる問題ももたらします。これは、コールを確立するために、各デバイスとコール処理アプリケーション間で複数のコール シグナリング メッセージを交換する必要があるためです。

保証帯域幅

音声は、一般に、重要なネットワーク アプリケーションと見なされるため、ベアラおよびシグナリング音声トラフィックが常にその宛先に到達することが不可欠となります。このため、専用の保証帯域幅を提供できる WAN トポロジおよびリンク タイプを選択することが重要です。次に示す WAN リンク テクノロジーは、専用の保証帯域幅を提供できます。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM/フレームリレーのサービス インターワーキング
- Multiprotocol Label Switching（MPLS）
- Cisco 音声およびビデオ対応 IP Security VPN（IPSec V3PN）

これらのリンク テクノロジーは、専用の方式で配置されているか、またはプライベート ネットワークに配置されている場合に、保証トラフィック スループットを提供できます。これらの WAN リンク テクノロジーはいずれも、特定の速度または帯域幅サイズでプロビジョニングできます。また、これらのリンク テクノロジーには、低リンク速度でもネットワーク トラフィックのスループットを保証できる組み込みメカニズムがあります。トラフィック シェーピング、フラグメンテーションとパケット インターリーブ、および Committed Information Rate（CIR; 認定情報レート）などの機能を使用すると、WAN においてパケットがドロップされないこと、すべてのパケットが定期的に WAN リンクにアクセスできること、およびこれらのリンクを通過しようとするすべてのネットワーク トラフィックが十分な帯域幅を使用できることを保証できます。

Dynamic Multipoint VPN（DMVPN）

スポークツースポーク DMVPN ネットワークは、ハブアンドスポーク トポロジと比較して、Cisco Unified Communications に対する利点を提供できます。スポークツースポーク トンネルは、WAN のホップ数と復号化/暗号化段階を削減することで、エンドツーエンドの遅延の低減をもたらします。また、DMVPN は、関連した管理および操作上のオーバーヘッドなしで、ポイントツーポイント トンネルのフル メッシュと同等の簡素化された設定方法を提供します。スポークツースポーク トンネルの使用はハブのトラフィックも削減し、その結果、帯域幅とルータ処理キャパシティを節約できます。ただし、スポークツースポーク DMVPN ネットワークは、スポークハブスポーク パスからスポークツースポーク パスへの RTP パケット ルーティングの転送時に発生する遅延変動（ジッタ）の影響を受けやす

くなっています。この DMVPN パス転送時の遅延における変動は、コールの非常に早い段階で発生し、通常は気が付きません。ただし、遅延の差が 100 ms を超える場合、単一の瞬間的なオーディオのひずみが聞こえる場合があります。

集中型コール処理を使用するマルチサイト DMVPN WAN の配置に関する詳細については、『*Cisco Unified Communications Voice over Spoke-to-Spoke DMVPN Test Results and Recommendations*』を参照してください。このドキュメントは、http://www.cisco.com/go/designzone で入手可能です。

ベストエフォート型の帯域幅

WAN トポロジの中には、専用の保証帯域幅を提供できないために、ネットワーク トラフィックが重要な場合であってもそのトラフィックが宛先に到達することを保証できないものがあります。このようなトポロジでは、音声トラフィックに重大な問題が発生する場合があります。その理由は、保証ネットワーク スループットをプロビジョニングするメカニズムがないためだけでなく、トラフィック シェーピング、パケット フラグメンテーションとインターリーブ、キューイング メカニズム、またはエンドツーエンド QoS を備えていないために、音声などの重要なトラフィックが優先的に処理されることを保証できないためです。

次に示す WAN ネットワーク テクノロジーおよびリンク タイプは、このようなベストエフォート型の帯域幅テクノロジーの例です。

- インターネット
- DSL
- ケーブル
- 衛星
- 無線

ほとんどの場合、これらのリンク タイプはいずれも、重要な音声および音声アプリケーションに必要となる、保証されたネットワーク接続性および帯域幅を提供できません。ただし、これらのテクノロジーは、個人用または在宅勤務者用のネットワーク配置に適している場合があります。これらのトポロジは、可用性の高いネットワーク接続性と、十分なネットワーク スループットを提供できる一方で、長期間にわたって使用不能になる場合や、速度が抑制されるために音声などのリアルタイム アプリケーションでネットワーク スループットが不足する場合、あるいは大量のパケット損失を引き起こすために繰り返し再送信することが必要になる場合があります。言い換えると、これらのリンクとトポロジは、保証帯域幅を提供できません。また、トラフィックをこれらのリンク上で送信する場合は、ベストエフォートで送信されるため、その宛先に到達することが保証されません。このため、企業クラスの音声サービスおよび品質が要求される音声対応のネットワークには、ベストエフォート型の WAN トポロジを*使用しない*ことを推奨します。

（注） DSL およびケーブル テクノロジーの新しい QoS メカニズムの中には、保証帯域幅を提供できるものがあります。ただし、これらのメカニズムは、多くのサービス プロバイダーによって一般的に配置されているものではありません。一般にベストエフォートに基づくネットワークで QoS 保証を提供するサービスの場合、サービス プロバイダーの Service Level Agreement（SLA; サービス レベル契約）で提供される帯域幅および QoS 保証を確認して理解することが重要です。

（注） アップストリームおよびダウンストリームの QoS メカニズムが、ワイヤレス ネットワークにおいてサポートされるようになりました。Voice over Wireless LAN の QoS の詳細については、http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html で入手可能な『*Voice over Wireless LAN Design Guide*』を参照してください。

WAN の QoS

ネットワークに音声およびビデオのトラフィックを送る場合は、事前に、必要なすべてのアプリケーションに十分な帯域幅があることを確認することが重要です。この帯域幅をプロビジョニングしたら、すべてのインターフェイス上で音声プライオリティ キューイングを実行する必要があります。トラフィックのバーストがバッファをオーバーサブスクリプションにする場合、ジッタとパケット損失を削減するには、このキューイングが必要です。このキューイング要件は、LAN インフラストラクチャの要件とほぼ同じです。

次に、WAN では、一般に、トラフィック シェーピングなどの追加メカニズムを使用して、WAN リンク上で処理能力を超えるトラフィックが送信されないことを保証する必要があります。処理能力を超えるトラフィックが送信されると、パケットがドロップされる場合があります。

最後に、リンク効率化技術を WAN パスに適用できます。たとえば、Link Fragmentation and Interleaving（LFI; リンク フラグメンテーション/インターリーブ）を使用すると、小さな音声パケットが大きなデータ パケットの後に続いてキューに入ることを防止できます。このようにキューに入ると、低速リンク上で許容できない遅延が発生することがあります。

これらの QoS メカニズムの目標は、音声トラフィックの遅延、パケット損失、およびジッタを削減することで、信頼性の高い、高品質の音声を保証することです。表 3-7 は、この目標を実現するために WAN インフラストラクチャで必要となる QoS 機能とツールを示しています。

表 3-7　WAN テクノロジーとリンク速度ごとの Unified Communications サポートに必要な QoS 機能とツール

WAN テクノロジー	リンク速度：56 ～ 768 kbps	リンク速度：768 kbps 以上
専用回線	• MLP（マルチリンク ポイントツーポイント プロトコル） • MLP LFI（リンク フラグメンテーション/インターリーブ） • LLQ（低遅延キューイング） • オプション：cRTP（RTP ヘッダー圧縮）	• LLQ
フレームリレー（FR）	• トラフィック シェーピング • LFI（FRF.12） • LLQ • オプション：cRTP • オプション：Voice-Adaptive Traffic Shaping（VATS） • オプション：Voice-Adaptive Fragmentation（VAF）	• トラフィック シェーピング • LLQ • オプション：VATS
非同期転送モード（ATM）	• TX-ring バッファ変更 • MLP over ATM • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • LLQ

表 3-7　WAN テクノロジーとリンク速度ごとの Unified Communications サポートに必要な QoS 機能とツール（続き）

WAN テクノロジー	リンク速度：56 ～ 768 kbps	リンク速度：768 kbps 以上
フレームリレーと ATM のサービス インターワーキング（SIW）	• TX-ring バッファ変更 • MLP over ATM と FR • MLP LFI • LLQ • オプション：cRTP（MLP が必要）	• TX-ring バッファ変更 • MLP over ATM と FR • LLQ
Multiprotocol Label Switching（MPLS）	• インターフェイス テクノロジーに応じて、上記と同じ • 一般に、サービス プロバイダーの仕様に応じて、フローをリマークするにはクラスベースのマーキングが必要	• インターフェイス テクノロジーに応じて、上記と同じ • 一般に、サービス プロバイダーの仕様に応じて、フローをリマークするにはクラスベースのマーキングが必要

次の各項では、音声とデータの両方のトラフィックをサポートするように WAN を設計する場合に、考慮すべき最も重要な機能と手法を説明しています。

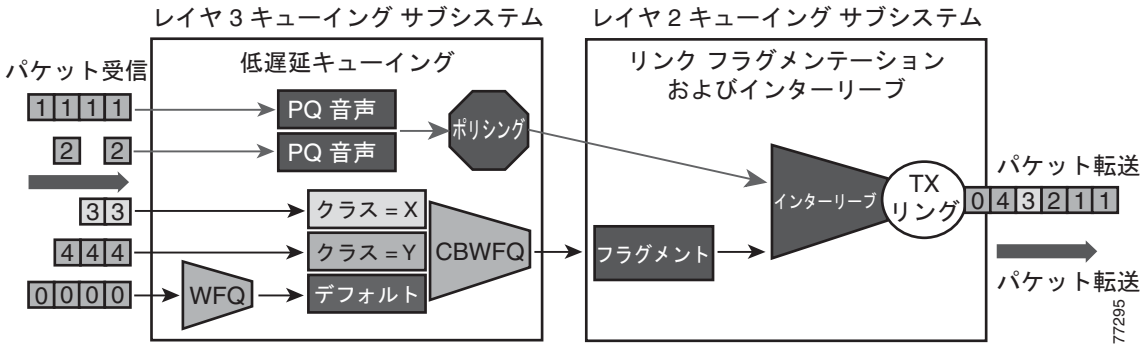
- 「トラフィックの優先順位」（P.3-41）
- 「リンク効率化手法」（P.3-43）
- 「トラフィック シェーピング」（P.3-45）

トラフィックの優先順位

多数の使用可能な優先付け体系の中から選択する場合、関係するトラフィックのタイプと、WAN 上のメディアのタイプが主に考慮すべき要素です。IP WAN を介したマルチサービス トラフィックの場合は、すべてのリンクに対して Low-Latency Queuing（LLQ; 低遅延キューイング）を使用することを推奨します。この方法では、最大 64 のトラフィック クラスをサポートできるほか、たとえば、音声と双方向ビデオに対するプライオリティ キューイング動作、音声制御トラフィックに対する最小帯域幅のクラスベース WFQ、主幹業務のデータに対する追加の最小帯域幅の WFQ、およびその他すべてのトラフィック タイプに対するデフォルトのベストエフォート型キューを指定できます。

図 3-11 は、優先付け体系の例を示しています。

図 3-11　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先付けの基準を使用することを推奨します。

- *音声*がプライオリティ キューに入る基準は、Differentiated Services Code Point（DSCP）値 46、または Per-Hop Behavior（PHB）値 EF です。
- *ビデオ会議*トラフィックがプライオリティ キューに入る基準は、DSCP 値 34、または PHB 値 AF41 です。ただし、ビデオ トラフィックはパケット サイズが大きいため、このパケットをプライオリティ キューに入れるのは、768 Kbps を超える速度の WAN リンク上に限定する必要があります。この値に満たないリンク速度では、パケット フラグメンテーションが必要です。ただし、プライオリティ キューに入るパケットはフラグメント化されません。そのため、小さな音声パケットが大きなビデオ パケットの後に続いてキューに入る可能性があります。768 Kbps 以下の速度のリンクでは、ビデオ会議トラフィックは別のクラスベース WFQ（CBWFQ）に入る必要があります。

  （注）　片方向ビデオ トラフィック（ビデオ オンデマンドやライブ ビデオ フィードなどのサービス向けのストリーミング ビデオ アプリケーションによって生成されるトラフィックなど）は、常に CBWFQ 方式を使用する必要があります。これは、このタイプのトラフィックは、双方向ビデオ会議トラフィックよりも遅延許容度がはるかに高いためです。

- WAN リンクが輻輳すると、*音声制御シグナリング* プロトコルが停止する可能性があります。したがって、IP Phone が IP WAN を介してコールできなくなります。そのため、音声制御プロトコル（たとえば、H.323、MGCP、および Skinny Client Control Protocol（SCCP））には、独自のクラスベース WFQ が必要です。このキューに入る基準は、DSCP 値 24 または PHB 値 CS3 です。

  （注）　シスコでは、音声制御プロトコルのマーキングを DSCP 26（PHB AF31）から DSCP 24（PHB CS3）に移行しました。ただし、一部の製品は、引き続きシグナリング トラフィックを DSCP 26（PHB AF31）としてマークします。したがって、コール シグナリング用に AF31 と CS3 の両方を予約することを推奨します。

- 場合によっては、特定のデータ トラフィックで、ベストエフォート型よりも優れた処理が必要になることがあります。このトラフィックは、*ミッションクリティカル データ*と呼ばれ、必要な帯域幅を持つ 1 つ以上のキューに入ります。このクラス内のキューイング方式は、最小帯域幅が割り当てられた First-In-First-Out（FIFO; ファーストインファーストアウト）です。このクラスのトラフィックは、設定された帯域幅限界を超えると、デフォルト キューに入れられます。このキューへの入力基準は、Transmission Control Protocol（TCP）ポート番号、レイヤ 3 アドレス、または DSCP/PHB 値にすることができます。
- 残りの企業トラフィックはすべて、ベストエフォート型処理のデフォルト キューに入れることができます。キーワード **fair** を指定すると、キューイング アルゴリズムは WFQ になります。

Scavenger Class

Scavenger Class は、特定のアプリケーションに対してベストエフォート未満のサービスを提供することを目的としています。このクラスに割り当てられるアプリケーションは、企業の組織的目標にはほとんどまたはまったく貢献せず、本質的にはエンターテイメント志向であることが一般的です。

Scavenger トラフィックを最小帯域幅キューに割り当てることにより、輻輳期間中はこのトラフィックが抑制されて事実上発生しなかったことにされますが、オフピーク時に発生するなどで帯域幅が業務目的で使用されていない場合には、このトラフィックが使用可能になります。

- Scavenger トラフィックは、DSCP CS1 としてマークされる必要があります。
- Scavenger トラフィックは、最小限の設定可能なキューイング サービスに割り当てられる必要があります。たとえば、Cisco IOS では、Scavenger Class に 1% の CBWFQ を割り当てることになります。

リンク効率化手法

次のリンク効率化技術によって、低速 WAN リンクの品質と効率が向上します。

Compressed Real-Time Transport Protocol（cRTP）

cRTP を使用すると、リンク効率化を高めることができます。このプロトコルは、40 バイトの IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、および RTP ヘッダーを約 2 ～ 4 バイトに圧縮します。cRTP は、ホップごとに動作します。個々のリンクで cRTP を使用するのは、そのリンクが次の条件を*すべて*満たす場合だけにしてください。

- 音声トラフィックによる負荷が、特定リンク上で 33% を超えている場合。
- リンクが低ビット レート コーデック（たとえば G.729）を使用する場合。
- 他のリアルタイム アプリケーション（たとえば、ビデオ会議）が同じリンクを使用しない場合。

リンクが上記の条件のいずれかを満たさない場合、cRTP は無効であり、そのリンクで使用しないでください。cRTP を使用する前に考慮する必要があるもう一つの重要なパラメータは、ルータの CPU 使用率です。これは、圧縮操作と圧縮解除操作によって悪影響を受けます。

ATM とフレームリレーの Service Inter-Working（SIW; サービス インターワーキング）リンクで cRTP を使用する場合は、Multilink Point-to-Point Protocol（MLP; マルチリンク ポイントツーポイント プロトコル）を使用する必要があります。

cRTP 圧縮は、パケットが出力インターフェイスを通過する前、つまり、LLQ クラスベース キューイングが行われた後の最終段階として行われます。Cisco IOS Release 12.2(2)T からは、cRTP により、*音声*クラスの帯域幅を圧縮パケット値に基づいて設定できる LLQ クラスベース キューイング メカニズムへのフィードバック メカニズムを使用できるようになりました。12.(2)2T よりも前の Cisco IOS リリースでは、このメカニズムは使用されていないため、LLQ は圧縮帯域幅を認識しません。したがって、圧縮が行われないものとして*音声*クラスの帯域幅をプロビジョニングする必要があります。表 3-8 は、512 Kbps リンクで G.729 コーデックを使用して 10 コールに対応する場合の、*音声*クラスの帯域幅の設定における違いの例を示しています。

表 3-8 では、cRTP 以外の G.729 コールの場合が 24 Kbps で、cRTP の G.729 コールの場合が 10 Kbps であることを前提としていることに注意してください。これらの帯域幅の数値は、音声ペイロードと IP/UDP/RTP ヘッダーだけに基づいています。レイヤ 2 ヘッダーの帯域幅は考慮に入れていません。ただし、実際の帯域幅プロビジョニングでは、レイヤ 2 ヘッダーの帯域幅も、WAN リンクで使用されたタイプに基づいて考慮に入れられます。

表 3-8　512 Kbps リンク帯域幅と G.729 コーデックを使用して 10 コールに対応する場合の LLQ 音声クラスの帯域幅要件

Cisco IOS リリース	cRTP が設定されていない場合	cRTP が設定されている場合
12.2(2)T よりも前	240 kbps	240 kbps[1]
12.2(2)T 以降	240 kbps	100 kbps

1. 不要な帯域幅の 140 Kbps は、LLQ *音声*クラスで設定される必要があります。

また、Cisco IOS Release 12.2(13)T からは、Class-Based cRTP 機能を使用して、cRTP を音声クラスの一部として設定できるようになったことにも注意してください。このオプションを使用すると、サービス ポリシーを介してインターフェイスに接続されているクラス内で cRTP を指定できます。この新しい機能により、**show policy interface** コマンドを使用して、圧縮の統計情報や帯域幅の状況を表示できます。このコマンドは、cRTP が IP/RTP ヘッダーを圧縮している事実を踏まえて、インターフェイス サービス ポリシー クラスに対して提供されるレートを確認するときに非常に役立つ場合があります。

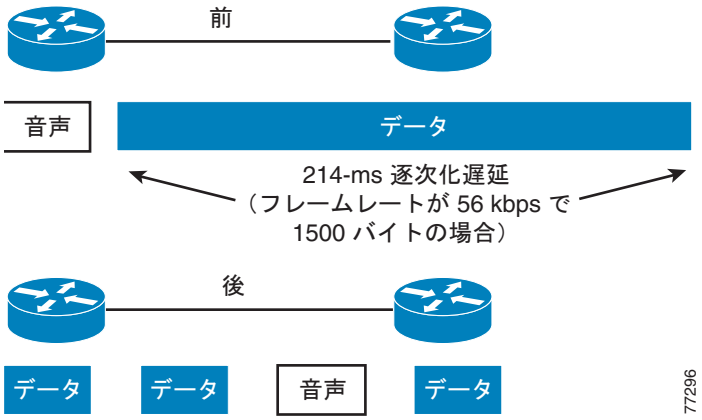
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns817/landing_voice_video.html

リンク フラグメンテーション/インターリーブ（LFI）

低速リンク（768 Kbps 未満）の場合、許容できる音声品質を確保するには、LFI メカニズムを使用する必要があります。この手法は、図 3-12 に示されているように、大きなデータ フレームの背後で、音声トラフィックが遅延しないようにして、ジッタを制限します。この目的のための 2 つの手法は、Multilink Point-to-Point Protocol（MLP; マルチリンク ポイントツーポイント プロトコル）LFI（専用回線、ATM、および SIW 用）と、フレームリレー用の FRF.12 です。

図 3-12　　リンク フラグメンテーション/インターリーブ（LFI）



Voice-Adaptive Fragmentation（VAF）

上記の LFI メカニズムのほかに、フレームリレー リンク用の LFI メカニズムには Voice-Adaptive Fragmentation（VAF）もあります。VAF は FRF.12 フレームリレー LFI を使用します。ただし、VAF が設定されている場合、フラグメンテーションが発生するのは、LLQ プライオリティ キューにトラフィックが存在する場合、またはインターフェイス上で H.323 シグナリング パケットが検出された場合だけです。この方法を使用すると、WAN インターフェイス上で音声トラフィックが送信されているときに、大きなパケットがフラグメント化およびインターリーブされることが保証されます。ただし、WAN リンク上に音声トラフィックが存在しない場合は、フラグメント化されていないリンクを介してトラフィックが転送されるため、フラグメンテーションに必要なオーバーヘッドが低減されます。

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合せて使用されます（「Voice-Adaptive Traffic Shaping（VATS）」（P.3-46）を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてか

ら、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

トラフィック シェーピングは、ATM やフレーム リレーなどの複数アクセスの非ブロードキャスト メディアに必要です。この場合、物理的なアクセス速度は 2 つのエンドポイント間で異なり、複数の支店サイトは、一般に中央サイトの単一ルータ インターフェイスに集約されます。

図 3-13 は、同一 IP WAN 上での音声とデータの転送時にトラフィック シェーピングが必要な主な理由を示しています。

図 3-13　フレームリレーと ATM を使用したトラフィック シェーピング

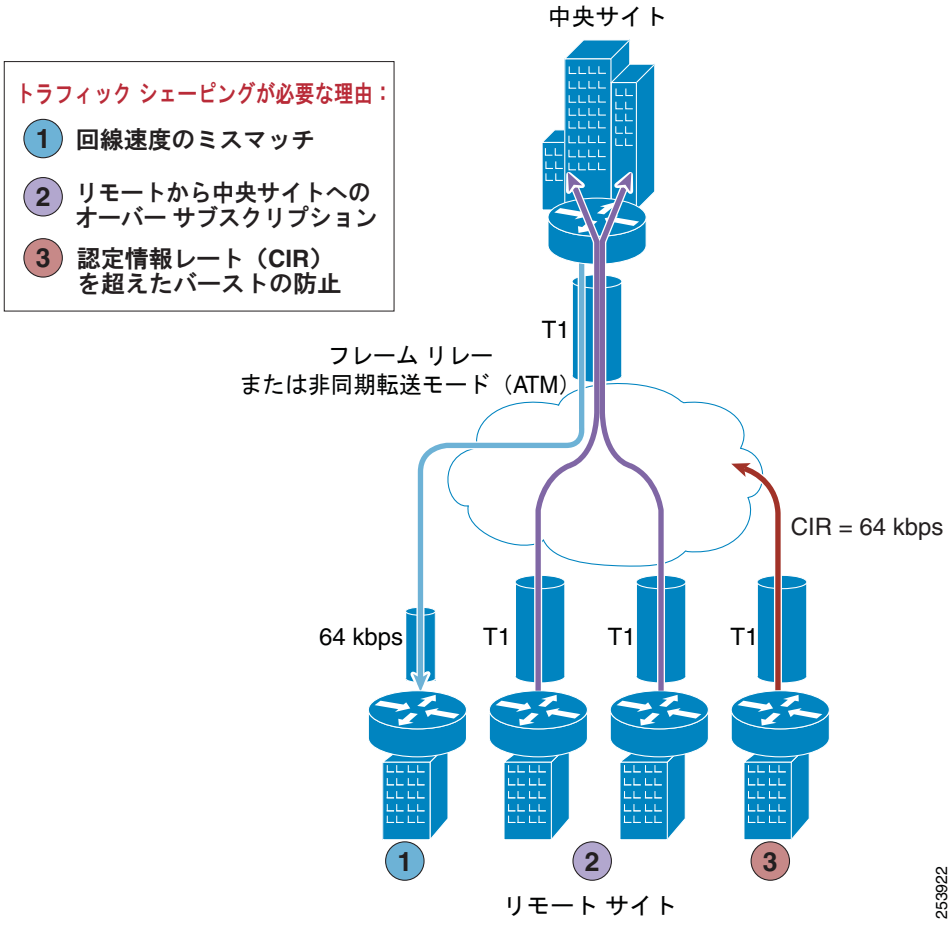


図 3-13 は、次の 3 つのシナリオを示しています。

1. 回線速度のミスマッチ

中央サイトのインターフェイスは、一般に高速インターフェイス（たとえば、T1 以上）ですが、小規模なリモート サイトの支店のインターフェイス回線速度はかなり遅くなります（たとえば、64 Kbps）。データが中央サイトから低速リモート サイトにフル レートで送信される場合、リモート サイトのインターフェイスが輻輳し、その結果、音声品質の低下の原因となるパケットのドロップが発生する可能性があります。

2. 中央サイトとリモート サイト間のリンクのオーバーサブスクリプション

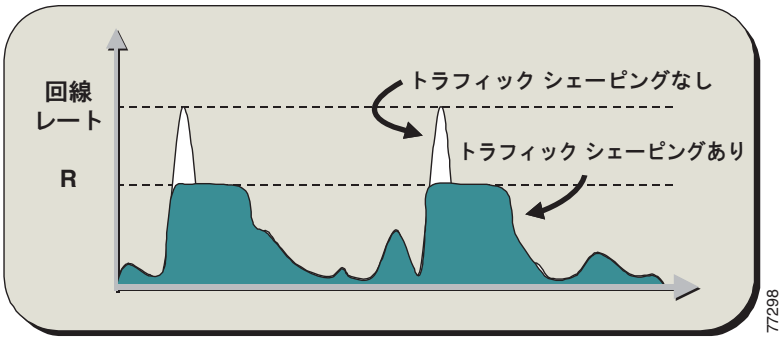
   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

3. 認定情報レート（CIR）を超えたバースト

   もう 1 つの一般的な設定は、CIR を超えたトラフィック バーストを許可することです。CIR は、サービス プロバイダーが、損失なく、遅延の少ないネットワークを介して転送することを保証したレートです。たとえば、T1 インターフェイスを備えたリモート サイトでは、CIR が 64 Kbps に過ぎない場合があります。64 Kbps 超に相当するトラフィックが WAN を介して送信される場合、プロバイダーは、追加トラフィックに「廃棄適性」のマークを付けます。プロバイダーのネットワークで輻輳が起きた場合、このトラフィックはトラフィック分類に関係なくドロップされるため、音声品質に悪影響を与える可能性があります。

トラフィック シェーピングは、インターフェイスから送出されるトラフィックを、回線レート未満のレートに制限して、WAN の両端で輻輳が起きないようにし、こうした問題を解決します。図 3-14 は、このメカニズムの一般的な例を説明しています。ここで、R は、トラフィック シェーピングが適用される場合のレートです。

図 3-14　　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

VATS は、オプションのダイナミック メカニズムで、WAN を介して音声が送信されているかどうかに基づいてさまざまなレートで、フレームリレー Permanent Virtual Circuits（PVC; 相手先固定接続）上のトラフィックをシェーピングします。LLQ 音声プライオリティ キューにトラフィックが存在する場合や、リンク上で H.323 シグナリングが検出された場合は、VATS が連動します。一般に、フレームリレーは、常時、PVC の保証帯域幅または CIR に合せて、トラフィックをシェーピングします。ただし、この PVC では、一般に、CIR を超えた（回線速度までの）バーストが許可されているため、トラフィック シェーピングによって、WAN に存在する可能性のある追加の帯域幅をトラフィックが継続的に使用するようになります。フレームリレー PVC 上で VATS が有効の場合、リンク上に音声トラ

フィックが存在するときは、WAN インターフェイスは CIR でトラフィックを送信できます。ただし、音声が存在しないときは、音声以外のトラフィックが回線速度までバーストして、WAN に存在する可能性がある追加の帯域幅を利用できます。

VATS を Voice-Adaptive Fragmentation（VAF）と組み合せて使用する場合（「リンク フラグメンテーション/インターリーブ（LFI）」（P.3-44）を参照）、インターフェイス上で音声アクティビティが検出されたときは、音声以外のトラフィックはすべてフラグメント化され、トラフィックはすべて WAN リンクの CIR に合せてシェーピングされます。

VAF の場合と同様、VATS をアクティブにすると音声以外のトラフィックに悪影響を与える可能性があるため、VATS を有効にするときは注意してください。リンク上に音声が存在すると、データ アプリケーションのスループットは低下します。これは、アプリケーションが CIR をはるかに下回る速度まで抑制されるためです。この動作の結果、音声以外のトラフィックで、パケット ドロップや遅延が発生する場合があります。さらに、音声トラフィックが検出されなくなってから、トラフィックが回線速度までバーストするまでの間に、非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。VATS を使用する場合は、エンド ユーザの期待を設定し、WAN を介した音声コールが存在するとデータ アプリケーションの速度が定期的に低下することをエンド ユーザに知らせることが重要です。VATS は、Cisco IOS Release 12.2(15)T 以降で使用できます。

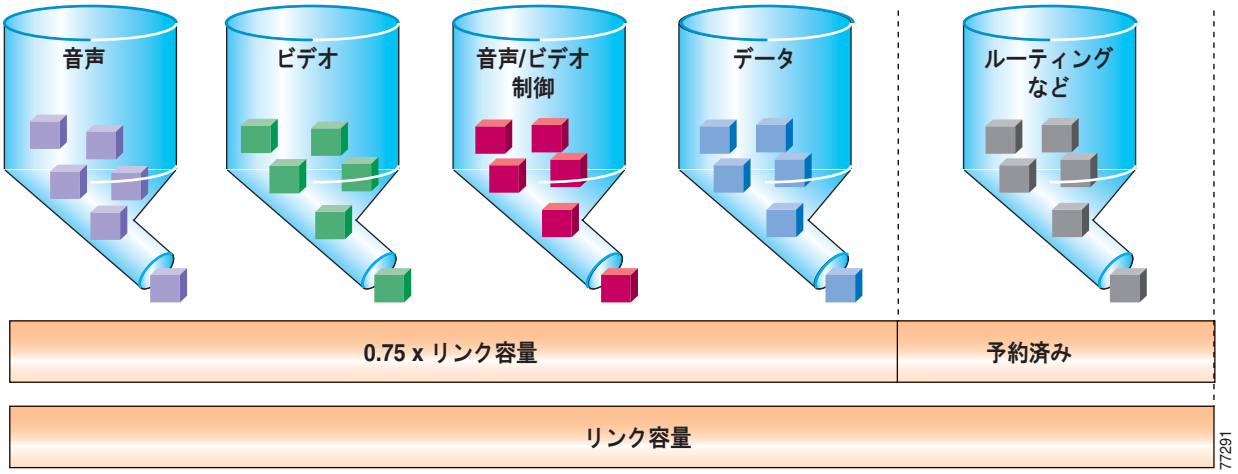
Voice-Adaptive Traffic Shaping 機能とフラグメンテーション機能の詳細、およびそれらの設定方法については、次の Web サイトで入手可能なドキュメントを参照してください。

http://www.cisco.com/en/US/docs/ios/12_2t/12_2t15/feature/guide/ft_vats.html

帯域幅のプロビジョニング

成功する IP ネットワークを設計する主要部分は、ネットワーク帯域幅の適切なプロビジョニングです。主要なアプリケーション（たとえば、音声、映像、およびデータ）ごとの帯域幅必要量を加算すると、必要な帯域幅を計算できます。この合計値は、任意のリンクの最小帯域幅必要量を表します。この値は、そのリンクに使用可能な合計帯域幅の約 75% 以下でなければなりません。この 75% ルールは、ルーティングやレイヤ 2 キープアライブなどのオーバーヘッド トラフィックに、いくらかの帯域幅が必要であることを前提としています。図 3-15 は、こうした帯域幅のプロビジョニング プロセスを示しています。

図 3-15　リンクの帯域幅プロビジョニング



使用可能な合計帯域幅の 75% 以下をデータ、音声、およびビデオに使用することに加え、すべての LLQ プライオリティ キューに対して設定する合計帯域幅は、通常、リンクの合計帯域幅の 33% 以下にする必要があります。使用可能な帯域幅の 33% 超をプライオリティ キュー用にプロビジョニングすると、いくつかの理由で問題となる場合があります。まず、帯域幅の 33% 超を音声用にプロビジョニングすると、CPU 使用率が高くなる場合があります。各音声は毎秒 50 パケットを送信する（20 ms サンプルを使用する）ので、プライオリティ キューに多数のコールをプロビジョニングすると、パケット レートが高いため、CPU レベルが高くなる場合があります。また、プライオリティ キューに複数のタイプのトラフィックをプロビジョニングすると（たとえば、音声とビデオ）、プライオリティ キューは実質的に First-in, First-out（FIFO; ファーストイン ファーストアウト）キューとなるため、QoS を有効にする意味がなくなります。予約するプライオリティ帯域幅の割合を大きくすると、より多くのリンク帯域幅が FIFO となるため、実質的に QoS の効果がなくなります。最後に、使用可能な帯域幅の 33% 超を割り当てると、プロビジョニングされたすべてのデータ キューが実質的に不足状態になる場合があります。単一のコールでもリンク帯域幅の 33% 超を要求する可能性があるため、非常に低速のリンク（192 Kbps 未満）では、リンク帯域幅の 33% 以下をプライオリティ キュー用にプロビジョニングするという推奨事項は、明らかに非現実的となる場合があります。このような場合や、この推奨事項に従うと特定のビジネス ニーズを満たせない場合は、必要に応じて 33% ルールを超えてもかまいません。

トラフィックの観点から見ると、IP テレフォニー コールは次の 2 つの部分から構成されています。

- 実際の音声サンプルが入っている Real-Time Transport Protocol（RTP）パケットから構成される、音声およびビデオ ベアラ ストリーム。
- コールに関係するエンドポイントに応じて、複数のプロトコルのいずれか（たとえば、H.323、MGCP、SCCP、または (J)TAPI）に属するパケットから構成される、呼制御シグナリング。たとえば、呼制御機能は、コールのセットアップ、保持、終了、または転送に使用される機能です。

帯域幅のプロビジョニングには、ベアラ トラフィックだけでなく、呼制御トラフィックも含まれていなければなりません。実際に、マルチサイト WAN 配置では、呼制御トラフィック（およびベアラ ストリーム）は、WAN を通過する必要があるので、そのトラフィックに十分な帯域幅を割り当てないと、悪影響を与える可能性があります。

次の 3 つの項では、トラフィックのタイプについて、帯域幅プロビジョニングの推奨事項を説明します。

- すべてのマルチサイト WAN 配置における音声およびビデオ ベアラ トラフィック（「ベアラ トラフィック用のプロビジョニング」（P.3-48）を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「集中型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-52）を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置における呼制御トラフィック（「分散型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-56）を参照）

ベアラ トラフィック用のプロビジョニング

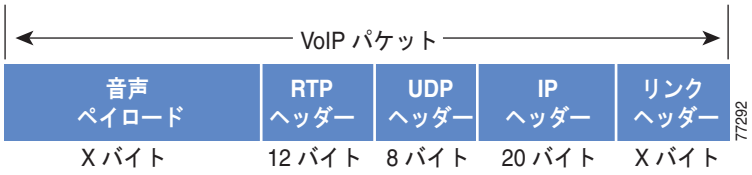
この項では、次のトラフィック タイプの帯域幅プロビジョニングについて説明します。

- 「音声ベアラ トラフィック」（P.3-49）
- 「ビデオ ベアラ トラフィック」（P.3-51）

音声ベアラ トラフィック

図 3-16 に示されているように、VoIP（Voice-over-IP）パケットは、音声ペイロード、IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、Real-Time Transport Protocol（RTP）ヘッダー、およびレイヤ 2 リンク ヘッダーから構成されています。Secure Real-Time Transport Protocol（SRTP）暗号化を使用すると、各パケットの音声ペイロードは 4 バイト増加します。リンク ヘッダーの大きさは、使用されるレイヤ 2 メディアによって異なります。

図 3-16　一般的な VoIP パケット



VoIP ストリームによって消費される帯域幅を計算するには、次に示すように、パケットのペイロードとすべてのヘッダーを加算し（ビット単位）、1 秒あたりのパケット レート（デフォルトでは、毎秒 50 パケット）を掛けます。

レイヤ 2 帯域幅（kbps）= [（1 秒あたりのパケット数）*（音声ペイロード *X* バイト + RTP/UDP/IP ヘッダー 40 バイト + レイヤ 2 オーバーヘッド *Y* バイト）* 8 ビット] / 1000

レイヤ 3 帯域幅（kbps）= [（1 秒あたりのパケット数）*（音声ペイロード *X* バイト + RTP/UDP/IP ヘッダー 40 バイト）* 8 ビット] / 1000

1 秒あたりのパケット数 = [1/（サンプリング レート（msec））] * 1000

音声ペイロード（バイト）= [（コーデック ビット ビット レート（kbps））*（サンプリング レート msec）] / 8

表 3-9 は、VoIP フローあたりのレイヤ 3 帯域幅を詳しく記述しています。表 3-9 は、音声ペイロードと IP ヘッダーだけによって消費される帯域幅を示しています。ここでは、パケット レートとして、デフォルトのパケット レートである 50 パケット / 秒（pps）と、暗号化されていないペイロードと暗号化されたペイロードの両方のレートである 33.3 pps を使用しています。表 3-9 には、レイヤ 2 ヘッダーのオーバーヘッドは含まれていません。また、RTP ヘッダー圧縮（cRTP）などの可能な圧縮方式を考慮していません。Unified CM Administration の Service Parameters メニューを使用すると、コーデック サンプリング レートを調整できます。

表 3-9　音声ペイロードと IP ヘッダーだけの帯域幅使用量

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
G.711 および G.722-64k	20 ms	160	50.0	80.0 kbps
G.711 および G.722-64k（SRTP）	20 ms	164	50.0	81.6 kbps
G.711 および G.722-64k	30 ms	240	33.3	74.7 kbps
G.711 および G.722-64k（SRTP）	30 ms	244	33.3	75.8 kbps
iLBC	20 ms	38	50.0	31.2 kbps
iLBC（SRTP）	20 ms	42	50.0	32.8 kbps
iLBC	30 ms	50	33.3	24.0 kbps

表 3-9　音声ペイロードと IP ヘッダーだけの帯域幅使用量（続き）

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒あたりのパケット数	1 会話あたりの帯域幅
iLBC（SRTP）	30 ms	54	33.3	25.1 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A（SRTP）	20 ms	24	50.0	25.6 kbps
G.729A	30 ms	30	33.3	18.7 kbps
G.729A（SRTP）	30 ms	34	33.3	19.8 kbps

より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-10 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

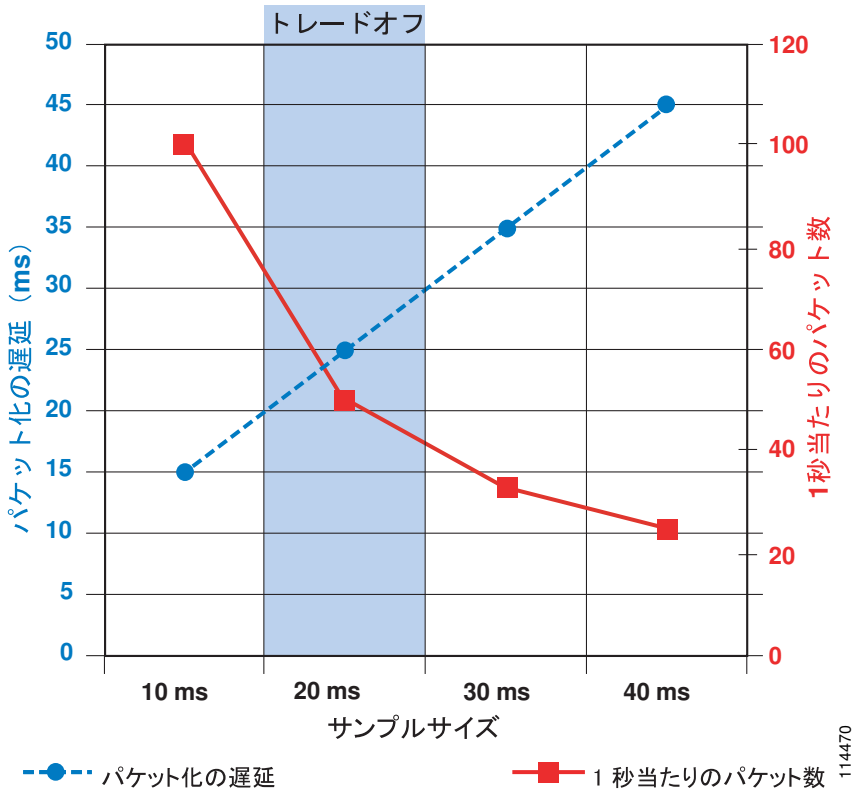
表 3-10　レイヤ 2 ヘッダーが含まれた帯域幅使用量

	ヘッダー タイプとサイズ						
コーデック	イーサネット 14 バイト	PPP 6 バイト	ATM 53 バイトのセルと 48 バイトのペイロード	フレーム リレー 4 バイト	MLPPP 10 バイト	MPLS 4 バイト	WLAN 24 バイト
G.711 および G.722-64k（50.0 pps）	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711 および G.722-64k（SRTP）（50.0 pps）	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	該当なし
G.711 および G.722-64k（33.3 pps）	78.4 kbps	76.3 kbps	84.8 kbps	75.7 kbps	77.3 kbps	75.7 kbps	81.1 kbps
G.711 および G.722-64k（SRTP）（33.3 pps）	79.5 kbps	77.4 kbps	84.8 kbps	76.8 kbps	78.4 kbps	76.8 kbps	該当なし
iLBC（50.0 pps）	36.8 kbps	33.6 kbps	42.4 kbps	32.8 kbps	35.2 kbps	32.8 kbps	40.8 kbps
iLBC（SRTP）（50.0 pps）	38.4 kbps	35.2 kbps	42.4 kbps	34.4 kbps	36.8 kbps	34.4 kbps	42.4 kbps
iLBC（33.3 pps）	27.7 kbps	25.6 kbps	28.3 kbps	25.0 kbps	26.6 kbps	25.0 kbps	30.4 kbps
iLBC（SRTP）（33.3 pps）	28.8 kbps	26.6 kbps	42.4 kbps	26.1 kbps	27.7 kbps	26.1 kbps	31.5 kbps
G.729A（50.0 pps）	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A（SRTP）（50.0 pps）	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	35.2 kbps
G.729A（33.3 pps）	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.8 kbps	25.1 kbps
G729A（SRTP）（33.3 pps）	23.5 kbps	21.4 kbps	28.3 kbps	20.8 kbps	22.4 kbps	20.8 kbps	26.2 kbps

30 ms を超えるサンプリング レートを設定することは可能ですが、これを行うと、通常、音声品質が非常に低下します。図 3-17 に示されているように、サンプリング サイズが増加すると、1 秒あたりのパケット数が減少するため、デバイスの CPU に与える影響は小さくなります。同様に、サンプル サイズ

が増加すると、1 パケットあたりのペイロードが大きくなるため、IP ヘッダーのオーバーヘッドが低下します。ただし、サンプル サイズが増加すると、パケット化の遅延も増加するため、音声トラフィックのエンドツーエンドの遅延が増加します。サンプル サイズを設定する場合は、パケット化の遅延と 1 秒あたりのパケット数とのトレードオフを考慮する必要があります。このトレードオフが 20 ms で最適化されている場合、30 ms のサンプル サイズでも、1 秒あたりのパケット数に対する遅延の比率は妥当なものになります。しかし、40 ms のサンプル サイズでは、パケット化の遅延が大きくなりすぎます。

図 3-17　音声のサンプル サイズ：1 秒あたりのパケット数とパケット化の遅延との比較



ビデオ ベアラ トラフィック

オーディオの場合、各パケットのサンプル サイズを指定して、パケットあたりのオーバーヘッドの比率を計算することは比較的簡単です。これに対して、ビデオの場合は、ビデオで表されるモーションの量（最後のフレームから変更されるピクセル数）によってペイロードが変わるため、正確なオーバーヘッドの比率を計算することは、ほとんど不可能です。

ビデオの正確なオーバーヘッド率を計算できないという問題を解決するために、パケットが通過するレイヤ 2 メディアのタイプにかかわらず、コール速度に 20% を加算することを推奨します。追加の 20% は、イーサネット、ATM、フレーム リレー、PPP、HDLC、およびその他の転送プロトコル間の差を吸収するための余裕となり、ビデオ トラフィックのバースト性に対するクッションにもなります。

エンドポイントで要求されるコール速度（128 kbps、256 kbps など）はコールの最大バースト速度を表し、クッションとして追加分が含まれていることに注意してください。コールの平均速度は、通常、この値を大幅に下回ります。

呼制御トラフィック用のプロビジョニング

Unified Communications エンドポイントが WAN によって呼制御アプリケーションと分けられている場合、または相互接続された 2 つの Unified Communications システムが WAN によって分けられている場合、これらのエンドポイント間やシステム間の呼制御およびシグナリング トラフィック用にプロビジョニングする必要がある帯域幅の量について、考慮が必要です。ここでは、集中型または分散型のコール処理モデルが配置されている場合の、コール シグナリング トラフィック用の WAN 帯域幅プロビジョニングについて説明します。Unified Communications の集中型および分散型のコール処理配置モデルについては、「Unified Communications の配置モデル」（P.5-1）を参照してください。

集中型コール処理を使用した呼制御トラフィック用のプロビジョニング

集中型コール処理配置では、Unified CM クラスタとアプリケーション（たとえば、ボイスメール）は、中央サイトに置かれ、複数のリモート サイトが IP WAN を介して接続されます。リモート サイトでは、コール処理に中央の Unified CM を使用します。

この配置モデルには、次の考慮事項が適用されます。

- リモート サイトの支店の電話機がコールを発信するたびに、制御トラフィックは、支店内へのコールであっても、IP WAN を通過して、中央サイトの Unified CM に到達します。
- この配置モデルで IP WAN を通過するシグナリング プロトコルは、SCCP（暗号化と非暗号化）、SIP（暗号化と非暗号化）、H.323、MGCP、および CTI-QBE です。すべての制御トラフィックは、中央サイトの Unified CM と、リモート サイトの支店のエンドポイントまたはゲートウェイとの間で交換されます。
- クラスタで RSVP が配置されている場合、中央サイトの Unified CM クラスタとリモート サイトの Cisco RSVP Agent の間の制御トラフィックは、SCCP プロトコルを使用します。

その結果、支店のルータと中央サイトの WAN アグリゲーション ルータとの間で WAN を通過する制御トラフィック用の帯域幅を提供する必要があります。

このシナリオで WAN を通過する制御トラフィックは、次の 2 つのカテゴリに分割できます。

- 休止トラフィック。このトラフィックは、コールのアクティビティに関係なく、支店のエンドポイント（電話機、ゲートウェイ、および Cisco RSVP Agent）と Unified CM との間で定期的に交換されるキープアライブ メッセージから構成されます。このトラフィックはエンドポイント数の関数になります。
- コール関連トラフィック。このトラフィックは、コールのセットアップ、終了、転送などが必要なときに、支店のエンドポイントと、中央サイトの Unified CM との間で交換されるシグナリング メッセージから構成されます。このトラフィックは、エンドポイント数とエンドポイントに関連付けられたコール量の関数になります。

生成される呼制御トラフィックの見積もりをするには、支店の各 IP Phone が発信する、1 時間あたりの平均コール数について推測する必要があります。わかりやすくするために、この項での計算では、電話機あたりの毎時平均コール数を 10 と想定します。

（注）　この平均数が、特定の配置のニーズを満たさない場合、「拡張公式」（P.3-54）に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

上記を前提とし、最初はシグナリングの暗号化が設定されていないリモート サイトの支店の場合を考慮すると、呼制御トラフィックに必要な推奨帯域幅は、次の公式で得られます。

公式 1A：SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= 265 *（支店内の IP Phone とゲートウェイの数）

公式 1B：SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= 538 *（支店内の IP Phone とゲートウェイの数）

サイトに SCCP エンドポイントと SIP エンドポイントが混在している場合は、使用する電話機のタイプごとに上記の 2 つの公式を個別に使用し、結果を合計します。

公式 1 やこの項に記載されている他のすべての公式には、25% 過剰プロビジョニング係数が含まれています。制御トラフィックにはバースト性があり、高いアクティビティのピークの後に、アクティビティの低い期間が続きます。このため、制御トラフィック キューに必要な最小の帯域幅だけを割り当てると、アクティビティの高い期間に、バッファリング遅延や、場合によってはパケット ドロップなど、望ましくない影響が現れることがあります。Cisco IOS の Class-Based Weighted Fair Queuing（CBWFQ; クラスベース WFQ）キューに対するデフォルトのキュー項目数は、64 パケットです。このキューに割り当てられた帯域幅によって、そのサービス レートが決まります。設定されている帯域幅が、このタイプのトラフィックによって消費される平均帯域幅になっていることを前提とすると、明らかに、アクティビティが高い期間ではすべての着信パケットをキューから「排出」するのに十分なサービス レートとならないため、パケットはバッファに入れられます。64 パケットの制限に到達した場合、それ以降のパケットはすべて、ベストエフォート型のキューに割り当てられるか、またはドロップされます。したがって、トラフィック パターンの変動を吸収し、一時的なバッファ オーバーランのリスクを最小限に抑えるために、この 25% の過剰プロビジョニング係数を導入することを推奨します。この導入は、キューのサービス レートを増やすことに相当します。

暗号化を設定すると、Unified CM とエンドポイント間で交換されるシグナリング パケットのサイズが増加するため、推奨帯域幅が影響を受けます。次の公式では、シグナリングの暗号化の影響を考慮に入れています。

公式 2A：SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）= 415 *（支店内の IP Phone とゲートウェイの数）

公式 2B：SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）= 619 *（支店内の IP Phone とゲートウェイの数）

Cisco IOS ルータ上のキューに割り当てることができる最小帯域幅が 8 Kbps であるという事実を考慮すると、支店のさまざまな規模に対する最小帯域幅と推奨帯域幅の値を、表 3-11 のようにまとめることができます。

表 3-11　呼制御トラフィック用の推奨レイヤ 3 帯域幅（シグナリングの暗号化の有無別）

支店の規模（IP Phone とゲートウェイの数）	SCCP 制御トラフィック用の推奨帯域幅（暗号化なし）	SCCP 制御トラフィック用の推奨帯域幅（暗号化あり）	SIP 制御トラフィック用の推奨帯域幅（暗号化なし）	SIP 制御トラフィック用の推奨帯域幅（暗号化あり）
1 ～ 10	8 kbps	8 kbps	8 kbps	8 kbps
20	8 kbps	9 kbps	11 kbps	12 kbps
30	8 kbps	13 kbps	16 kbps	19 kbps
40	11 kbps	17 kbps	22 kbps	25 kbps
50	14 kbps	21 kbps	27 kbps	31 kbps
100	27 kbps	42 kbps	54 kbps	62 kbps
150	40 kbps	62 kbps	81 kbps	93 kbps

（注）　表 3-11 では、電話機あたりの毎時平均コール数を 10 と想定し、RSVP 制御トラフィックを含みません。この表の値に追加する RSVP 関連の帯域幅を判断するには、「RSVP を使用するコールに関する考慮事項」（P.11-38）を参照してください。

（注）　サイト間コールに RSVP ベースのロケーション ポリシーを使用する場合は、表 3-11 の値を増やし、Cisco RSVP Agent の制御トラフィックの分を補正する必要があります。たとえば、コールの 10% が WAN を経由する場合、表 3-11 の値に 1.1 を掛けます。

拡張公式

この項で示されている上記の公式は、電話機 1 台あたりの平均コール レートを毎時 10 コールと想定しています。しかし、コール パターンが大きく異なる場合（たとえば、支店にコール センター エージェントが配置されている場合）、この想定が、実際の配置に該当しない場合があります。こうした場合の呼制御帯域幅必要量を計算するには、次の公式を使用してください。これらの公式には、電話機 1 台あたりの毎時平均コール数を表す追加変数（CH）が含まれています。

公式 3A：支店の SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= (53 + 21 * CH) *（支店内の IP Phone とゲートウェイの数）

公式 3B：支店の SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化なし

帯域幅（bps）= (138 + 40 * CH) *（支店内の IP Phone とゲートウェイの数）

公式 4A：支店の SCCP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）=（73.5 + 33.9 * CH）*（支店内の IP Phone とゲートウェイの数）

公式 4B：支店の SIP 制御トラフィックに必要な推奨帯域幅、シグナリングの暗号化あり

シグナリングの暗号化を使用する場合の帯域幅（bps）=（159 + 46 * CH）*（支店内の IP Phone とゲートウェイの数）

（注）　公式 3A と 4A は、デフォルトの SCCP キープアライブ間隔である 30 秒に基づいています。公式 3B と 4B は、デフォルトの SIP キープアライブ間隔である 120 秒に基づいています。

シェアド ライン アピアランスに関する考慮事項

シェアド ライン アピアランスに発信されるコール、またはブロードキャスト ディストリビューション アルゴリズムを使用する回線グループに送信されるコールは、システムが消費する帯域幅に 2 つのネット効果を与えます。

- 設定された回線のすべての電話機が同時に鳴るため、システムの負荷は回線の毎時コール数（CH）よりも大幅に高い CH 値に対応します。その結果、対応する帯域幅の使用量が増加します。WAN 接続されたシェアド ライン機能を配置する場合は、ネットワーク インフラストラクチャの帯域幅プロビジョニングを調整する必要があります。公式 3 および 4 で使用する CH 値を、次の公式に従って増やす必要があります。

  CHS = CHL *（ライン アピアランス数）/（回線数）

  CHS は公式 3 および 4 で使用する時間あたりのシェアド ライン コール数で、CHL は回線の時間あたり平均コール数です。たとえば、5 回線で設定されたサイトで、時間あたりの平均コール数が 6 で、そのうち 2 回線が 4 台の電話機で共有されている場合、次のようになります。

  回線数 = 5

ライン アピアランス数 = (2 回線が 4 台の電話機に出現し、3 回線が 1 台ずつの電話機に出現) = (2 * 4) + 3 = 11 回線が出現

CHL = 6

CHS = 6 * (11 / 5) = 13.2

- 呼び出す各電話機が個別のシグナリング制御ストリームを必要とするため、Unified CM から同じ支店に送信されるパケット量は、呼び出す電話機の数に比例して増加します。Unified CM は 100 Mbps インターフェイスでネットワークに接続されるため、大量のパケットをすぐに生成できますが、キューイング メカニズムがシグナリング トラフィックを処理するまで、このパケットはバッファに入れる必要があります。処理速度は、通常、100 Mbps よりも 2 桁小さい WAN インターフェイスの実効情報転送速度によって制限されます。

  このトラフィックによって、中央サイトの WAN ルータのキュー項目数があふれることがあります。デフォルトでは、Cisco IOS の各トラフィック クラスで使用できるキュー項目数は 64 です。WAN インターフェイスのキューに入れられる前にパケットがドロップされることを防ぐには、シグナリング キューの項目数が、各シェアド ライン型の電話機について少なくとも 1 つの完全なシェアド ライン イベントで発生するすべてのパケットを保持できるサイズであることを確認してください。ドロップされたパケットを再送信することでシステムからの応答時間が損なわれるような競合状態を防ぐには、ドロップの防止が不可欠です。

  そのため、シェアド ライン型の電話機が動作するために必要なパケット量は、次のようになります。

  - SCCP プロトコル：シェアド ライン型の電話機ごとに 13 パケット
  - SIP プロトコル：シェアド ライン型の電話機ごとに 11 パケット

  たとえば、SCCP と、同じ回線を共有する 6 台の電話機を使用する場合、トラフィックのシグナリング クラス用のキュー項目数は 78 以上に調整する必要があります。表 3-12 は、支店サイトでのシェアド ライン アピアランスの量に基づいた推奨されるキュー項目数を示しています。

表 3-12　支店サイトごとの推奨されるキュー項目数

シェアド ライン アピアランスの数	キュー項目数（パケット数）	
	SCCP	SIP
5	65	55
10	130	110
15	195	165
20	260	220
25	325	275

フレーム リレーなどのレイヤ 2 WAN テクノロジーを使用する場合、この調整は、シェアド ライン型の電話機がある支店に対応する回線で行う必要があります。

MPLS などのレイヤ 3 WAN テクノロジーを使用する場合は、単一のシグナリング キューで複数の支店を処理できます。この場合、処理するすべての支店の合計に対して、調整を行う必要があります。

分散型コール処理を使用した呼制御トラフィック用のプロビジョニング

分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには、Unified CM クラスタが含まれ、単一サイト モデルか、集中型コール処理モデルのどちらかを設定できます。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

この配置モデルには、次の考慮事項が適用されます。

- WAN を介したコールの発信に使用されるシグナリング プロトコルは、H.323 または SIP です。
- 制御トラフィックは、各サイトの Cisco IOS ゲートキーパーと Unified CM クラスタとの間、および Unified CM クラスタ相互間で交換されます。

したがって、制御トラフィック用の帯域幅は、Unified CM 相互間の WAN リンクだけでなく、各 Unified CM とゲートキーパー間の WAN リンクでもプロビジョニングされなければなりません。トポロジはハブアンドスポークに限定され、一般にゲートキーパーはハブに置かれるので、各サイトを他のサイトに接続する WAN リンクは、通常、ゲートキーパーに接続するリンクと一致します。

WAN を通過する制御トラフィックは、次のカテゴリのいずれかに属します。

- 休止トラフィック。このトラフィックは、各 Unified CM とゲートキーパー間で定期的に交換される登録メッセージから構成されます。
- コール関連トラフィック。このトラフィックは、次の 2 つのタイプのトラフィックから構成されます。
  - コール アドミッション制御トラフィック。コールのセットアップ前とコールの終了後に、Unified CM とコール アドミッション制御デバイス（ゲートキーパー、Cisco RSVP Agent など）との間で交換されます。
  - メディア ストリームに関連付けられたシグナリング トラフィック。コールのセットアップ、終了、転送などが必要なときに、クラスタ間トランクで交換されます。

制御トラフィックの合計数は、任意の時間にセットアップし、終了するコール数によって異なるので、コール パターンとリンク使用状況について、何らかの想定をする必要があります。各スポーク サイトをハブに接続する WAN リンクは、通常、さまざまなタイプのトラフィック（たとえば、データ、音声、およびビデオ）を受け入れるように設定されます。従来型のテレフォニーから類推すると、WAN リンクの中で音声用に設定された部分を、複数の*仮想タイ ライン*と見なすことができます。

平均コール所要時間を 2 分、各仮想タイ ラインの利用率を 100% と想定すると、各タイ ラインの伝送量は毎時 30 コールであると推論できます。この前提により、呼制御トラフィック用の推奨帯域幅を仮想タイ ライン数の関数として表す、次の公式が得られます。

公式 6：仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅（bps）= 116 *（仮想タイ ライン数）

Cisco IOS ルータ上のキューに割り当て可能な最小帯域幅は、8 Kbps です。つまり 8 Kbps の最小キュー サイズは、*最大 70 の仮想タイ ライン*によって生成される呼制御トラフィックを受け入れることができると推定できます。これは、大部分の大企業での配置に十分な量です。

ワイヤレス LAN インフラストラクチャ

統合されたネットワークの wireless LAN（WLAN; ワイヤレス LAN）部分に Unified Communications を追加する場合は、ワイヤレス LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless IP Phone が導入されている場合、音声トラフィックは WLAN 上に移るため、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN インフラストラクチャの場合と同様、WLAN に音声を追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質を保証するために、QoS を理解してワイヤレス ネットワーク上に配置する必要もあります。次の項では、これらの要件について説明します。

- 「WLAN の設計と設定」（P.3-57）
- 「WLAN の QoS」（P.3-61）

Voice over Wireless LAN の詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』の最新版を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html

WLAN の設計と設定

WLAN を適切に設計する場合は、最初に、既存の有線ネットワークが、可用性の高い、耐障害性のある冗長な方式で配置されていることを確認する必要があります。次に、ワイヤレス テクノロジーについて理解する必要があります。最後に、ワイヤレス Access Point（AP; アクセス ポイント）とワイヤレス テレフォニー エンドポイントを効果的な方法で設定および配置すると、柔軟性のある、セキュアで冗長な、拡張性の高いネットワークを構築できます。

次の項では、WLAN インフラストラクチャのレイヤとネットワーク サービスについて説明します。

- 「ワイヤレス インフラストラクチャに関する考慮事項」（P.3-57）
- 「ワイヤレス AP の設定と設計」（P.3-60）

ワイヤレス インフラストラクチャに関する考慮事項

次の項では、WLAN インフラストラクチャを設計するためのガイドラインとベスト プラクティスについて説明します。

- 「VLAN」（P.3-57）
- 「ローミング」（P.3-58）
- 「ワイヤレス チャネル」（P.3-58）
- 「無線の干渉」（P.3-59）
- 「WLAN 上のマルチキャスト」（P.3-60）

VLAN

有線 LAN インフラストラクチャの場合と同様、ワイヤレス LAN に音声を配置する場合は、アクセス レイヤにある 2 つ以上の VLAN を有効にする必要があります。ワイヤレス LAN 環境のアクセス レイヤには、アクセス ポイント（AP）と最初のホップのアクセス スイッチが含まれます。AP とアクセス スイッチ上では、データ トラフィック用のネイティブ VLAN と、音声トラフィック用の Voice VLAN（Cisco IOS の場合）または Auxiliary VLAN（CatOS の場合）を設定する必要があります。この Voice / Auxiliary VLAN は、ネットワークにある他のすべての有線 Voice VLAN とは分離される必要があります。また、有線 LAN 上の音声エンドポイントの場合と同様、ワイヤレス音声エンドポイント

は、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定される必要があります。ワイヤレス インフラストラクチャを配置する場合は、WLAN AP の管理用に独立した管理 VLAN を設定することも推奨します。この管理 VLAN には WLAN アピアランスを設定しないでください。つまり、関連付けられた Service Set Identifier（SSID）を設定することも、WLAN から直接アクセスできるように設定することもしないでください。

ローミング

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。WLAN ネットワーク インフラストラクチャが自律分散型 AP で構成されている場合、Cisco LAN コントローラによって、Cisco Unified Wireless IP Phone は、IP アドレスを保持し、アクティブ コールを維持しながらレイヤ 3 でローミングできます。シームレスなレイヤ 3 ローミングが行われるのは、クライアントが同じモビリティ グループ内でローミングする場合だけです。Cisco LAN コントローラおよびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/wireless/index.html

Lightweight アクセス ポイント インフラストラクチャにわたるクライアントのシームレスなレイヤ 3 ローミングは、動的インターフェイス トンネリングを使用する WLAN コントローラによって実現されます。WLAN コントローラと VLAN にわたってローミングする Cisco Unified Wireless IP Phone は、同じ SSID を使用する場合、IP アドレスを保持できるので、アクティブ コールを維持できます。

（注）　デュアルバンド WLAN（2.4 GHz と 5 GHz 帯域を装備）では、クライアントが両方の帯域をサポートする場合、同じ SSID によって 802.11b/g と 802.11a 間でローミングできます。ただし、これにより、音声パスにギャップが発生する場合があります。これらのギャップを回避するには、音声帯域を 1 つだけ使用します。

ワイヤレス チャネル

ワイヤレス エンドポイントと AP は、特定のチャネル上で無線を介して通信します。1 つのチャネル上で通信する場合、ワイヤレス エンドポイントは、一般に、他の非オーバーラップ チャネル上で発生するトラフィックと通信を認識しません。

2.4 GHz 802.11b および 802.11g 用のチャネル設定を最適化するには、設定するチャネルの間に 5 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。許可されるチャネルが 1 ～ 11 の北米では、チャネル 1、6、および 11 が、AP とワイヤレス エンドポイント デバイスに使用可能な 3 つの非オーバーラップ チャネルです。それに対して、許可されるチャネルが 1 ～ 13 の欧州では、5 チャネルの間隔がある組み合せは複数可能です。日本も許可されるチャネルが 1 ～ 14 なので、5 チャネルの間隔がある組み合せは複数可能です。

5 GHz 802.11a 用のチャネル設定を最適化するには、1 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。北米では、次の 20 のオーバーラップのないチャネルを使用できます。36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、および 161。欧州では、同じオーバーラップのないチャネルを使用できます。ただし、多くの国はチャネル 40 の使用をサポートしていないので、19 のオーバーラップのないチャネルだけ使用できます。日本では、次の 8 つのオーバーラップのないチャネルだけがサポートされます。36、40、44、48、52、56、60、および 64。より大きなオーバーラップのないチャネルのセットにより、802.11a では、より高密度に配置された WLAN に対応できます。

一部のチャネルでは、レーダー（軍事、衛星、および気象）による干渉を防止するために、802.11a 帯域が Dynamic Frequency Selection（DFS; 動的周波数選択）および Transmit Power Control（TPC; 伝送パワー コントロール）をサポートする必要があることに注意してください。規制により、チャネル 52 ～ 64、100 ～ 116、および 132 ～ 140 が DFS および TPC をサポートする必要があります。TPC

は、これらのチャネル上の伝送が干渉を引き起こすほど強力にならないように制御します。DFC は、チャネルのレーダー パルスをモニタし、レーダー パルスを検出した場合、DFC はチャネル上の伝送を停止して、新しいチャネルに切り替えます。

AP カバレッジは、同じチャネルで設定された AP 間でオーバーラップが発生しない（または最小になる）ように、配置する必要があります。同じチャネルのオーバーラップは、通常、19 dBm の間隔で発生します。ただし、オーバーラップのないチャネルで適切な AP 配置およびカバレッジを行うには、最低限 20% のオーバーラップが必要です。このオーバーラップ量であれば、ワイヤレス エンドポイントが AP カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 20% 未満の場合、ローミングに時間がかかり、音質が悪くなることがあります。

高層オフィスビルや病院など、多階の建物にワイヤレス デバイスを配置する場合は、ワイヤレス AP とチャネル カバレッジのプランニングに 3 つめの次元が加わります。802.11 の 2.4 GHz と 5.0 GHz の波形は、いずれもフロア、天井、および壁を通過できます。このため、同一フロア上のオーバーラップ セルまたはチャネルを考慮するだけでなく、隣接フロア間のチャネル オーバーラップを考慮する必要もあります。3 チャネルだけで適切なオーバーラップを実現するには、慎重に 3 次元の計画を立てる必要があります。

（注）　ワイヤレス ネットワークを正しく動作させるには、ワイヤレス インフラストラクチャ内で AP の配置とチャネルの設定を慎重に行う必要があります。このため、運用環境にワイヤレス ネットワークを配置する前に、実地調査を徹底的に行う必要があります。調査では、非オーバーラップ チャネル設定、AP カバレッジ、および必要なデータ レートとトラフィック レートを確認し、不正 AP を排除し、考えられる干渉源の影響を特定して軽減する必要があります。

無線の干渉

ワイヤレス環境に干渉源があると、エンドポイントの接続性やチャネル カバレッジが大幅に制限される可能性があります。また、物体や障害物があると、信号反射やマルチパス歪みが発生する可能性があります。マルチパス歪みが発生するのは、トラフィックまたはシグナリングが送信元から宛先に向かって複数の方向に進む場合です。一般に、トラフィックの一部は、残りの部分よりも先に宛先に到着します。そのため、場合によっては、遅延やビット エラーが発生する可能性があります。マルチパス歪みの影響を軽減するには、干渉源や障害物を排除または削減し、ダイバーシティ アンテナを使用してトラフィックを一度に受信するアンテナが 1 つだけになるようにします。実地調査中に干渉源を特定し、可能であれば排除する必要があります。少なくとも、干渉の影響を軽減するために、AP を適切に配置し、ロケーションに適した指向性の、または無指向性のダイバーシティ無線アンテナを使用する必要があります。

考えられる干渉源には、次のものがあります。

- オーバーラップ チャネル上にある他の AP
- 他の 2.4 GHz アプライアンス（2.4 GHz コードレス電話機、個人用ワイヤレス ネットワーク デバイス、硫黄プラズマ照明システム、電子レンジ、不正 AP および 2.4 GHz 帯域のライセンスフリーで動作する他の WLAN 機器など）
- 金属機器、構造物、およびその他の金属面や反射面（金属 I ビーム、ファイリング キャビネット、機器ラック、ワイヤー メッシュまたは金属壁、防火扉と防火壁、コンクリート、および冷暖房のダクトなど）
- 高出力の電気装置（変圧器、強力電気モーター、冷蔵庫、エレベータ、およびエレベータ機器など）

Bluetooth 対応デバイスは、802.11 b および g デバイスと同じ 2.4 GHz 無線帯域を使用するので、Bluetooth および 802.11 b または g デバイスが相互に干渉し、その結果接続に関する問題が起きる可能性があります。Bluetooth デバイスは 802.11 b および g WLAN 音声デバイスと干渉，妨害を引き起こす潜在的な可能性があるので（その結果，音声品質の低下，登録解除，およびコールセットアップ遅延

を引き起こす）、可能な場合には、すべての WLAN 音声デバイスを、5 GHz 無線帯域を使用する 802.11a に配置することを推奨します。ワイヤレス電話機を 802.11a 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

WLAN 上のマルチキャスト

設計上、マルチキャストはユニキャストの確認応答レベルを備えていません。802.11 仕様に従って、アクセス ポイントは、次の Delivery Traffic Indicator Message（DTIM）周期に到達するまで、すべてのマルチキャスト パケットをバッファに入れる必要があります。DTIM 周期はビーコン周期の倍数です。ビーコン周期が 100 ms（通常のデフォルト）で DTIM 値が 2 の場合、アクセス ポイントは、バッファに入れられた単一のマルチキャスト パケットを転送する前に、最大 200 ms 待機する必要があります。ビーコン間の周期（DTIM 設定の積としての）は、バッテリ電源式デバイスによって、一時的に省電力モードに移行するために使用されます。この省電力モードは、デバイスがバッテリ電源を節約するのに役立ちます。

WLAN 上のマルチキャストは、管理者がバッテリの寿命要件に対するマルチキャスト トラフィックの品質要件を比較検討しなければならない二重の問題を提起します。第 1 に、マルチキャスト パケットの遅延は、特に、音声などのリアルタイム トラフィックをマルチキャストするアプリケーションに対して、マルチキャスト トラフィックの品質に悪影響を及ぼします。マルチキャスト トラフィックの遅延を制限するには、通常、DTIM 周期を 1 の値に設定して、マルチキャスト パケットがバッファに入れられる時間が、マルチキャスト トラフィックの配信で感知できる遅延を排除するために十分な低さになるようにする必要があります。ただし、DTIM 周期を 1 の値に設定することで、バッテリ電源式 WLAN デバイスが省電力モードに移行できる時間が短縮され、その結果、バッテリの寿命が短くなります。バッテリ電源を節約し、バッテリの寿命を長くするには、通常、DTIM 周期を 2 以上の値に設定する必要があります。

マルチキャスト アプリケーションまたはトラフィックが存在しない WLAN ネットワークでは、DTIM 周期を 2 以上の値に設定する必要があります。マルチキャスト アプリケーションが存在する WLAN ネットワークでは、可能な場合は常に、DTIM 周期を 2 の値に設定する必要があります。ただし、マルチキャスト トラフィックの品質が低下する場合、または許容できない遅延が発生する場合は、DTIM 値を 1 に下げる必要があります。DTIM 値が 1 に設定されている場合、管理者は、バッテリ駆動式デバイスのバッテリ寿命が大幅に短縮されることに注意する必要があります。

ワイヤレス ネットワーク上でマルチキャスト アプリケーションを有効にする前に、これらのアプリケーションをテストして、パフォーマンスや動作が許容できるレベルにあることを確認するよう推奨します。

マルチキャスト トラフィックを使用する場合の追加の考慮事項については、「メディア リソース」（P.17-1）を参照してください。

ワイヤレス AP の設定と設計

エンド ユーザに高品質の音声が提供されるように、ワイヤレス ネットワークが音声トラフィックを処理することを保証するには、AP を適切に選択、配置、および設定することが不可欠となります。

AP の選択

ワイヤレス音声用のアクセス ポイントの配置に関する推奨事項については、http://www.cisco.com/en/US/products/ps5678/Products_Sub_Category_Home.html にあるマニュアルを参照してください。

AP の配置

音声配置用に Cisco アクセス ポイント（AP）を使用するときは、いかなる場合も、15 ～ 25 を超えるデバイスを、単一の 802.11b または 802.11b/g AP に関連付けないことを推奨します。802.11a または 802.11a/g AP では、45 ～ 50 を超えるデバイスを、単一の AP に関連付けないことを推奨します。これらの数は、使用プロファイルおよび使用可能なデータ レートによって異なります。AP 上のデバイスの

数は、各デバイスがメディアにアクセスできる期間に影響します。デバイスの数が増加すると、トラフィックの競合も増加します。上記に指定された数を越えるデバイスを関連付けると、AP のパフォーマンスが低下し、関連付けられたデバイスの応答時間が遅くなる可能性があります。

限定された数のデバイスだけが単一の AP に関連付けられることを保証するメカニズムはありませんが、システム管理者は、定期的なサイト調査を行い、ユーザとデバイスのトラフィック パターンを分析することによって、デバイスと AP の割合を管理できます。追加のデバイスおよびユーザを特定の領域でネットワークに追加した場合は、追加のサイト調査を行い、ネットワークにアクセスする必要があるエンドポイントの数に対応するために追加の AP が必要かどうかを判断する必要があります。

AP の設定

ワイヤレス音声を配置する場合は、特定の AP 設定に関する次の要件に従います。

- Address Resolution Protocol（ARP; アドレス解決プロトコル）キャッシングを有効にする

  AP には ARP キャッシングが必要です。これは、ARP キャッシングを使用すると、AP がワイヤレス エンドポイント デバイスの ARP 要求に応答する際に、省電力モードまたはアイドル モードを終了するようエンドポイントに要求する必要がなくなるためです。この機能により、ワイヤレス エンドポイント デバイスのバッテリ寿命が長くなります。

- AP 上のダイナミック伝送パワー コントロール（DTPC）を有効にする

  これにより、AP 上の伝送パワーと音声エンドポイント上の伝送パワーの一致が保証されます。伝送パワーの一致により、片方向オーディオ トラフィックの可能性を排除できます。音声エンドポイントは、関連付けられた AP の Limit Client Power（mW）設定に基づいて伝送パワーを調整します。

- AP 上に設定されている各 VLAN に Service Set Identifier（SSID）を割り当てる

  SSID を使用すると、エンドポイントで、トラフィックの送受信に使用するワイヤレス VLAN を選択できます。このワイヤレス VLAN と SSID は、有線 VLAN にマッピングされます。音声エンドポイントでは、このマッピングにより、プライオリティ キューイング処理が行われること、および有線ネットワーク上の Voice VLAN にアクセスできることが保証されます。

- AP 上で **QoS Element for Wireless Phones** を有効にする

  この機能を使用すると、AP がビーコンで QoS Basic Service Set（QBSS）情報要素を提供することが保証されます。QBSS 要素は、AP でのチャネル使用率の推計を示します。また、QBSS 要素を使用することにより、Cisco ワイヤレス音声デバイスは、ローミングに関する決定を下し、負荷が高すぎる場合にコール試行を拒否できます。Cisco IOS Release 12.3(7)JA から、AP はビーコンで 802.11e Clear Channel Assessment（CCA）QBSS も提供するようになりました。CCA ベースの QBSS 値は、実際のチャネル使用率を反映したものになります。

- AP 上で 2 つの QoS ポリシーを設定して、VLAN とインターフェイスに割り当てる

  音声ポリシーとデータ ポリシーに各 VLAN のデフォルトの分類を設定することで、音声トラフィックがプライオリティ キューイング処理されることを保証します（詳細については、「インターフェイス キューイング」（P.3-62）を参照してください）。

WLAN の QoS

LAN および WAN 有線ネットワーク インフラストラクチャで高品質の音声を保証するために QoS が必要であるのと同様、ワイヤレス LAN インフラストラクチャでも QoS が必要です。データ トラフィックにはバースト性があり、音声などのリアルタイム トラフィックはパケット損失や遅延の影響を受けやすいため、ワイヤレス LAN バッファを管理し、無線の衝突を制限し、パケット損失、遅延、および遅延変動を最小限に抑えるには、QoS ツールが必要です。

ただし、ほとんどの有線ネットワークとは異なり、ワイヤレス ネットワークは共有メディアです。また、ワイヤレス エンドポイントにはトラフィックを送受信するための専用帯域幅がありません。ワイヤレス エンドポイントでは、トラフィックを 802.1p CoS、DSCP、および PHB でマークできますが、ワイヤレス ネットワークには共有性があるため、このエンドポイントでは、アドミッション制御とネットワーク アクセスが制限されます。

ワイヤレス QoS には、次の主要な設定領域があります。

- 「トラフィック分類」（P.3-62）
- 「インターフェイス キューイング」（P.3-62）
- 「帯域幅のプロビジョニング」（P.3-63）

トラフィック分類

有線ネットワーク インフラストラクチャの場合と同様、できるだけネットワークのエッジの近くで適切なワイヤレス トラフィックを分類またはマークすることが重要です。トラフィック マーキングは、有線およびワイヤレス ネットワーク全体でキューイング方式の入力基準となるため、マーキングはできるだけワイヤレス エンドポイントで行われる必要があります。ワイヤレス ネットワーク デバイスによるマーキングまたは分類は、有線ネットワーク デバイスの場合（表 3-3 を参照）と同じである必要があります。

Cisco Wireless IP Phone は、有線ネットワークのトラフィック分類ガイドラインに従って、音声メディア トラフィックまたは RTP トラフィックを DSCP 46（または PHB EF）でマークし、音声シグナリング トラフィック（SCCP）を DSCP 24（または PHB CS3）でマークします。このトラフィックをマークしたら、ネットワーク全体でプライオリティ処理およびキューイング、またはベストエフォート型よりも優れた処理およびキューイングを行うことができます。ワイヤレス音声デバイスはすべて、この方法でトラフィックをマークできる必要があります。ワイヤレス ネットワーク上の他のトラフィックはすべて、ベストエフォート型としてマークされるか、有線ネットワークのマーキング ガイドラインで規定されているいくつかの中間分類を使用してマークされる必要があります。

インターフェイス キューイング

マーキングが行われたら、有線ネットワークの AP およびデバイスが QoS キューイングを実行できるようにする必要があります。これにより、音声のトラフィック タイプに別のキューが割り当てられるため、このトラフィックがワイヤレス LAN を通過するときにドロップまたは遅延する可能性が低くなります。ワイヤレス ネットワーク上のキューイングは、アップストリームとダウンストリームの 2 つの方向で行われます。アップストリーム キューイングは、ワイヤレス エンドポイントから AP に向かって移動するトラフィックと、AP から有線ネットワークに向かって移動するトラフィックを対象とします。ダウンストリーム キューイングは、有線ネットワークから AP に向かって移動するトラフィックと、AP からワイヤレス エンドポイントに向かって移動するトラフィックを対象とします。

アップストリーム キューイングでは、Wi-Fi Multimedia（WMM）をサポートするデバイスは、プライオリティ キューイングなどのキューイング メカニズムを利用できます。

ダウンストリーム QoS に関しては、Cisco AP は現在、ワイヤレス クライアントに送信されているダウンストリーム トラフィックに対して最大 8 つのキューを割り当てることができます。これらのキューへの入力基準は、DSCP、Access Control List（ACL; アクセス コントロール リスト）、および VLAN などの要素の数に基づいて設定できます。8 つのキューが使用可能ですが、ワイヤレス音声を配置する場合は 2 つのキューだけを使用することを推奨します。音声メディアとシグナリング トラフィックはすべて、最高レベルのプライオリティ キューに入り、他のトラフィックはすべて、ベストエフォート型キューに入る必要があります。これにより、音声トラフィックが最適にキューイング処理されることが保証されます。

この 2 つのキューを自律分散型 AP に対して設定するには、AP 上に 2 つの QoS ポリシーを作成します。1 つめのポリシーには Voice という名前を付け、VLAN のすべてのパケットに対するデフォルトの分類として **Voice < 10 ms Latency (6)** サービス クラスを設定します。2 つめのポリシーには Data という名前を付け、VLAN のすべてのパケットに対するデフォルトの分類として **Best Effort (0)** サービス クラスを設定します。次に、Data ポリシーをデータ VLAN の着信および発信無線インターフェイスに割り当て、Voice ポリシーを Voice VLAN の着信および発信無線インターフェイスに割り当てます。QoS ポリシーを VLAN レベルで適用すると、AP が着信または発信するすべてのパケットを検査して、パケットに適用する必要があるキューイングのタイプを判別することはなくなります。

Lightweight AP では、WLAN コントローラは、同じキューイング ポリシーを提供できる組み込み QoS プロファイルを備えています。音声 VLAN または音声トラフィックは、音声キューにプライオリティ キューイングを設定する、**Platinum** ポリシーを使用するように設定されます。データ VLAN またはデータ トラフィックは、データ キューにベストエフォート型キューイングを設定する、**Silver** ポリシーを使用するように設定されます。次に、これらのポリシーは、VLAN に基づいて着信および発信無線インターフェイスに割り当てられます。

上記のように設定すると、ダウンストリーム方向のすべての音声メディアおよびシグナリングがプライオリティ キューイング処理されることが保証されます。

帯域幅のプロビジョニング

シスコでは、ワイヤレス音声ネットワークのテストに基づいて、802.11b クライアントを持つデータ レート 11 Mbps の 802.11b 専用 AP では、最大 7 つのアクティブな G.711 音声ストリームまたは 8 つの G.729 音声ストリームをサポートできることを確認しています。AP レートが 11 Mbps より低く設定されている場合、各 AP のコール キャパシティが低下します。

54 Mbps のデータ レートの 802.11a では、アクティブな音声ストリームの最大数は AP ごとに 14 ～ 18 に増加します。

54 Mbps のデータ レートの 802.11g 環境の場合、理論上のアクティブ音声ストリームの最大数も、AP あたり 14 ～ 18 に増加します。ただし、大部分の 802.11g 環境は、802.11b クライアント（したがって、11 Mbps のデータレート）および 802.11g クライアントを含む混在環境なので、AP ごとに 8 ～ 12 のアクティブな音声ストリームが含まれ、通常、キャパシティは大幅に低下します。

（注） 同じ AP に関連付けられた 2 台の電話機間のコールは、2 つのアクティブ音声ストリームとしてカウントされます。

これらの制限を超えないようにするには、いくつかのコール アドミッション制御の形式が必要になります。Cisco AP およびワイヤレス音声クライアントには、コール アドミッション制御に使用される 2 つのメカニズムがあります。

- QoS Basic Service Set（QBSS）

  QBSS はビーコン情報要素であり、この情報要素により、AP はワイヤレス IP 電話機にチャネル使用率情報を送信します。この QBSS 値は、ワイヤレス電話機が他の AP にローミングするかどうかを判別するのに役立ちます。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、デバイスがその AP にローミングするべきでないことを示しています。この QBSS 情報は便利ですが、コールが適切な QoS を保持することを保障するものではなく、またコールを処理するのに十分な帯域幅が存在することを保証するものではないため、真のコール アドミッション制御メカニズムではありません。Cisco Unified Wireless IP Phone が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側のデバイスに Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、ワイヤレス IP Phone と別のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

  WMM TSPEC は QoS メカニズムであり、このメカニズムによって、WLAN クライアントはその帯域幅と QoS 要件を通知して、AP がその要件に対応できるようにします。クライアントが電話を掛けようと準備する場合、クライアントは TSPEC を示す Add Traffic Stream（ADDTS）メッセージを，関連付けられた AP に送信します。次に、AP は、帯域幅とプライオリティ処理が使用できるかどうかに応じて、ADDTS 要求を受け入れるかまたは拒否します。コールが拒否された場合、電話機は Network Busy メッセージを受信します。ローミング中、TSPEC をサポートしている通話中のクライアントは、ADDTS メッセージを新しい AP にアソシエーション プロセス の一部として送信して、プライオリティ処理に使用可能な帯域幅を確保します。十分な帯域幅がない場合、ローミングは、隣接する AP が使用可能であれば、それにロードバランスされます。

Cisco Unified Wireless IP Phone 7921G および 7925G は、QBSS と TSPEC の両方をサポートしています（TSPEC は QBSS より優先されます）。したがって、Cisco Unified Wireless IP Phone 7921G または 7925G でのコール アドミッション制御は、TSPEC を使用する場合、より正確になり、AP のコール キャパシティを超過する可能性を排除できます。

（注）　Cisco IOS Release 12.3(7)JA から、AP は 802.11e CCA ベースの QBSS を送信するようになりました。これらの QBSS 値は、特定の AP の実際のチャネル使用率を表します。

QBSS 情報要素が AP から送信されるのは、AP 上で **QoS Element for Wireless Phones** が有効になっている場合だけです（「ワイヤレス AP の設定と設計」（P.3-60）を参照）。

Service Advertisement Framework（SAF）

Cisco Service Advertisement Framework（SAF）を使用すると、ネットワーク アプリケーションで IP ネットワーク内のネットワーク サービスに関する情報をアドバタイズしたり検出したりできます。SAF は、次の機能コンポーネントおよびプロトコルで構成されています。

- SAF クライアントは、サービスに関する情報をアドバタイズしたり消費したりします。
- SAF フォワーダは、SAF サービスの可用性情報を配布したり維持したりします。
- SAF クライアント プロトコルは、SAF クライアントと SAF フォワーダ間で使用されます。
- SAF フォワーダ プロトコルは、SAF フォワーダ間で使用されます。

アドバタイズされたサービスの特性は、SAF フォワーダのネットワークにとって重要ではありません。SAF フォワーダ プロトコルは、サービスの可用性に関する情報を、SAF ネットワークに登録されている SAF クライアント アプリケーションに動的に配布するように設計されています。

SAF でアドバタイズできるサービス

理論上は、どのサービスでも SAF を介してアドバタイズできます。SAF を使用する最も重要なサービスは、Cisco Unified Communications の Call Control Discovery（CCD; コール制御ディスカバリ）です。CCD は SAF を使用して、Cisco Unified CM、Unified CME などの呼制御エージェントによってホストされる内部 Directory Number（DN; ディレクトリ番号）の可用性に関する情報を配布および維持します。また、CCD は、これらの内部ディレクトリ番号に公衆網から到達できるようにする対応した番号プレフィックスも配布します（「To PSTN」プレフィックス）。

SAF の動的な特性、およびコール エージェントがホストする DN 範囲と To PSTN プレフィックスの可用性を SAF ネットワーク内の他のコール エージェントにアドバタイズできることにより、静的でより労働集約的な他のダイヤル プラン配布方式を大幅に上回るメリットを提供します。SAF CCD の詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）を参照してください。

SAF ネットワーク

SAF ネットワークには、次の項で説明するように、多数の機能コンポーネントが含まれています。

SAF フォワーダ、SAF クライアント、および非 SAF ネットワーク

Cisco SAF ネットワークでは、サービス情報は、サービスに関する知識を効率的に配布して検出を容易にする特定の機能を想定した SAF 対応ノードのネットワークを介して配布されます。Cisco SAF ネットワーク ノードは、次の 2 つの機能的役割に分類されます。

- SAF フォワーダ
- SAF クライアント

Cisco SAF ネットワークを設定するには、SAF フォワーダと SAF クライアントの両方を設定する必要があります。Cisco SAF が備えている柔軟性により、必要に応じて、Cisco SAF フォワーダおよび Cisco SAF クライアントとして動作するように単一のエッジ ルータを設定できます。

SAF フォワーダをサポートしているプラットフォームは、次のとおりです。

- Cisco IOS Release 15.0(1)M を搭載した Cisco Integrated Services Routers（ISR; サービス統合型ルータ）、ISR Generation 2（ISR G2）、および 7200 シリーズ ルータ（http://wwwin.cisco.com/ios/release/15mt を参照）
- Cisco IOS Release 12.2(33)SRE を搭載した Cisco 7600 シリーズ ルータ
- Cisco IOS Release 12.2XE 2.5.0 (RLS5) を搭載した Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ

SAF クライアントをサポートしているプラットフォームは、次のとおりです。

- Cisco IOS Release 15.0(1)M を搭載した Cisco Integrated Services Routers（ISR; サービス統合型ルータ）および ISR Generation 2（ISR G2）（http://wwwin.cisco.com/ios/release/15mt を参照）
- Cisco Unified Communications Manager 8.0(1) 以降のバージョン

Cisco SAF フォワーダ

SAF フォワーダは Cisco IOS ルータ上で稼動します。Cisco SAF フォワーダは、Cisco SAF クライアントによってアドバタイズされたサービスを受信し、SAF フォワーダのネットワークを通じてサービスを確実に配布して、Cisco SAF クライアントがサービスを使用できるようにします。

Cisco SAF フォワーダは IP マルチキャストを使用して、LAN 上の他の Cisco SAF フォワーダを自動的に検出し、ピアとして通信します。IP マルチキャストをサポートしていないネットワークでは、SAF フォワーダは、SAF ネイバーとの間にユニキャストのポイントツーポイントの隣接関係を構築することで、ピアとして静的に接続できます。

ネットワーク内で SAF を有効にするために必要なことは、ルータのサブセットを SAF フォワーダとして設定することだけです。SAF フォワーダ間にピア関係が作成されると、SAF フォワーダ間で交換される TCP/IP ベースの SAF メッセージは、どの IP ネットワークでも通過できるようになります。非 SAF ルータと SAF ルータのネットワークでは、任意の IP ルーティング プロトコルを実行できます。

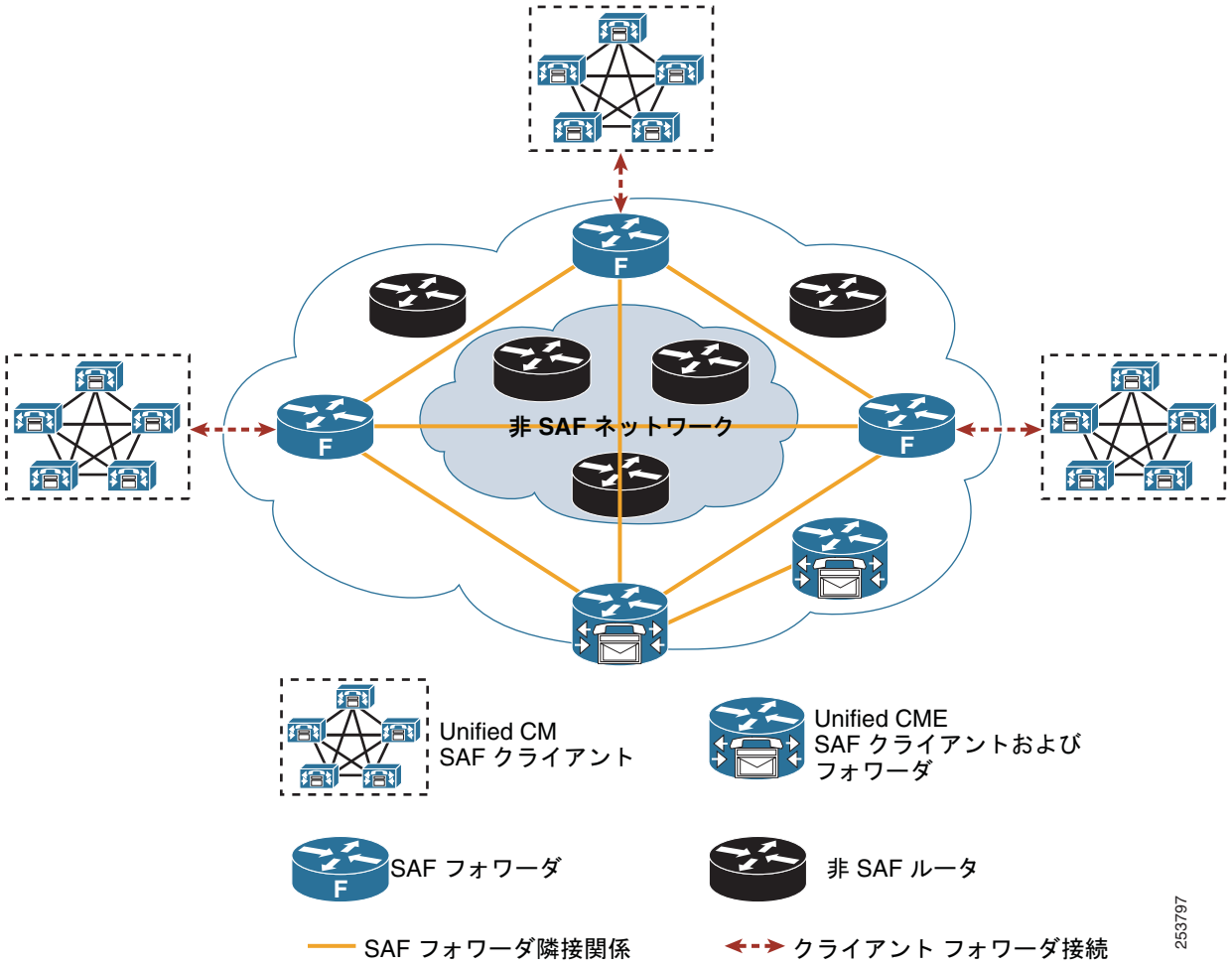
SAF Forwarder Protocol（SAF-FP; SAF フォワーダ プロトコル）は、IP ルーティング プロトコルではなく、「サービス」ルーティング プロトコルです。SAF フォワーダ プロトコルは、サービスに関する情報を IP ネットワークでルーティングします。SAF-FP は、EIGRP テクノロジーに基づくものであり、歴史的に EIGRP ベースの IP ルーティング用に開発されてきた機能の多くを利用して、サービス情報の配布にこの機能を適用します。

SAF フォワーダ プロトコルには、次の特性があります。

- DUAL アルゴリズムおよびスプリット ホライズン ルールを使用して、ルーティング ループが発生しないようにする。
- 定期的なブロードキャストを送信しないで、変更が発生した場合にだけ更新を送信する。
- キープアライブ メカニズムを使用して、ピア SAF フォワーダの可用性を追跡する。
- スケーラブルであり、SAF フォワーダでの障害発生時に迅速なコンバージェンスを提供する。
- SAF ピア（ネイバー）認証方式を提供する。

Cisco SAF フォワーダは、Cisco SAF クライアントと SAF ネットワーク間の関係の基礎を提供します。Cisco SAF フォワーダはネットワーク内の任意の場所に設置できますが、通常はネットワークの端、つまり境界に配置します（図 3-18 を参照）。クライアント/フォワーダの関係は、アドバタイズされる各サービスの状態を維持するために使用されます。クライアントがサービスを削除するか、またはフォワーダ ノードから切り離した場合、ノードは、使用できなくなったサービスについて SAF ネットワークに通知します。SAF フォワーダ ノードが他のフォワーダ ノードからアドバタイズメントを受信すると、アドバタイズメント全体のコピーを作成してから、他の SAF ピアに転送します。

図 3-18　SAF クライアント、SAF フォワーダ、および非 SAF ネットワーク間の隣接関係



Cisco SAF クライアントの概要

Cisco SAF クライアントは、サービスの作成者（サービスを SAF ネットワークにアドバタイズする）、サービスの消費者（SAF ネットワークの 1 つ以上のサービスを要求する）、またはその両方になることができます。SAF クライアントは、次の 3 つの基本機能を実行します。

- SAF ネットワークへの登録
- サービスのパブリッシュ
- サービスへのサブスクライブ

SAF クライアントは、次の 2 つの形式を使用します（図 3-19 を参照）。

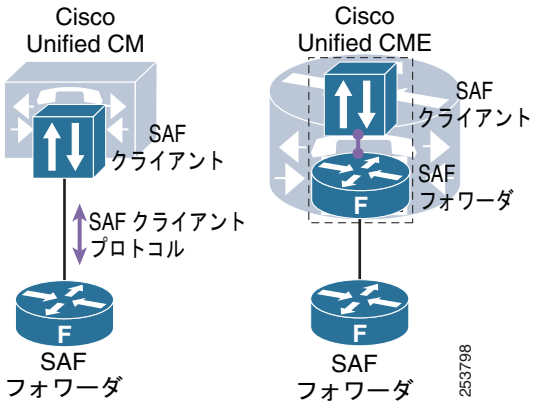
- 内部 SAF クライアント

  内部 SAF クライアントは、SAF フォワーダと同じ Cisco IOS プラットフォームに配置されます。クライアント/フォワーダ接続は、インターネット Application Programming Interface（API; アプリケーション プログラミング インターフェイス）を介して確立されます。Cisco Unified Communications Manager Express（Unified CME）など、Cisco IOS に配置されている呼制御アプリケーションは、内部 SAF クライアントを使用して、共存する内部 SAF フォワーダに接続できます。

- 外部 SAF クライアント

  外部 SAF クライアントは Cisco IOS 内には配置されず、SAF Client Protocol（SAF-CP; SAF クライアント プロトコル）を使用して Cisco IOS ベースの SAF フォワーダと通信します。Cisco Unified CM によって使用される SAF クライアントなどの外部 Cisco SAF クライアントは、設定済みの IP アドレスおよびポート番号を使用して Cisco SAF フォワーダへの TCP/IP 接続を開始します。

図 3-19　　外部および内部 SAF クライアントと SAF フォワーダ



クライアントとフォワーダ間の接続が確立されると、Cisco SAF クライアントは Cisco SAF フォワーダに登録メッセージを送信します。この登録メッセージは、ハンドル（「クライアント ラベル」と呼ばれる）を使用して、Cisco SAF フォワーダに接続されている他のすべての Cisco SAF クライアントから、その Cisco SAF クライアントを一意に識別します。Cisco SAF クライアントが SAF フォワーダへの登録を完了すると、SAF ネットワークにサービスをアドバタイズ（パブリッシュ）したり、SAF ネットワークのサービスを要求（サブスクライブ）したりできるようになります。

サービスをアドバタイズする場合、Cisco SAF クライアントは、提供されるサービスの詳細を含むアドバタイズメントを Cisco SAF フォワーダにパブリッシュ（送信）します。Cisco SAF クライアントは、それぞれに異なるサービスをアドバタイズする複数のパブリッシュ要求を送信できます。Cisco SAF フォワーダは、Cisco SAF クライアントによってパブリッシュされたすべてのサービスをアドバタイズします。

サービスを要求する場合、Cisco SAF クライアントはサブスクライブ要求をフォワーダに送信します。サブスクライブ要求には、Cisco SAF クライアントの目的のサービス セットを表すフィルタが含まれています。この要求に応えて、Cisco SAF フォワーダは、フィルタに一致する現在のサービス セットを一連の通知要求で Cisco SAF クライアントに送信します。フロー制御を提供するために複数の通知要求が送信されるため、Cisco SAF クライアントは、Cisco SAF フォワーダが次の要求を送信する前に、それぞれの通知要求に応答する必要があります。パブリッシュ要求と同様に、Cisco SAF クライアントは、それぞれに異なるフィルタが含まれた複数のサブスクライブ要求を生成できます。また、Cisco SAF クライアントは、既存のサブスクリプションの 1 つを削除するサブスクライブ解除要求も生成できます。

Cisco 外部 SAF クライアントおよび SAF フォワーダとの相互作用

クライアント/フォワーダ認証

外部 SAF クライアントと SAF フォワーダ間での TCP/IP 接続の確立時に、ユーザ名およびパスワードを含む共有秘密キーが認証に使用されます。ユーザ名は、共有秘密キーとして使用するパスワードを決定するためのインデックスとして使用されます。Cisco SAF クライアントは要求を送信するときに、そのユーザ名、実際のメッセージ内容、およびパスワードの MD5 ハッシュを含む属性を送信します。Cisco SAF フォワーダは要求を受信すると、ユーザ名属性を探し、そのユーザ名属性を使用してパスワードのローカル コピーにアクセスします。続いて、ローカルに格納されているパスワードの MD5 ハッシュを計算します。パスワードが一致すると、Cisco SAF クライアントは認証され、接続が続行されます。ただし、Cisco SAF フォワーダが要求を拒否することもあります。

クライアント/フォワーダ キープアライブ

SAF クライアントが SAF ネットワークにサービスをパブリッシュすると、Cisco SAF フォワーダはキープアライブ メカニズムを使用して、Cisco SAF クライアントのステータスを追跡します。Cisco SAF フォワーダおよび Cisco SAF クライアントは、登録時にキープアライブ タイマー値を交換します。Cisco SAF フォワーダは、キープアライブ タイマー値と等しい時間内に Cisco SAF クライアントからの要求が確認されなかった場合、Cisco SAF クライアントで障害が発生したと見なします。Cisco SAF クライアントは、要求間の間隔がこの値を超えないようにします。Cisco SAF クライアントに送信するデータがない場合は、タイマーをリフレッシュする登録メッセージを生成します。

Cisco SAF クライアントで障害が発生したことを Cisco SAF フォワーダが検出すると、その Cisco SAF クライアントの代わりに、アドバタイズされたサービスをネットワークから削除して、Cisco SAF クライアントが確立したすべてのサブスクリプションを抹消します。Cisco SAF クライアントを手動で登録解除して、Cisco SAF フォワーダにすべてのサービスおよびサブスクリプションを適切に削除させることができます。

SAF フォワーダの配置オプション

Unified Communications ネットワークで SAF を有効にするには、1 つ以上の SAF フォワーダを Unified Communications ネットワークに追加する必要があります。Unified CME などの Cisco IOS 呼制御アプリケーションの場合、SAF クライアントとフォワーダをルータ上に共存させて、SAF ネットワーク内の他の SAF フォワーダとの相互接続に使用できます。Unified CM など、外部 SAF クライアントを使用する非 IOS の呼制御アプリケーションは、Unified Communications ネットワーク内に設定されている Cisco IOS SAF フォワーダに接続する必要があります。呼制御アプリケーションと共存しない SAF フォワーダは、ネットワーク内の任意の場所に配置できます。これらのフォワーダの数および場所は、SAF ネットワーク内で必要な復元性および冗長性の程度に大きく依存します。冗長性を提供するには、2 つ以上の SAF フォワーダが必要です（図 3-20 を参照）。SAF ネットワークにさらに SAF フォワーダを追加すると、Unified CM クラスタの各グループに、追加の冗長性およびローカルの SAF フォワーダ リソースを提供できます（図 3-21 を参照）。Cisco ISR および 7200 シリーズ ルータで稼動している Cisco IOS Release 15.0(1) 用の初期バージョンの SAF では、最大 50 台のクライアントを単一の SAF フォワーダに接続できます。

図 3-20　2 つの専用 SAF フォワーダと 2 つの Unified CME SAF フォワーダを使用した SAF ネットワーク

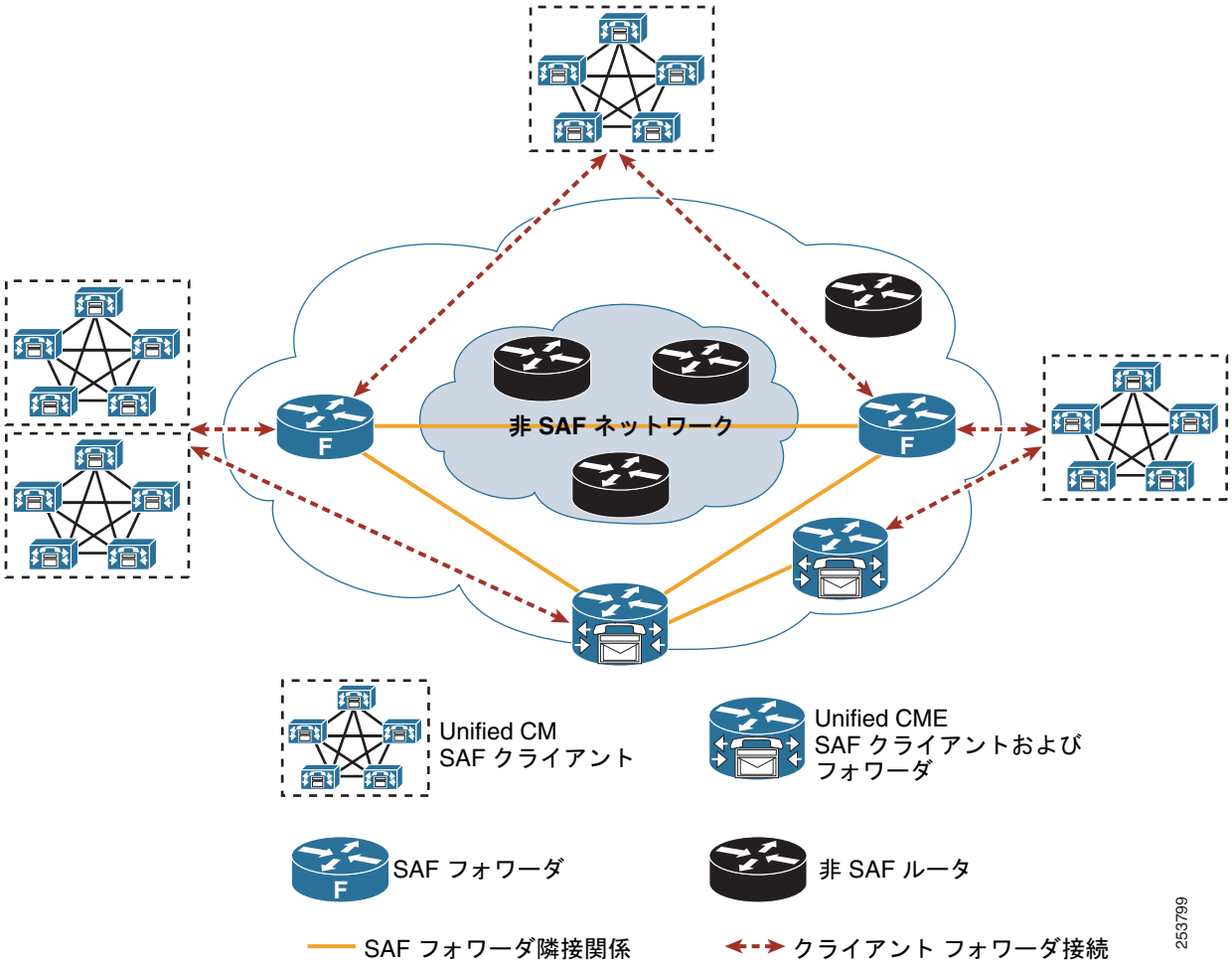
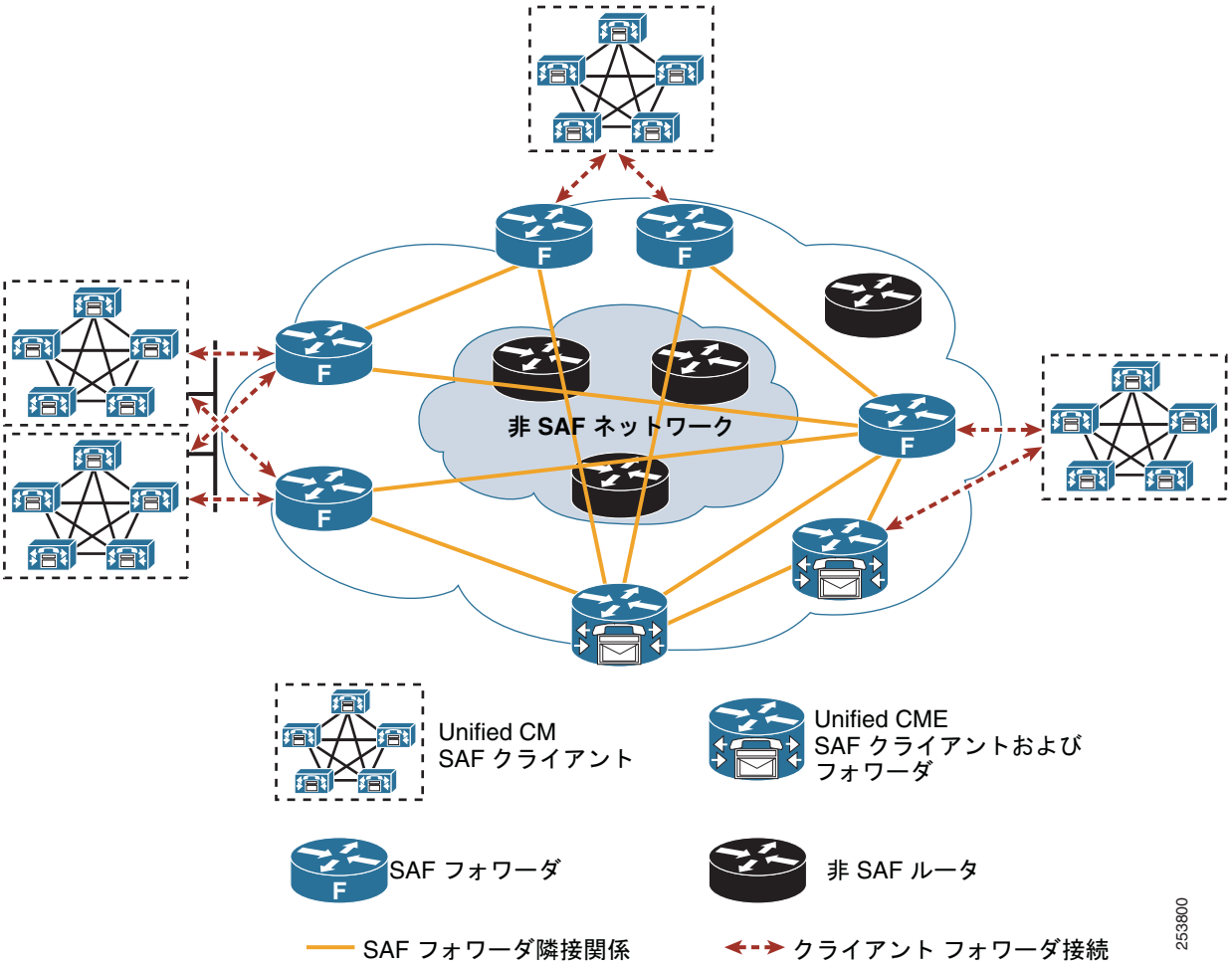


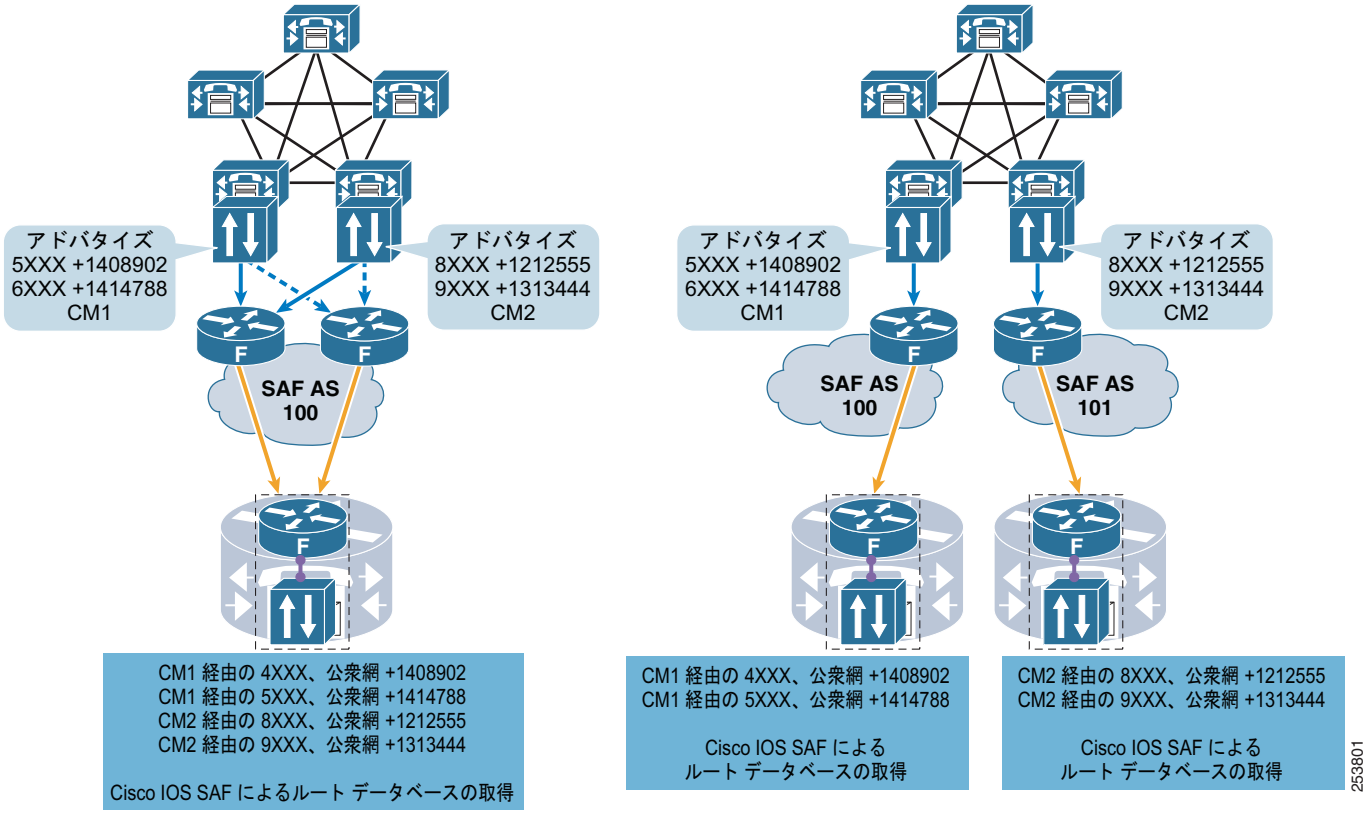
図 3-21　複数の冗長専用 SAF フォワーダと 2 つの Unified CME SAF フォワーダを使用した SAF ネットワーク



SAF 自律システム

IP ルーティング プロトコルと同様に、SAF は Autonomous System（AS; 自律システム）の概念を使用して、SAF ネットワークとその SAF ネットワーク内の共通 SAF フォワーダの境界を定義します（図 3-22 を参照）。大部分の SAF 展開では単一の SAF AS だけが必要ですが、場合によっては（SAF サービスの分離が必要な場合など）、複数の SAF AS を展開することもあります。外部 SAF クライアントは、それぞれに単一の SAF AS に接続してパブリッシュできます。Unified CM クラスタに複数の外部 SAF クライアントを配置している場合、クラスタは複数の SAF AS にサービスをパブリッシュして、各 AS からアドバタイズメントを受信できます。内部 SAF クライアントは、任意の数の Cisco IOS 共存 SAF AS に対してパブリッシュおよびサブスクライブを実行できます。SAF AS 間の SAF サービスの再配送は、現在は使用できません。

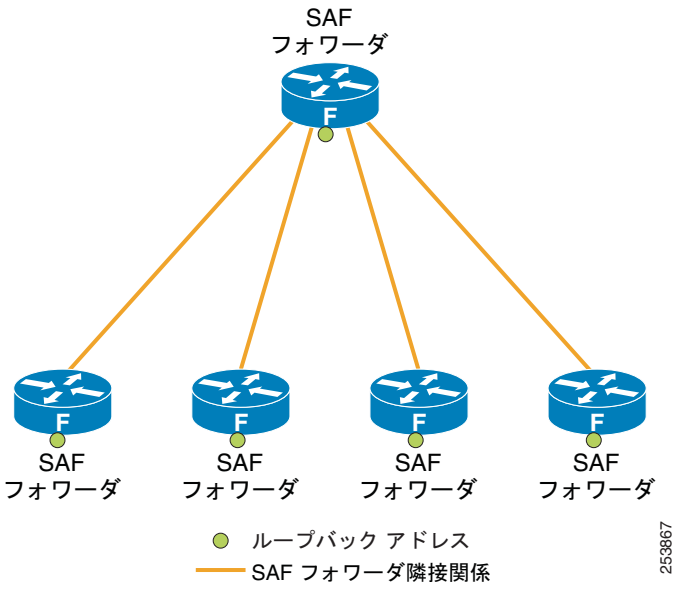
図 3-22　SAF 自律システム



SAF フォワーダのループバック アドレスおよびスプリット ホライズン

図 3-23 のように、ループバック アドレスを SAF フォワーダの設定で使用すると、スプリット ホライズン ルールが有効になり、セントラル SAF フォワーダはスポーク フォワーダ間でアドバタイズメントを転送しません。セントラル SAF フォワーダがスポーク フォワーダ間でアドバタイズメントを転送できるようにするには（これによって SAF ピアのフル メッシュを設定する必要をなくすには）、セントラル SAF フォワーダのループバック インターフェイスで **no split horizon** コマンドを使用します。

図 3-23　SAF およびスプリット ホライズン



Cisco IOS SAF 設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Service Advertisement Framework Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html

CHAPTER 4

Unified Communications のセキュリティ

音声コールの完全性と機密を保護するために、Cisco Unified Communications システムのさまざまなコンポーネントを保護する必要があります。

この章では、IP テレフォニー テクノロジーおよび音声ネットワークに関連したセキュリティ ガイドラインを示します。データ ネットワーク セキュリティの詳細については、次の Web サイトで入手可能な Cisco SAFE Blueprint に関するマニュアルを参照してください。

http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html

この章のガイドラインに従うことは、安全な環境を保証するものではなく、ネットワーク上のすべての侵入攻撃を防止するものではありません。適切なセキュリティを達成するには、適切なセキュリティ ポリシーを確立し、そのセキュリティ ポリシーを適用する必要があります。また、ハッカーおよびセキュリティ コミュニティでの最新の動向を常に把握し、信頼性の高いシステム管理プラクティスにより、すべてのシステムを保守およびモニタする必要があります。

この章では、集中型コール処理および分散型コール処理について説明します。WAN を介したクラスタリングは含まれていますが、Survivable Remote Site Telephony（SRST）などのローカル フェールオーバー メカニズムは含まれていません。この章では、ヘッドエンド障害が発生したときに、すべてのリモート サイトが、ヘッドエンドまたはローカル コール処理バックアップへの冗長リンクを使用できることを前提としています。基本的にここでは、ネットワーク アドレス変換（NAT）と IP テレフォニーの間の対話については説明しません。この章では、すべてのネットワーク プライベート アドレスが指定されており、重複する IP アドレスが含まれていないことも前提としています。

この章の新規情報

表 4-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 4-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
認証証明書	「電話機の認証および暗号化」（P.4-20）	2011 年 6 月 2 日
シングル サインオン	「シングル サインオン」（P.4-41）	2011 年 6 月 2 日
IPv6 の Adaptive Security Appliance（ASA）サポート	「ファイアウォール」（P.4-25）	2011 年 1 月 31 日
アプリケーション インスペクション	「ファイアウォール」（P.4-25）	2011 年 1 月 31 日
802.1X 認証	「802.1X ポート ベースの認証」（P.4-16）	2010 年 7 月 23 日
Adaptive Security Appliance（ASA）Unified Communications Proxy 機能	「ASA Unified Communications Proxy 機能」（P.4-28）	2010 年 4 月 2 日

表 4-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Intercompany Media Engine（IME）	「ASA Intercompany Media Engine プロキシ」（P.4-31）	2010 年 4 月 2 日
IPv6 アドレッシング	「IPv6 アドレッシング」（P.4-6）	2010 年 4 月 2 日
Link Layer Discovery Protocol for Media Endpoint Devices（LLDP-MED）	「アクセス セキュリティ」（P.4-6）	2010 年 4 月 2 日
Service Advertisement Framework（SAF）	「SAF サービス」（P.4-39）	2010 年 4 月 2 日
Unified CM トランクおよび Cisco Unified Border Element	「Cisco Unified Border Element との Unified CM トランク統合」（P.4-39）	2010 年 4 月 2 日
電話機の VPN クライアント	「IP Phone の VPN クライアント」（P.4-21）	2010 年 4 月 2 日

セキュリティの概要

この項では、ネットワーク内の音声データを保護するために使用できる、一般的なセキュリティ機能とセキュリティ プラクティスについて説明します。

セキュリティ ポリシー

この章では、企業が、すでにセキュリティ ポリシーを配置していることを前提としています。関連付けるセキュリティ ポリシーがない場合は、いかなるテクノロジーも配置しないように推奨します。セキュリティ ポリシーは、ネットワーク内の機密データを特定し、ネットワーク内で転送する際にはデータを適切に保護します。セキュリティ ポリシーを配置すると、ネットワーク上のデータ トラフィックのタイプで要求されているセキュリティ レベルを定義するのに役立ちます。各データ タイプで独自のセキュリティ ポリシーが必要な場合もあれば、必要でない場合もあります。

企業ネットワークにデータ用のセキュリティ ポリシーが存在しない場合、この章で任意のセキュリティ推奨事項を有効にする前に、セキュリティ ポリシーを作成する必要があります。セキュリティ ポリシーがないと、ネットワークで有効なセキュリティ機能が設計どおりに動作しているかどうかを検証する方法がありません。またセキュリティ ポリシーがないと、ネットワーク内で実行されるすべてのアプリケーションやデータ タイプに対してセキュリティを有効にする、体系的な方法がありません。

（注）　この章で説明するセキュリティに関するガイドラインと推奨事項に従うのは重要ですが、実際の企業のセキュリティ ポリシーを制定するには、この章のガイドラインと推奨事項だけでは不十分です。任意のセキュリティ テクノロジーを実装する前に、社内セキュリティ ポリシーを定義する必要があります。

この章では、ネットワーク上の音声データを保護するために使用可能な、シスコシステムズ ネットワークの特徴と機能性について詳しく説明します。保護する対象のデータ、そのデータ タイプで必要な保護の程度、およびその保護を提供するのに使用するセキュリティ技法をどのように定義するかは、セキュリティ ポリシーによって異なります。

IP テレフォニーが含まれるセキュリティ ポリシーで困難な問題の 1 つは、通常、データ ネットワークと従来の音声ネットワークの両方に存在するセキュリティ ポリシーの結合です。ネットワークへの音声データ統合のすべての側面が、導入済みのセキュリティ ポリシーまたは社内環境の適切なレベルで保護されていることを確認してください。

適正なセキュリティ ポリシーの基本は、ネットワーク内でデータの重要度を定義することです。重要度に応じてデータをランク付けしたら、データ タイプごとに、セキュリティ レベルを確立する方法を決定できます。それから、ネットワークとアプリケーション機能の両方を使用して、適切なレベルのセキュリティを達成できます。

要約すると、セキュリティ ポリシーを定義するには、次のプロセスに従います。

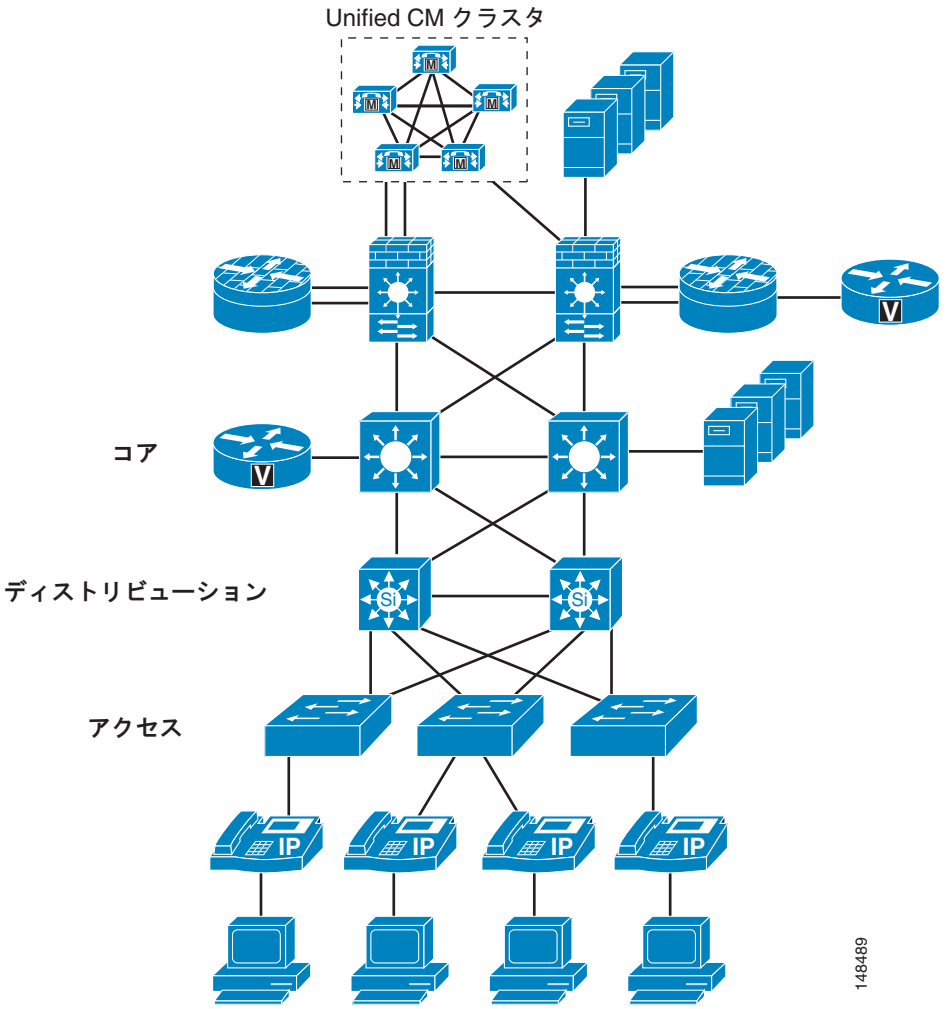
- ネットワーク上のデータを定義する。
- データの重要性を定義する。
- データの重要性に基づいてセキュリティを適用する。

レイヤ化したセキュリティ

この章では、最初にユーザが PC に接続できる電話機ポートについて説明します。また、電話機がネットワークを介して、アクセス スイッチ、ディストリビューション レイヤ、コア レイヤ、最後にデータセンターに到達する方法について説明します（図 4-1 を参照）。アクセス ポートからネットワーク自体に至るまで、セキュリティ レイヤの上にレイヤを構築します。各機能について説明するにあたり、社内セキュリティ ポリシーの観点から考慮する必要がある、それぞれの利点と欠点について説明します。

たとえば、図 4-1 は、IP テレフォニー ネットワークを使用することの利点と欠点の両方を示しています。音声製品は IP を使用してすべてのデバイスに接続するため、ネットワーク内の任意の場所に配置できます。この特性を使用すると、ネットワークの設計者は、IP テレフォニー アプリケーションを配置するうえで物理的にも論理的にも簡単な場所に、デバイスを配置できます。しかし、簡単に配置できるということは、セキュリティがより複雑になることを意味します。接続性があるところであればネットワーク内のどこにでも、IP テレフォニー デバイスを配置できるからです。

図 4-1　セキュリティ レイヤ



インフラストラクチャの保護

IP テレフォニー データがネットワークを横断するときのデータの安全性とセキュリティは、データを転送するデバイスと同程度にしかすぎません。導入済みのセキュリティ ポリシーで定義されているセキュリティ レベルによっては、ネットワーク デバイスのセキュリティを向上させる必要がある場合もあれば、IP テレフォニー トラフィックを転送するのにすでに十分に安全な場合もあります。

ネットワーク全体のセキュリティを向上させるためにデータ ネットワークで実行できる、多くのベストプラクティスがあります。たとえば、攻撃者がパスワードをクリア テキスト形式で見ることができないように、Telnet（パスワードをクリア テキスト形式で送信します）を使用して任意のネットワーク デバイスに接続する代わりに、Secure Shell（SSH、Telnet の安全な形式）を使用できます。

ゲートウェイとゲートキーパーは、Cisco IOS 機能セットを使用して設定できます。この機能セットは、必要な音声機能を提供しますが、Telnet だけをサポートし、Secure Shell（SSH）はサポートしません。Access Control List（ACL; アクセス コントロール リスト）を使用して、Telnet によるルータへ

の接続を誰に許可するかを制御することを推奨します。Telnet ではユーザ名とパスワードがクリア テキスト形式で送信されるため、ゲートキーパーには安全なネットワーク セグメントにあるホストから接続するとさらに安全です。

これらのデバイスを不正アクセスから保護するには、ファイアウォール、アクセス コントロール リスト、認証サービス、およびその他の Cisco セキュリティ ツールも使用する必要があります。

物理的なセキュリティ

従来の PBX は、通常、安全な環境にロックされますが、IP ネットワークも同じように扱う必要があります。IP テレフォニー トラフィックを伝送する各デバイスは実際には IP PBX の一部です。通常の一般的なセキュリティ プラクティスを使用して、これらのデバイスへのアクセスを制御する必要があります。ユーザまたは攻撃者が、ネットワーク内のデバイスの 1 つに物理的にアクセスできる場合、あらゆる種類の問題が発生します。強力なパスワード セキュリティがあり、ユーザまたは攻撃者がネットワーク デバイスに侵入できない場合でも、それらのユーザや攻撃者がデバイスを切断してすべてのトラフィックを停止することにより、ネットワークの大破壊を引き起こす可能性はあります。

全般的なセキュリティ プラクティスの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

- http://www.cisco.com/en/US/netsol/ns744/networking_solutions_program_home.html
- http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html

IP アドレッシング

論理的に分離された IP テレフォニー ネットワークに流入および流出するデータを制御するうえで、IP アドレッシングが重要になる場合があります。ネットワーク内で IP アドレッシングを適切に定義するほど、ネットワーク上のデバイスの制御は簡単になります。

このマニュアルの他の項で説明されているとおり（「キャンパス アクセス レイヤ」（P.3-5）を参照）、RFC 1918 に基づいた IP アドレッシングを使用する必要があります。このアドレッシング方式では、ネットワークの IP アドレッシングをやり直すことなく、IP テレフォニー システムをネットワークに配置できます。音声エンドポイントの IP アドレスは適切に定義されていて理解しやすいので、RFC 1918 を使用すると、ネットワーク内の制御をより適切に実行できます。すべての音声エンドポイントが 10.x.x.x. のネットワーク内でアドレッシングされていると、アクセス コントロール リスト（ACL）、およびこれらのデバイスが受信または送信するデータのトラックは単純になります。

利点

音声配置のために適切に定義された IP アドレッシング プランがあると、IP テレフォニー トラフィックを制御するための ACL の書き込みが簡単になり、ファイアウォールの配置に役立ちます。

RFC 1918 を使用すると、スイッチごとに 1 つの VLAN を簡単に配置でき、Voice VLAN を Spanning Tree Protocol（STP; スパニング ツリー プロトコル）ループから保護できます。スイッチごとに 1 つの VLAN を配置するのは、キャンパスの設計におけるベスト プラクティスです。

ルート集約を正しく配置すると、ルーティング テーブルを、音声配置の前と同じ大きさか、それよりわずかに大きい程度に保つのに役立ちます。

欠点

ルーティング テーブルが正しく設計されていなかったり、ルート集約が使用されていなかったりすると、ルーティング テーブルは大きくなる場合があります。

IPv6 アドレッシング

IPv6 アドレッシングの導入により、ネットワーク アドレス スペースが拡張され、エンドポイントのプライバシーとセキュリティのためのオプションが増えました。IPv4 と IPv6 の両方にセキュリティに関する同様の問題がありますが、IPv6 にはいくつかの利点があります。たとえば、IPv6 の主な利点の 1 つはサブネットのサイズが非常に大きいことであり、自動スキャンおよび偵察攻撃を阻止します。

セキュリティの観点での IPv6 と IPv4 の比較については、次の Web サイトで入手可能な『*IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation*』を参照してください。

http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf

IP アドレッシングの方式として IPv6 を検討する際は、次のキャンパスおよび支社の設計ガイドに記載されているベスト プラクティスに従ってください。

- 『*Deploying IPv6 in Campus Networks*』
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Campus/CampIPv6.html
- 『*Deploying IPv6 in Branch Networks*』
  http://www.cisco.com/en/US/docs/solutions/Enterprise/Branch/BrchIPv6.html

アクセス セキュリティ

この項では、ネットワーク内の音声データを保護するために使用できる、アクセス レベルのセキュリティ機能について説明します。

Voice VLAN と Video VLAN

電話機に IP アドレスが与えられる前に、電話機は、電話機とスイッチの間で実行される Cisco Discovery Protocol（CDP）ネゴシエーションを使用して、配置先として適切な VLAN を判別します。このネゴシエーションにより、電話機は「Voice VLAN」内のスイッチに対して 802.1q タグ付きのパケットを送信でき、音声データと、電話機の背後にある PC から送られる他のすべてのデータはレイヤ 2 で分離されます。Voice VLAN は電話機が動作するための要件ではありませんが、ネットワーク上の他のデータからの追加の分離を提供します。

Sony 社製および Tandberg 社製の SCCP エンドポイントは、Cisco Discovery Protocol（CDP）または 802.1Q VLAN ID タギングをサポートしません。サードパーティ製デバイスが含まれる場合にデバイス検出を可能にするには、Link Layer Discovery Protocol（LLDP）を使用します。LLDP for Media Endpoint Devices（LLDP-MED）は、音声エンドポイントのサポートを向上させる LLDP の拡張です。LLDP-MED では、LLDP-MED 対応エンドポイントを検出したときに、スイッチ ポートが LLDP から LLDP-MED へどのように移行するかが定義されています。IP Phone および LAN スイッチでの LLDP と LLDP-MED 両方のサポートは、ファームウェアおよびデバイス モデルに依存します。特定の電話機またはスイッチ モデルで LLDP-MED がサポートされているかどうかを判別するには、次の Web サイトで入手可能な特定の製品リリース ノートまたはお知らせを確認してください。

- http://www.cisco.com/en/US/products/hw/phones/ps379/prod_release_notes_list.html
- http://www.cisco.com/en/US/products/sw/iosswrel/ps5012/prod_bulletins_list.html

（注）　LLDP-MED 対応の IP Phone が、LLDP をサポートしない以前の Cisco IOS リリースを実行している Cisco Catalyst スイッチに接続されると、スイッチは、余計なデバイスがスイッチ ポートに接続されていることを示す場合があります。これは、Cisco Catalyst スイッチがポート セキュリティを使用して接続デバイス数をカウントしている場合に発生します。LLDP パケットの発生により、ポート カウントが増え、スイッチがポートを無効にする場合があります。LLDP-MED リンク レイヤ プロトコルをサポートするファームウェアを持つ Cisco IP Phone を配置する前に、Cisco Catalyst スイッチが LLDP をサポートしていることを確認するか、ポート カウントを最低でも 3 に増やしてください。

Cisco Unified Video Advantage は PC で実行するクライアント アプリケーションですが、IP Phone にも関連付けられています。PC はデータ VLAN に存在し、電話機は音声 VLAN に存在しているのが普通です。IP Phone への関連付けのために、Cisco Unified Video Advantage は、TCP/IP で動作する Cisco Audio Session Tunnel（CAST）プロトコルを使用します。したがって、Cisco Unified Video Advantage は、ビデオ VLAN とデータ VLAN の間で IP パケットをルーティングするように設定された、レイヤ 3 ルータをすべて経由して通信する必要があります。これらの VLAN 間で設定されているアクセス コントロール リストまたはファイアウォールがある場合は、CAST プロトコルの動作を許可するように修正する必要があります。CAST は両方向で TCP ポート 4224 を使用しています。Cisco Unified Video Advantage は IP Phone とは通信しますが、Unified CM とは通信しません。ただし、ソフトウェア アップデートをダウンロードするために Cisco Unified Video Advantage が定期的に TFTP サーバ（1 つ以上の Unified CM サーバに共存可能）に確認する場合を除きます。したがって、データ VLAN と TFTP サーバの間で TFTP プロトコルを許可する必要もあります。

H.323 クライアント、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、およびゲートウェイは、H.323 プロトコルを使用して Unified CM と通信します。Unified CM H.323 トランク（H.225 やインタークラスタ トランクのほかに、RAS アグリゲーター トランク タイプなど）は、ウェルノウン TCP ポート 1720 ではなくランダムなポート範囲を使用します。したがって、これらのデバイスと Unified CM サーバの間で広範囲の TCP ポートを許可する必要があります。ポートの使用方法の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager TCP and UDP Port Usage*』ガイドの最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

MCU とゲートウェイはインフラストラクチャ デバイスと見なされ、通常は Unified CM サーバに隣接するデータ センターに存在します。一方、H.323 クライアントは通常はデータ VLAN に存在します。

SCCP モードで実行するように設定されている Unified Videoconferencing 3500 シリーズ MCU は、設定のダウンロードのために TFTP サーバと通信し、シグナリングのために Unified CM サーバと通信し、RTP メディア トラフィックのために他のエンドポイントと通信します。したがって、MCU と TFTP サーバの間で TFTP を許可し、MCU と Unified CM サーバの間で TCP ポート 2000 を許可し、MCU と音声 VLAN、データ VLAN、ゲートウェイ VLAN の間で RTP メディア用の UDP ポートを許可する必要があります。

利点

Voice VLAN は、スイッチから電話機に自動的に割り当てることができます。これにより、レイヤ 2 およびレイヤ 3 で、音声データと、ネットワーク上の他のすべてのデータが分離されます。分離した VLAN には Dynamic Host Configuration Protocol（DHCP）サーバで別個の IP スコープを与えることができるので、Voice VLAN を使用すると、異なる IP アドレッシング スキームを実行できます。

アプリケーションは、電話機からの CDP メッセージを使用して、緊急電話コール中に電話機のロケーションを判別するのを支援します。電話機が接続されているアクセス ポートで CDP が有効でない場合、電話機のロケーションを判別するのは特に困難です。

欠点

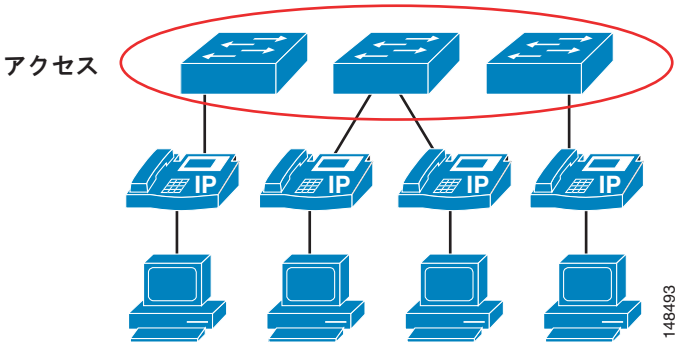
通常は電話機に送られる CDP メッセージから情報が収集され、その情報が一部のネットワークを検出するために使用される可能性があります。Unified CM で音声またはビデオ用に使用可能なすべてのデバイスが、音声 VLAN の検出に CDP を使用できるわけではありません。

スイッチ ポート

Cisco スイッチ インフラストラクチャには、データ ネットワークを保護するために使用できる多くのセキュリティ機能があります。この項では、ネットワーク内の IP テレフォニー データを保護するため、Cisco Access Switch で使用できるいくつかの機能について説明します（図 4-2 を参照）。この項では、現在のすべての Cisco スイッチで使用可能なすべてのセキュリティ機能について説明するのではなく、シスコが製造する多くのスイッチで使用されている一般的なセキュリティ機能をリストします。ネットワーク内に配置された特定の Cisco デバイスで使用可能なセキュリティ機能の追加情報については、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

図 4-2　　電話機が接続される代表的なアクセス レイヤ設計



ポートセキュリティ：MAC CAM フラッディング

スイッチ ネットワークに対する典型的な攻撃は、MAC 連想メモリ（CAM）フラッディング攻撃です。このタイプの攻撃では、スイッチに対して大量の MAC アドレスによるフラッディングが実行され、スイッチは、エンド ステーションまたはデバイスが接続されているポートを判別できなくなります。デバイスが接続されているポートを判別できない場合、スイッチは、そのデバイスが宛先になっているトラフィックを VLAN 全体にブロードキャストします。これにより、攻撃者は、VLAN 内のすべてのユーザに到達するすべてのトラフィックを見ることができます。

macof などのハッカー ツールを使用した悪意のある MAC フラッディング攻撃を許可しないようにするには、それらのポートの接続性要件に基づいて、個々のポートへのアクセスを許可されている MAC アドレスの数を制限します。悪意のあるエンド ユーザ ステーションは、macof を使用して、ランダムに生成された送信元 MAC アドレスからランダムに生成された宛先 MAC アドレスへの MAC フラッディングを発信できます。送信元と宛先の両方がスイッチ ポートに直接接続されている場合もあれば、送信元と宛先が IP Phone を経由して接続する場合もあります。macof ツールは非常にアグレッシブなツールで、通常は、Cisco Catalyst スイッチの連想メモリ（CAM）テーブルを 10 秒未満でいっぱいにできます。CAM テーブルがいっぱいなので、後続のパケットは取得されないまま残され、フラッディングが発生します。これは、攻撃先の VLAN の共有イーサネット ハブ上のパケットと同じほど破壊的で危険です。

MAC フラッディング攻撃を抑制するには、ポート セキュリティまたはダイナミック ポート セキュリティのいずれかを使用できます。許可メカニズムとしてポート セキュリティを使用する必要がないカスタマーの場合、特定のポートに接続する機能に対応する数の MAC アドレスを持つダイナミック ポート セキュリティを使用できます。たとえば、1 台のワークステーションが接続されているポートの場合、取得する MAC アドレスの数を 1 に制限できます。1 台の Cisco Unified IP Phone と、その背後に 1 台のワークステーションが接続されているポートの場合、電話機の PC ポートに 1 台のワークステーションを接続するには、取得する MAC アドレスの数を 2 に設定できます（1 つは IP Phone 用、1 つは電話機の背後にあるワークステーション用）。以前であれば、トランク モードでポートを設定する旧来の方法により、この場合の設定は 3 つの MAC アドレスになります。電話機ポートの設定でマルチ VLAN アクセス モードを使用する場合、この場合の設定は 2 つの MAC アドレスになります。1 つは電話機用、1 つは電話機に接続された PC 用です。PC ポートに接続するワークステーションがない場合、そのポートの MAC アドレスの数は 1 に設定する必要があります。これらの設定は、スイッチ上のマルチ VLAN アクセス ポート用です。トランク モードに設定されているポート（電話機と PC が接続されているアクセス ポートでは推奨されていない配置）では、設定が異なる場合があります。

ポート セキュリティ：Gratuitous ARP

ネットワーク上の他のデータ デバイスと同様、電話機が従来のデータ攻撃を受けることがあります。電話機には、企業ネットワークで発生する可能性がある、いくつかの一般的なデータ攻撃を防止する機能があります。そのような機能の 1 つは、Gratuitous Address Resolution Protocol（Gratuitous ARP または GARP）です。この機能は、電話機に対する man-in-the-middle（MITM; 中間者）攻撃を防止します。MITM 攻撃では、攻撃者は、エンド ステーションをだまして自らがルータであると信じ込ませ、ルータには自らがエンド ステーションであると信じ込ませます。この方式では、ルータとエンド ステーションの間のすべてのトラフィックが攻撃者を経由するようになり、攻撃者は、すべてのトラフィックをロギングしたり、データの会話に新しいトラフィックを注入したりできるようになります。

Gratuitous ARP は、攻撃者がネットワークの音声セグメントにアクセスできた場合に、攻撃者が電話機からのシグナリングや RTP 音声ストリームを取り込むことから電話機を保護するのに役立ちます。この機能で保護されるのは電話機だけです。インフラストラクチャの残りの部分は、Gratuitous ARP 攻撃から保護されません。スイッチ ポートには電話機とネットワーク デバイスの両方を保護する機能があるので、Cisco インフラストラクチャを実行している場合、この機能はそれほど重要ではありません。これらのスイッチ ポートの機能の説明については、「スイッチ ポート」（P.4-8）を参照してください。

（注）　Gratuitous ARP 機能は、IPv6 アドレッシングを使用して設定されたデバイスには適用されません。IPv6 では ARP ではなく Neighbor Discovery（ND; ネイバー探索）が使用されます。

利点

Gratuitous ARP 機能は、電話機から発信されてネットワークに至るシグナリングおよび RTP 音声ストリームに対する従来の MITM 攻撃から、電話機を保護します。

欠点

別の電話機から発信されたかネットワークを経由して到達するダウンストリーム シグナリングおよび RTP 音声ストリームは、電話機のこの機能では保護されません。保護されるのは、この機能が有効になっている電話機からのデータのみです（図 4-3 を参照）。

デフォルト ゲートウェイが Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を実行している場合や、HSRP 設定でデフォルト ゲートウェイの仮想 MAC アドレスの代わりに物理 MAC アドレスが使用されている場合、およびプライマリ ルータが新しい MAC アドレスを持つセカンダリ ルータにフェールオーバーした場合、電話機はデフォルト ゲートウェイの古い MAC アドレスを継続使用します。このシナリオでは、最大 40 分間の障害が発生することがあります。発生する可能性があるこの問題を避けるため、HSRP 環境では常に仮想 MAC アドレスを使用してください。

図 4-3　Gratuitous ARP は導入先の電話機は保護するが他のトラフィックは保護しない

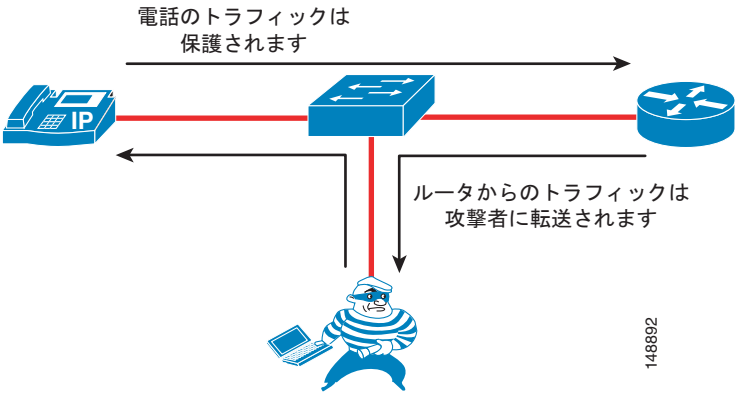


図 4-3 が示しているとおり、Gratuitous ARP 機能を持つ電話機からのトラフィックは保護されますが、エンドポイントに、データ フローを保護する機能がない可能性があるので、攻撃者が別のエンドポイントからのトラフィックを見ることができる場合があります。

ポート セキュリティ：ポート アクセスの防止

MAC アドレスによりポートで指定されているデバイスからのアクセスを除く、すべてのポート アクセスを防止します。これは、デバイスレベルのセキュリティ許可の 1 つの形式です。この要件は、デバイス MAC アドレスの単一のクレデンシャルを使用してネットワークへのアクセスを許可するときに使用します。ポート セキュリティ（非動的形式）を使用する場合、ネットワーク管理者は、すべてのポートに MAC アドレスを静的に関連付ける必要があります。これに対して、ダイナミック ポート セキュリティを使用する場合、ネットワーク管理者は、スイッチで取得する MAC アドレスの数を指定するだけです。その後、ポートに最初に接続するデバイスが適切なデバイスであるとの前提に基づき、一定期間、それらのデバイスにのみポートへのアクセスを許可します。

この期間は、固定タイマーまたは非活動タイマー（非持続アクセス）のいずれかで決定するか、永続的に割り当てることができます。後者の場合、スイッチのリロードまたはリブートが発生しても、取得された MAC アドレスはポートで保持されます。

デバイス モビリティに対し、スタティック ポート セキュリティまたは持続性のあるダイナミック ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

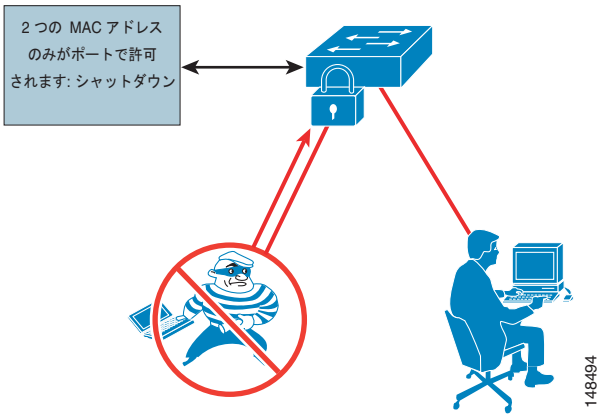
セキュリティ面を考慮すると、ポート アクセスを認証および許可するためのより強力なメカニズムがあります。MAC アドレス許可ではなく、ユーザ ID およびパスワード クレデンシャルに基づいたメカニズムです。MAC アドレスだけでは、ほとんどのオペレーティング システムで簡単にスプーフィングまたは偽造されます。

ポート セキュリティ：不良ネットワーク拡張の防止

ハブまたはワイヤレス Access Point（AP; アクセス ポイント）を経由する不良なネットワーク拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザがワイヤレス AP を接続した場合、ワイヤ

レス AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません（図 4-4 を参照）。一般的に、MAC フラッディングを停止するのに適切な設定は、不良アクセスを抑制するためにも適切です。

図 4-4　　MAC アドレス数の制限による不良ネットワーク拡張の防止



利点

ポート セキュリティは、攻撃者がスイッチの CAM テーブルに対してフラッディングを実行したり、すべての受信トラフィックをすべてのポートに送信するハブに VLAN を転送したりするのを防止します。また、エンドポイントにハブまたはスイッチを追加することにより、認可されていないネットワークの拡張を防止します。

欠点

MAC アドレスの数が正しく定義されていないと、ネットワークへのアクセスが拒否されたり、エラーによりポートが無効化されてすべてのデバイスがネットワークから削除されたりする場合があります。

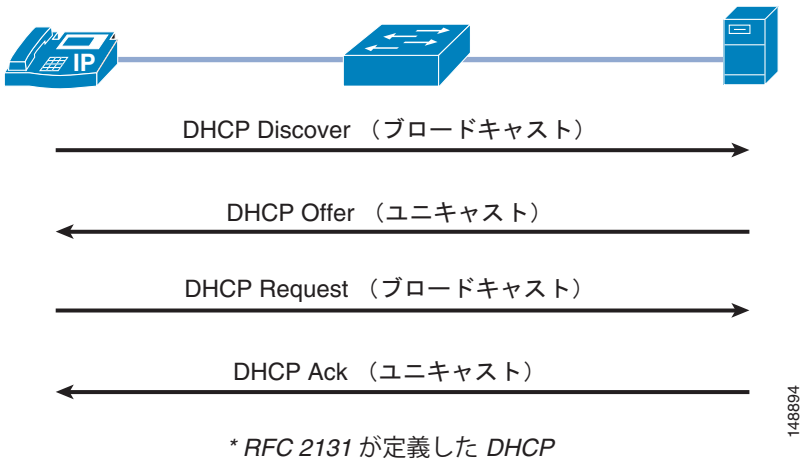
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

Dynamic Host Configuration Protocol（DHCP）スヌーピングは、承認されていない DHCP または不正な DHCP サーバがネットワーク上で IP アドレスを分配するのを防止します。具体的には、ポートが応答することが許可されている場合を除き、DHCP 要求へのすべての応答をブロックします。ほとんどの電話機配置では DHCP を使用して複数の電話機に IP アドレスを提供しているので、スイッチで DHCP スヌーピング機能を使用して、DHCP メッセージングを保護する必要があります。不正な DHCP サーバは、クライアントからのブロードキャスト メッセージに応答して不正な IP アドレスを分配したり、IP アドレスを要求しているクライアントを混乱させたりすることを試行できます。

DHCP スヌーピングを有効にすると、デフォルトでは、VLAN のすべてのポートが、信頼されていないポートとして扱われます。信頼されていないポートとは、予約済みの DHCP 応答を行うことが許可されていない、ユーザ方向のポートのことです。信頼されていない DHCP スヌーピング ポートが DHCP サーバ応答を行うと、ブロックされて応答されません。このように、不正な DHCP サーバが応答することが防止されます。ただし、正当に接続された DHCP サーバまたは正当なサーバへのアップリンクは、信頼する必要があります。

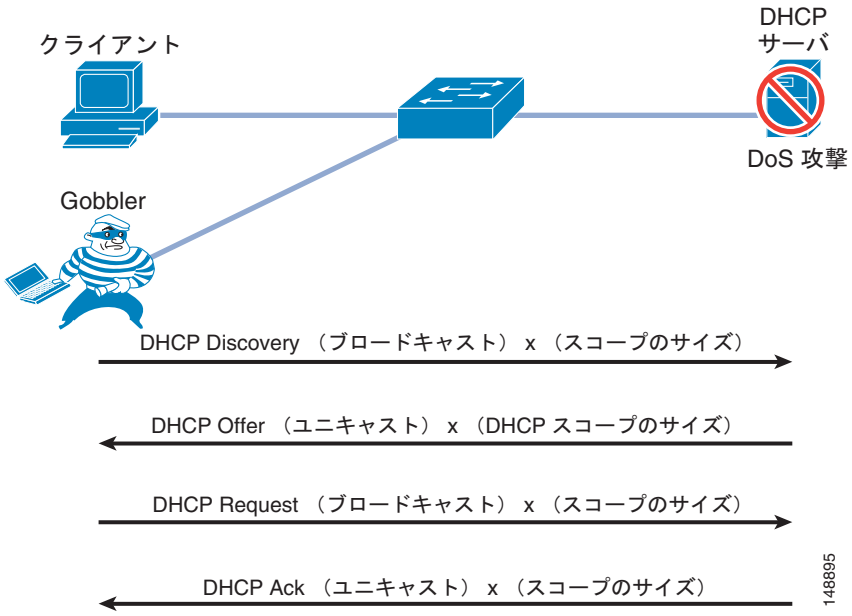
図 4-5 は、DHCP サーバに IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 4-5　DHCP 要求の通常の操作



ただし、攻撃者は、単一の IP アドレスではなく、VLAN 内で使用可能なすべての IP アドレスを要求できます（図 4-6 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Unified CM に接続できません。

図 4-6　攻撃者は VLAN で使用可能なすべての IP アドレスを取得できる



利点

DHCP スヌーピングは、承認されていない DHCP サーバがネットワークに配置されるのを防止します。

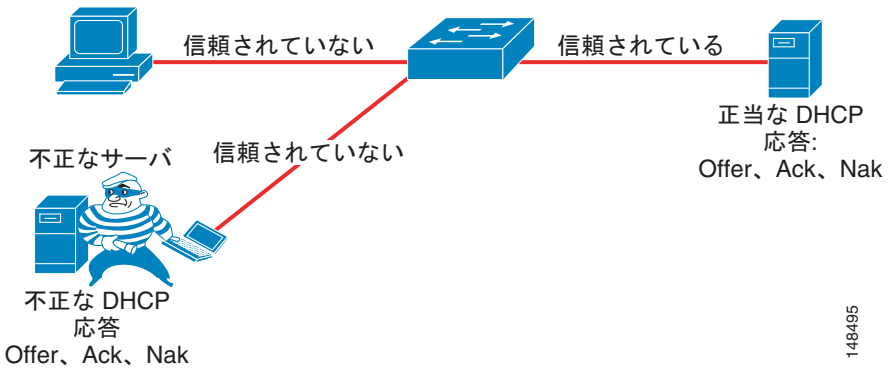
欠点

この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

DHCP スヌーピング：DHCP スターベーション攻撃の防止

Gobbler などのツールを使用した DHCP アドレス スコープ スターベーション攻撃は、DHCP Denial of Service（DoS; サービス拒否）攻撃を仕掛けるために使用されます。Gobbler ツールは、ランダムに生成される異なる送信元 MAC アドレスから DHCP 要求を実行するので、ポート セキュリティを使用して MAC アドレスの数を制限することにより、Gobbler ツールが DHCP アドレス スペースをスタービングするのを防止できます（図 4-7 を参照）。ただし、高度な DHCP スターベーション ツールでは、1 つの送信元 MAC アドレスから DHCP 要求を実行でき、DHCP ペイロード情報も多様です。DHCP スヌーピングを有効にすると、信頼されていないポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。

図 4-7　DHCP スヌーピングを使用した DHCP スターベーション攻撃の防止



利点

DHCP スヌーピングは、単一のデバイスが、特定の範囲内のすべての IP アドレスを取得するのを防止します。

欠点

この機能が正しく設定されていないと、認定ユーザの IP アドレスが拒否される場合があります。

DHCP スヌーピング：バインディング情報

DHCP スヌーピングには、DHCP サーバから正常に IP アドレスを取得する、信頼されていないポートの DHCP バインディング情報を記録するという機能もあります。バインディング情報は、Cisco Catalyst スイッチ上のテーブルに記録されます。DHCP バインディング テーブルには、各バインディング エントリの IP アドレス、MAC アドレス、リース長、ポート、および VLAN 情報が格納されます。DHCP スヌーピングから取得されたバインディング情報は、DHCP サーバで設定された DHCP バインディング期間（つまり、DHCP リース時間）の間、有効です。DHCP バインディング情報は、ARP 応答を、DHCP でバインディングされているアドレスに限定する目的で、Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）の動的エントリを作成するときに使用されます。DHCP バインディング情報は、IP パケットの送信元を、DHCP でバインディングされたアドレスに限定するために、IP ソース ガードでも使用されます。

DHCP スヌーピングのために各タイプのスイッチに格納できるバインディング テーブル エントリには、最大制限があります（この制限を判別するには、使用するスイッチの製品マニュアルを参照してください）。スイッチのバインディング テーブル内のエントリ数が気になる場合は、バインディング テーブルのエントリがより早くタイムアウトになるように、DHCP 範囲のリース時間を短縮できます。リースが期限切れになるまで、これらのエントリは DHCP バインディング テーブルに残されます。言

い換えると、エンド ステーションがそのアドレスを持っていると DHCP サーバが判断する限り、これらのエントリは DHCP スヌーピング バインディング テーブルに残されます。ワークステーションまたは電話機を切断しても、これらのエントリはポートから除去されません。

Cisco Unified IP Phone がポートに接続されており、それを別のポートに移動した場合、DHCP バインディング テーブルには、同じ MAC アドレスと IP アドレスを持つがポートが異なっている 2 つのエントリが含まれることがあります。この動作は、通常の動作と見なされます。

ダイナミック ARP インスペクションの要件

Dynamic Address Resolution Protocol（ARP）Inspection（DAI; ダイナミック ARP インスペクション）は、ルータのスイッチに接続されたデバイスに対する Gratuitous ARP 攻撃を防止するために、スイッチで使用される機能です。ダイナミック ARP はすでに説明した電話機の Gratuitous ARP 機能と似ていますが、LAN 上のすべてのデバイスを保護するので、単なる電話機の機能ではありません。

基本的な機能である Address Resolution Protocol（ARP）を使用すると、ステーションで MAC アドレスを ARP キャッシュ内の IP アドレスにバインドできるようになり、これにより 2 つのステーションが LAN セグメント上で通信可能になります。ステーションは、ARP 要求を 1 つの MAC ブロードキャストとして送出します。要求に含まれる IP アドレスを所有するステーションは、要求元のステーションに、ARP 応答を（IP アドレスと MAC アドレスと共に）送ります。要求元のステーションは、その応答を、ライフタイムの制限がある ARP キャッシュにキャッシュします。ARP キャッシュのデフォルトのライフタイムは、Microsoft Windows では 2 分間、Linux では 30 秒間、Cisco IP Phone では 40 分です。

また ARP は、Gratuitous ARP と呼ばれる機能を提供します。Gratuitous ARP（GARP）は、要求がなくても送信される ARP 応答です。通常の使用法では、MAC ブロードキャストとして送信されます。GARP メッセージを受信する、LAN セグメント上のすべてのステーションは、この非請求 ARP 応答をキャッシュに入れます。この非請求 ARP 応答により、送信者が、GARP メッセージに含まれる IP アドレスのオーナーであることが認定されます。Gratuitous ARP には、障害時に別のステーションのアドレスを引き継ぐ必要があるステーションを正当に使用します。

ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることができません。Ettercap は、プライベートな GARP メッセージを 30 秒ごとに繰り返し送信することにより、ARP ポイズニングを有効な状態に保持します。

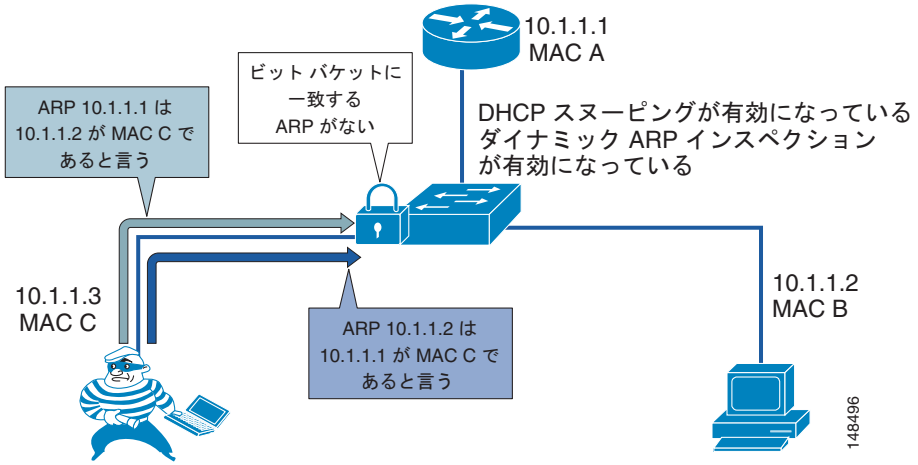
Dyamic ARP Inspection（DAI; ダイナミック ARP インスペクション）は、信頼されていない（またはユーザ報告の）ポートからのすべての ARP 要求および応答（Gratuitous または非 Gratuitous）を検査して、それらが ARP オーナーからのものであることを確認するために使用します。ARP オーナーとは、ARP 応答に含まれている IP アドレスに一致する、DHCP バインディングが置かれているポートのことです。DAI 信頼済みポートからの ARP パケットは検査されず、それぞれの VLAN にブリッジされます。

DAI の使用

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP インスペクション用のアクセス コントロール リスト（ACL）を作成する必要があります（図 4-8 を参照）。DHCP スヌーピングと同様、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして

定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。DAI を有効化する前に DHCP スヌーピングを有効化しないと、VLAN 内のいずれのデバイスも、ARP を使用して、デフォルト ゲートウェイを含む VLAN 内の他のデバイスに接続できません。その結果、VLAN 内のすべてにデバイスに対するサービスを、自ら拒否することになります。

図 4-8　　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



DAI のユーザにとって DHCP スヌーピング バインディング テーブルは重要なので、バインディング テーブルのバックアップを取ることは重要です。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、ファイル転送プロトコル（FTP）、リモート コピー プロトコル（RCP）、スロット 0、およびトリビアル ファイル転送プロトコル（TFTP）にバックアップできます。DHCP スヌーピング バインディング テーブルをバックアップしないと、スイッチのリブート中に、Cisco Unified IP Phone でデフォルト ゲートウェイとのコンタクトが失われる場合があります。例として、DHCP スヌーピング バインディング テーブルをバックアップせず、インラインパワーの代わりに電源アダプタを使用して Cisco Unified IP Phone を使用している場合を想定します。この場合、リブートの後にスイッチがバックアップされると、電話機用の DHCP スヌーピング バインディング テーブル エントリが存在しないので、電話機はデフォルト ゲートウェイと通信できません。これを回避するには、DHCP スヌーピング バインディング テーブルのバックアップを取り、電話機からトラフィックが流れ始める前に古い情報をロードする必要があります。

利点

DAI を使用すると、攻撃者がネットワーク内で ARP ベースの攻撃を仕掛け、レイヤ 2 で攻撃者に隣接する人々の間のトラフィックを妨害または探知するのを防止できます。

欠点

この機能が正しく設定されていないと、認定ユーザへのネットワーク アクセスが拒否される場合があります。DHCP スヌーピング バインディング テーブルにデバイスのエントリがない場合、そのデバイスでは、ARP を使用してデフォルト ゲートウェイに接続できず、そのためトラフィックを送信できません。固定 IP アドレスを使用する場合、これらのアドレスを DHCP スヌーピング バインディング テーブルに手動で入力する必要があります。リンクがダウンのときに、DHCP を再度使用して IP アドレスを取得することをしないデバイスがある場合（一部の UNIX または Linux マシンはこのように動作します）、DHCP スヌーピング バインディング テーブルをバックアップする必要があります。

802.1X ポート ベースの認証

802.1X 認証機能は、Cisco Unified IP Phone のデバイス クレデンシャルの、ネットワークへのアクセス権を与える前に行う識別と検証に使用できます。802.1X は、エンド デバイスと RADIUS サーバの間の相互作用を行う MAC レイヤ プロトコルです。このプロトコルは、Extensible Authentication Protocol（EAP）over LAN（EAPOL）をカプセル化し、エンド デバイスとスイッチの間での認証メッセージの転送を行います。802.1X 認証プロセスでは、Cisco Unified IP Phone は、802.1X サプリカントとして機能し、ネットワークにアクセスするための要求を開始します。オーセンティケータとして機能する Cisco Catalyst Switch は、その要求を認証サーバに渡し、その電話にネットワークへのアクセスを許可するかまたはその電話からのアクセスを制限するかのいずれかを行います。

802.1X は、Cisco Unified IP Phone に接続されているデータ デバイスの認証にも使用できます。Cisco Unified IP Phone では EAPOL パススルー メカニズムが使用され、これによって、ローカルに接続された PC が 802.1X オーセンティケータに EAPOL メッセージを渡すことが可能になります。音声 VLAN 上の 1 つのデバイスとデータ VLAN 上の複数の認証されたデバイスに許可を与えるには、Cisco Catalyst Switch のポートをマルチ認証モードで設定する必要があります。

802.1X 機能設定のサポートを確認するには、Cisco Unified IP Phone および Cisco Catalyst Switch の製品マニュアルを参照してください（http://www.cisco.com）。

（注）　接続されているデータ デバイスを認証するよりも前に IP 電話を認証することを推奨します。

利点

マルチ認証モードでは、アクセスが承認されたときに認証サーバから返された属性に基づいて、認証されたデバイスをデータ VLAN か 音声 VLAN のいずれかに割り当てます。802.1X ポートは、データ ドメインと音声ドメインに分けられます。

マルチ認証モードでは、802.1x ポート上でゲスト VLAN を有効にできます。スイッチは、認証サーバがその EAPOL ID フレームへの応答を受信しなかった場合、およびクライアントが EAPOL パケットを送信しなかった場合に、エンド クライアントをゲスト VLAN に割り当てます。これにより、Cisco IP Phone に接続されていて 802.1X をサポートしていないデータ デバイスをネットワークに接続することが可能になります。

欠点

スイッチ ポートがマルチ ホスト モードになっている場合は、IP 電話用に音声 VLAN を設定しなければなりません。Cisco Attribute-Value（AV; 属性 - 値）ペア属性を **device-traffic-class=voice** という値で送信するように RADIUS サーバを設定する必要があります。この値がないと、スイッチは、IP 電話をデータ デバイスとして扱います。

RADIUS サーバからのダイナミック VLAN 割り当ては、データ デバイスにしかサポートされません。

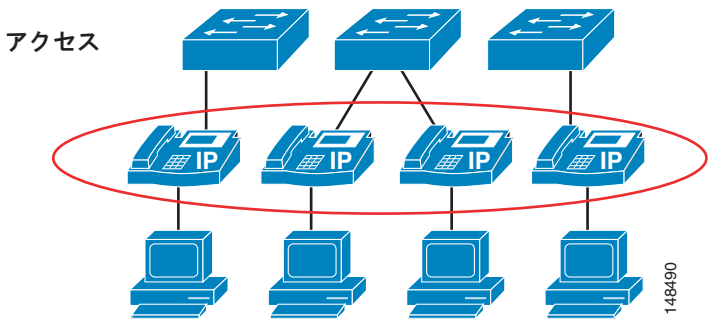
ポート上でデータ デバイスまたは音声デバイスが検出されると、その MAC アドレスは認証が成功するまではブロックされます。認証に失敗した場合、その MAC アドレスのブロックは 5 分間継続します。

音声 VLAN が設定されており、すでに Cisco IP Phone が接続されているアクセス ポート上で 802.1x 認証を有効にすると、電話が最大 30 秒間スイッチとの接続を失います。

電話機のセキュリティ

Cisco Unified IP Phone には、IP テレフォニー ネットワーク上のセキュリティを強化するための組み込み型の機能があります。これらの機能を電話機単位で有効または無効にして、IP テレフォニー配置のセキュリティを強化できます。セキュリティ ポリシーは、電話機の配置に応じて、これらの機能を有効にする必要があるかどうか、および有効にする必要がある場所を判別するのに役立ちます（図 4-9 を参照）。

図 4-9　　電話機レベルでのセキュリティ



次のセキュリティに関する留意点は IP 電話機に適用されます。

- 「電話機の PC ポート」（P.4-17）
- 「PC Voice VLAN へのアクセス」（P.4-18）
- 「電話機経由の Web アクセス」（P.4-19）
- 「ビデオ機能」（P.4-19）
- 「アクセス設定」（P.4-19）
- 「電話機の認証および暗号化」（P.4-20）
- 「IP Phone の VPN クライアント」（P.4-21）

電話機のセキュリティ機能の設定を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の電話機モデルでそれらの機能が使用可能であることを確認してください。

http://www.cisco.com/en/US/products/sw/voicesw/index.html

電話機の PC ポート

電話機は、一般的に PC が接続される電話機背面のポートのオン / オフを切り替えることができます。この機能は、そのタイプの制御が必要な場合に、ネットワークにアクセスするためのコントロール ポイントとして使用できます。

セキュリティ ポリシーおよび電話機の配置状況によっては、特定の電話機の背面にある PC ポートを無効にする必要があります。このポートを無効にすると、電話機の背面にデバイスを接続したり、電話機自体を介してネットワークにアクセスしたりできなくなります。ロビーのような一般的なエリアに設置した電話機の場合、通常はポートを無効にします。ロビーでは物理的なセキュリティが非常に弱いため、ほとんどの企業では、制御されていないポートから不特定のユーザがネットワークにアクセスするのを許可しません。セキュリティ ポリシーで、電話機の PC ポートを経由してデバイスがネットワークにアクセスするのを許可しない場合は、通常の作業エリアに設置した電話機でも、ポートを無効にすることがあります。配置された電話機のモデルによっては、Cisco Unified Communications Manager

（Unified CM）は、電話機の背面の PC ポートを無効にできます。この機能の有効化を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の Cisco Unified IP Phone モデルでこの機能がサポートされていることを確認してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

PC Voice VLAN へのアクセス

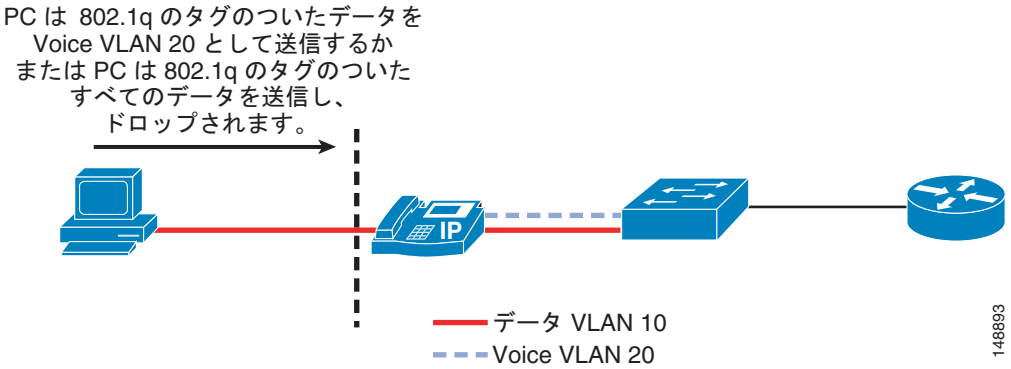
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して Voice VLAN にアクセスすることは許可されません。設定している電話機に応じて、この機能は 2 つの方法のいずれかで動作します。高機能の電話機では、電話機の背面の PC ポートに着信する Voice VLAN を宛先とした、すべてのトラフィックをブロックします。図 4-10 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

現在、アクセス ポートからの 802.1q タギングは、通常は使用しません。この機能が、電話機のポートに接続された PC の要件に含まれている場合、802.1q タグ付きパケットが電話機を通過するのを許可する電話機を使用する必要があります。

電話機の PC Voice VLAN Access 機能の設定を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の電話機モデルでそれらの機能が使用可能であることを確認してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

図 4-10　電話機の PC ポートから Voice VLAN へのトラフィックのブロック



電話機経由の Web アクセス

各 Cisco Unified IP Phone には、デバッグを実行したり管理目的で電話機のリモート ステータスを確認したりするのに役立つ、Web サーバが組み込まれています。Web サーバは、電話機が、Cisco Unified Communications Manager（Unified CM）から電話機にプッシュされたアプリケーションを受信するのを可能にします。この Web サーバへのアクセスは、Unified CM 設定の Web Access 機能を使用して、電話機で有効または無効にできます。この設定は、グローバルで行うことも、電話機ごとに有効または無効にすることもできます。

Web サーバがグローバルで無効だが、デバッグの参考として必要な場合、Unified CM の管理者は、電話機のこの機能を有効にする必要があります。この Web ページにアクセスする機能は、ネットワークの ACL で制御できます。ネットワーク オペレータは、この機能を使用して、必要なときに Web ページにアクセスできます。

Web アクセス機能を無効にすると、電話機は、Unified CM からプッシュされるアプリケーションを受信できません。

ビデオ機能

Cisco Unified Video Advantage が正しく動作するには、PC ポートとビデオ機能の両方を有効にする必要があります。その他の設定は無効にしてもかまいません。Device Security Mode は、Cisco Unified Video Advantage の使用中でも指定どおりに動作しますが、Cisco Unified Video Advantage 自体は Cisco Audio Session Tunnel（CAST）プロトコルまたはその RTP メディア トラフィックの認証または暗号化をサポートしません。IP Phone が Authenticated モードのときは、この電話機と Unified CM の間の Skinny Client Control Protocol（SCCP）シグナリングは認証されますが、電話機と Cisco Unified Video Advantage の間の CAST シグナリングは認証されません。同様に、電話機が Encrypted モードのときは、電話機間のオーディオ ストリームは暗号化されますが、Cisco Unified Video Advantage クライアント間のビデオ ストリームは暗号化されません。暗号化されたコール中であることを電話機上のアイコンが示しているように見える場合でも、ビデオ チャネルが暗号化されないことをユーザに通知しておく必要があります。

アクセス設定

各 Cisco Unified IP Phone にはネットワーク設定ページがあり、そのページには、電話機が動作するのに必要な多くのネットワーク要素や詳細情報がリストされます。攻撃者はこの情報を使用して、電話機の Web ページに表示される情報の一部と共に、ネットワーク上で調査を開始できます。たとえば、攻撃者は設定ページを参照して、デフォルト ゲートウェイ、TFTP サーバ、および Unified CM の IP アドレスを判別できます。これらの断片的な情報が、音声ネットワークにアクセスしたり、音声ネットワーク内のデバイスを攻撃したりするのに使用される場合があります。

このアクセスを電話機ごとに無効にすることにより、エンド ユーザまたは攻撃者が、Unified CM IP アドレスや TFTP サーバ情報などの追加情報を取得するのを防止できます。電話機設定ページへのアクセスを無効にすると、エンド ユーザは、スピーカー ボリューム、連絡先、呼び出しタイプなど、通常は制御可能な多くの電話機設定を変更できなくなります。電話機インターフェイスについてエンド ユーザに課される制限により、このセキュリティ機能を使用することが現実的ではない場合があります。

電話機設定ページの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

電話機の認証および暗号化

Unified CM では、音声システム内の電話機に対して複数のレベルのセキュリティを実現するように設定できます。ただし、電話機でこれらの機能がサポートされている必要があります。導入済みのセキュリティ ポリシー、電話機の配置、および電話機サポートに応じて、社内の必要に合せてセキュリティを設定できます。

特定のセキュリティ機能に対する Cisco Unified IP Phone モデルのサポート状況の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

電話機および Unified CM クラスタでセキュリティを有効にするには、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Security Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Unified CM でセキュリティ機能が正しく設定されている場合、サポートされているすべての電話機で、次の機能を使用できます。

- 完全性：この機能が有効な場合は、電話機に対する TFTP ファイル操作を許可しませんが、トランスポート レイヤ セキュリティ（TLS）シグナリングを許可します。
- 認証：電話機のイメージは、Unified CM から電話機に対して認証され、デバイス（電話機）は Unified CM に対して認証されます。電話機と Unified CM の間のすべてのシグナリング メッセージは、認可されているデバイスから送信されるときに検証されます。
- 暗号化：サポートされているデバイスで、盗聴を防止するためシグナリングとメディアを暗号化できます。
- Secure Real-time Transport Protocol（SRTP）: Cisco IOS ゲートウェイでサポートされています。当然、電話機間でもサポートされています。Cisco Unity もボイスメールのための SRTP をサポートしています。

Unified CM は、2 つの Cisco Unified IP Phone の間のコールの、認証、完全性、および暗号化をサポートしていますが、すべてのデバイスまたは電話機についてサポートしているわけではありません。ご使用のデバイスがこれらの機能をサポートしているかどうかを判別するには、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

Unified CM では ID を保護し、暗号化を有効にするために証明書を使用します。証明書には、Manufacturing Installed Certificate（MIC; 製造元でインストールされる証明書）または Locally Significant Certificate（LSC; ローカルで有効な証明書）のどちらかを使用できます。MIC はすでにプレインストールされていて、LSC は Unified CM の Cisco Certificate Authority Proxy Function（CAPF）によりインストールされます。Unified CM は、自己署名証明書を作成しますが、PKCS #10 Certificate Signing Request（CSR; 証明書署名要求）を使用した第三者 Certificate Authority（CA; 認証局）による証明書の署名もサポートされます。第三者 CA を使用する場合、CA により CAPF に署名できますが、電話機の LSC は、その後も CAPF により生成されます。

クラスタを混合モードで設定すると、自動登録は動作しません。混合モードは、デバイス認証に必要なモードです。クラスタにデバイス認証が存在しない場合、つまり、Cisco Certificate Trust List（CTL）クライアントがインストールおよび設定されていない場合、シグナリングまたはメディア暗号化の実装はできません。IP テレフォニー トラフィックがファイアウォールおよび Network Address Translation（NAT; ネットワーク アドレス変換）を通過するのを可能にするアプリケーション レイヤ プロトコル検査および Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）も、シグナリングが暗号化されていると動作しません。暗号化されたメディアでは、一部のゲートウェイ、電話機、または会議はサポートされません。

メディアの暗号化によって、コールのレコーディングとモニタリングはより困難で高価になります。VoIP の問題のトラブルシューティングも難しくなります。

IP Phone の VPN クライアント

VPN クライアントが組み込まれた Cisco Unified IP Phone には、ネットワーク外の電話機を企業内の Unified Communications ソリューションに接続するためのセキュアなオプションがあります。この機能では、外部 VPN ルータは必要なく、レイヤ 3 のセキュア通信トンネルと、配置されたロケーションにある電話機と企業ネットワーク間の非信頼ネットワーク経由のトラフィックの増大が提供されます。

Cisco Unified IP Phone 内の VPN クライアントは、Cisco SSL VPN テクノロジーを使用しており、Cisco ASA 5500 シリーズ VPN ヘッドエンドと Cisco IOS SSL VPN ソフトウェア機能を備えた Cisco サービス統合型ルータの両方に接続できます。音声トラフィックは UDP で搬送され、Datagram Transport Layer Security（DTLS）プロトコルによって保護されます。統合された VPN トンネルは、音声および IP Phone Service だけに適用されます。PC ポートに接続された PC はこのトンネルを使用できず、PC からのトラフィック用に独自の VPN トンネルを確立する必要があります。

VPN クライアントが組み込まれた電話機の場合、最初に、VPN コンセントレータ アドレス、VPN コンセントレータ クレデンシャル、ユーザまたは電話機 ID、クレデンシャル ポリシーなどの VPN 設定パラメータを使用して電話機を設定する必要があります。この情報は機密であるため、電話機が非信頼ネットワーク経由での接続を試行する前に、電話機を企業ネットワーク内でプロビジョニングする必要があります。最初に電話機を企業ネットワーク内でステージングしないで電話機を配置することは、サポートされていません。

ユーザは、電話機のユーザ インターフェイスの設定メニューで、VPN トンネルの確立を有効または無効にできます。VPN トンネルの確立が有効の場合、電話機は VPN トンネルの確立を開始します。電話機は、冗長性を持たせるために最大 3 つの VPN コンセントレータを使用して設定できます。VPN クライアントは、ロード バランシング メカニズムとして、VPN コンセントレータから他の VPN コンセントレータへのリダイレクションをサポートします。

VPN クライアント用の電話機を設定する手順については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

（注）　VPN クライアントをサポートするには、電話機でファームウェア リリース 9.0(2) 以上が実行されている必要があります。この機能は、Cisco Unified CM 8.*x* に登録されたファームウェアのバージョンが 9.0(2) の Cisco Unified IP Phones 79*x*2 および 79*x*5 上でのみ使用できます。IPv4 アドレスを使用してプロビジョニングされた電話機だけが、VPN クライアント機能でサポートされます。

Quality of Service（QoS）

Quality of Service（QoS）は、企業ネットワーク用のすべてのセキュリティ ポリシーで、重要な部分を占めます。一般的に、QoS はネットワーク内のトラフィック重要度の設定と考えられていますが、ネットワークに入ることが許可されるデータの量も制御します。Cisco スイッチの場合、電話機からイーサネット スイッチにデータが送られるときのコントロール ポイントはポート レベルにあります。アクセス ポートでネットワークのエッジに適用される制御が多いほど、ネットワークでデータを集約するときに発生する問題は少なくなります。

ロビーに設置された電話機の例ですでに説明したとおり、アクセス ポート レベルでトラフィックの十分なフロー コントロールを提供することにより、攻撃者が、ロビー内のそのポートから DoS 攻撃を仕掛けるのを防止できます。QoS 設定ではポートに送信されたトラフィックが最大レートを超えることが許可されていますが、トラフィックは Scavenger Class にリマークされているので、この例の設定は、それほどアグレッシブではありません。よりアグレッシブな QoS ポリシーを使用すると、ポリシーの最大制限を超える量のトラフィックはポートでドロップされ、その「不明な」トラフィックがネットワークに入ることはありません。IP テレフォニー データにエンドツーエンドで高い優先度を与えるには、ネットワーク全体で QoS を有効にする必要があります。

QoS の詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章、および次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design（SRND）Guide*』を参照してください。

http://www.cisco.com/go/designzone

利点

QoS を使用すると、ネットワーク内のトラフィックの優先度だけでなく、任意の特定のインターフェイスを通過できるトラフィックの量も制御できます。ネットワーク内の音声 QoS をアクセス ポート レベルで配置するのに役立つ、Cisco Smartports テンプレートが作成されました。

厳しい QoS ポリシーでは、トラフィック レートを制御することによって、ネットワーク内の DoS 攻撃を制御および防止できます。

欠点

QoS 設定が標準的な Cisco Smartports テンプレートの範囲外の場合、大規模な IP テレフォニー配置では、設定が複雑になり管理が難しくなることがあります。

アクセス コントロール リスト

この項では、Access Control List（ACL; アクセス コントロール リスト）、および音声データの保護における ACL の使用方法について説明します。

VLAN アクセス コントロール リスト

VLAN アクセス コントロール リスト（ACL）を使用すると、ネットワーク上を流れるデータを制御できます。Cisco スイッチには、VLAN ACL 内でレイヤ 2 ～ 4 を制御する機能があります。ネットワーク内のスイッチのタイプによっては、VLAN ACL を使用して、特定の VLAN に流入または流出するトラフィックをブロックできます。また、VLAN ACL を使用して VLAN 内のトラフィックをブロックし、VLAN 内のデバイス間で発生する処理を制御することもできます。

VLAN ACL を配置する計画がある場合、IP テレフォニー ネットワーク内で使用される各アプリケーションで電話機が正しく動作するようにするにはどのポートが必要かを検証する必要があります。通常、任意の VLAN ACL は、電話機が使用する VLAN に適用されます。これにより、アクセス ポートで、アクセス ポートに接続されているデバイスにできるだけ近い制御ができるようになります。

VLAN ACL の設定については、次の製品マニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_installation_and_configuration_guides_list.html

- Cisco Catalyst 4500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

- Cisco Catalyst 6500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

VLAN ACL を適用する方法の詳細については、次のマニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_installation_and_configuration_guides_list.html

- Cisco Catalyst 4500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

- Cisco Catalyst 6500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

利点

ACL は、VLAN に入るまたは VLAN から出るネットワーク トラフィックを制御する機能、および VLAN 内でトラフィックを制御する機能を提供します。

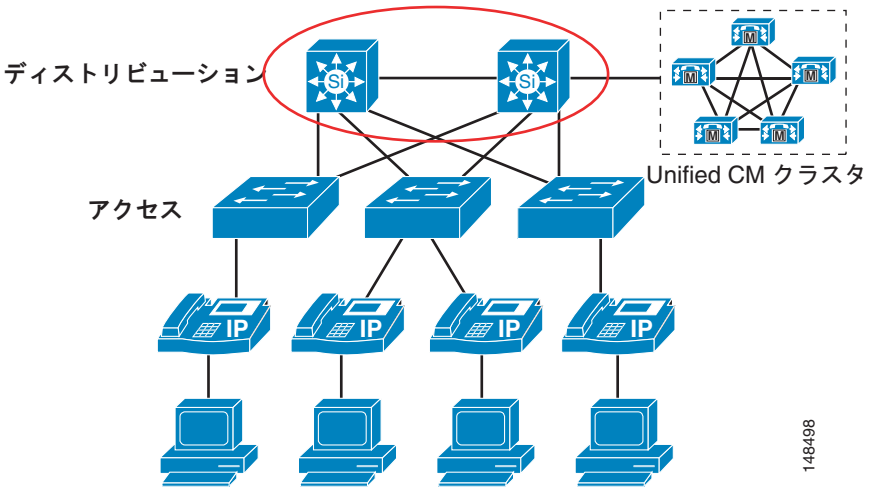
欠点

VLAN ACL を、モバイル性の高いアクセスポート レベルで配置および管理するのは非常に困難です。これらの管理上の問題があるので、ネットワークのアクセス ポートに VLAN ACL を配置するときは注意が必要です。

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 4-11 を参照）。

図 4-11　レイヤ 3 のルータ ACL



レイヤ 3 に配置可能な ACL には、多くのタイプがあります。一般的なタイプの説明と例については、次の Web サイトで入手可能な『*Configuring Commonly Used IP ACLs*』を参照してください（シスコ パートナーとしてのログインが必要）。

http://cisco.com/en/US/partner/tech/tk648/tk361/technologies_configuration_example09186a0080100548.shtml

導入済みのセキュリティ ポリシーに応じて、レイヤ 3 ACL は、非 Voice VLAN からの IP トラフィックがネットワーク内の音声ゲートウェイにアクセスするのを禁止するという単純な設定にも、他のデバイスが IP テレフォニー デバイスと通信するために使用する個別のポートや時間帯を制御するという詳細な設定にもできます。ソフトフォンが導入されていないと仮定すると、Unified CM、音声ゲートウェイ、電話機、および音声専用サービスで使用される他の任意の音声アプリケーションに対する、すべてのトラフィック（IP アドレス別、または IP 範囲別）をブロックするための ACL を書き込むことができます。この方法により、レイヤ 3 ACL を、レイヤ 2 または VLAN ACL よりも簡素化できます。

利点

レイヤ 3 では、より簡単に ACL を管理および配置できます。レイヤ 3 は、ネットワーク内の音声データおよび他の非音声データにコントロールを適用できる最初の機会です。

欠点

ACL が高精度および詳細になると、ネットワーク内のポート使用法の変更が原因で、音声だけでなく、ネットワーク内の他のアプリケーションも遮断される場合があります。

ネットワークにソフトフォンがある場合、電話機への Web アクセスが許可されている場合、または Attendant Console を使用するか、Voice VLAN サブネットへのアクセスが必要な他のアプリケーションを使用する場合、ACL の配置と制御はさらに難しくなります。

ファイアウォール

ファイアウォールを ACL と組み合せて使用すると、IP テレフォニー デバイスと通信することが許可されていないデバイスから、音声サーバおよび音声ゲートウェイを保護できます。IP テレフォニーで使用するポートには動的な特性があるので、ファイアウォールを配置すると、IP テレフォニー通信で必要な広範囲のポートの開放を制御するのに役立ちます。ファイアウォールを導入するとネットワークの設計が複雑になるので、適正と見なされるトラフィックが通過するのを許可し、ブロックする必要があるトラフィックをブロックするようにファイアウォール、およびファイアウォールの周辺デバイスを配置および設定するときは、細心の注意が必要です。

IP テレフォニー ネットワークには、一意のデータ フローがあります。電話機はクライアント/サーバ モデルを使用してコール セットアップ用のシグナリングを生成し、Unified CM はそのシグナリングを使用して電話機を制御します。IP テレフォニー RTP ストリームのデータ フローは、ピアツーピア ネットワークに似ており、電話機またはゲートウェイは、RTP ストリームを介して相互に直接通信します。ファイアウォールがシグナリング トラフィックを検査できるようシグナリング フローがファイアウォールを経由しないようにする場合、ファイアウォールが、会話用の RTP ストリームを許可するのにどのポートを開放する必要があるかを判別できないので、RTP ストリームがブロックされることがあります。

正しく設計されたネットワークにファイアウォールを配置すると、すべてのデータがそのデバイスを経由するように強制できるので、キャパシティとパフォーマンスについて考慮する必要があります。パフォーマンスには、遅延の量が関係しています。ファイアウォールに高い負荷がかかっている場合やファイアウォールが攻撃されている場合は、1 つのファイアウォールにより遅延の量が増大することがあります。IP テレフォニーの配置に関する原則では、ファイアウォールの通常使用時の CPU 使用率を 60% 未満に抑えます。CPU の使用率が 60% を超えると、IP Phone、コール セットアップ、および登録に影響が出る可能性が高まります。CPU の使用率が継続的に 60% を超えると、登録済みの IP Phone は影響を受け、進行中のコールの品質は低下し、新しいコールのコール セットアップは問題を抱えます。CPU 使用率が 60% を超えた状態が続くと、最悪の場合、電話機の登録解除が始まります。このことが発生すると、電話機は Unified CM への再登録を試みるようになり、ファイアウォールの負荷はさらに増大します。この状態が発生すると、結果的に、登録解除と Unified CM への再登録の試行を繰り返す電話機の連続ブラックアウトが発生します。ファイアウォールの CPU 使用率が継続的に 60% 未満に落ち着くまで、この連続ブラックアウトは続き、すべてまたはほとんどの電話機が影響を受けます。現在、ネットワーク内で Cisco ファイアウォールを使用している場合、ネットワークに IP テレフォニー トラフィックを追加するときは、トラフィックが悪影響を受けないように、CPU 使用率を注意深くモニタしてください。

ファイアウォールを配置する方法はいくつもあります。この項では、ルーテッドおよびトランスペアレントの両方のシナリオにおける、アクティブ/スタンバイ モードの Cisco Adaptive Security Appliance（ASA）について集中的に説明します。この項で説明する各設定は、ファイアウォール設定の音声セクション内で、シングル コンテキスト モードで設定されたものです。

（注） Cisco Firewall Services Module（FWSM）は、Cisco Unified Communications 8.*x* アプリケーションではサポートされません。ネットワークで FWSM を使用する場合は、ACL を指定して、これらのアプリケーションのトラフィックを許可する必要があります。

すべての Cisco ファイアウォールは、マルチ コンテキスト モードまたはシングル コンテキスト モードのいずれかで実行できます。シングル コンテキスト モードでは、ファイアウォールは、ファイアウォールを通過するすべてのトラフィックを制御する単一のファイアウォールを指します。マルチ コンテキスト モードでは、ファイアウォールは複数の仮想ファイアウォールを指します。これらのコンテキストまたは仮想ファイアウォールにはそれぞれ独自の設定があり、異なるグループまたは管理者が制御できます。ファイアウォールに新しいコンテキストを追加するたびに、ファイアウォールの負荷およびメモリ要件は大きくなります。新しいコンテキストを配置するときは、音声 RTP ストリームが悪影響を受けないように、CPU 要件を満たしていることを確認してください。

Adaptive Security Appliance では、Unified Communications アプリケーション サーバおよびエンドポイントの IPv6 トラフィックのアプリケーション インスペクションのサポートは限定されています。ASA がネットワークに配置されている場合、Unified Communications には IPv6 を使用しないことを推奨します。

（注）　ASA のペイロード暗号化なしモデルでは、Unified Communications の機能が無効にされています。

ファイアウォールの全般的な利点

ファイアウォールは、ネットワーク上で実行されるアプリケーションのために、ネットワークのセキュリティ コントロール ポイントを提供します。トラフィックがファイアウォールを通過する場合、ファイアウォールは、IP テレフォニー会話用にポートを動的に開く機能も提供します。

アプリケーション インスペクション機能を使用すると、ファイアウォールを通過するトラフィックがファイアウォールで検査され、そのトラフィックが、ファイアウォールで予期されていたタイプのトラフィックかどうかが判別されます。たとえば、HTTP トラフィックが本当に HTTP トラフィックなのか、あるいは攻撃なのかが判別されます。それが攻撃だった場合、ファイアウォールはそのパケットをドロップし、そのパケットがファイアウォールの背後にある HTTP サーバに到達するのを許可しません。

ファイアウォールの全般的な欠点

ファイアウォールのアプリケーション レイヤ プロトコル検査では、すべての IP テレフォニー アプリケーション サーバまたはアプリケーションがサポートされているわけではありません。そのようなアプリケーションの一部として、Cisco Unity ボイスメール サーバ、Cisco Unified Attendant Console、Cisco Unified Contact Center Enterprise、および Cisco Unified Contact Center Express があります。トラフィックがファイアウォールを経由して流れるのを許可するため、これらのアプリケーション用の ACL を書き込むことができます。

（注）　ファイアウォールに備えられたフェールオーバーのタイマーは、デフォルトで高い値が設定されています。フェールオーバー時にファイアウォールを通過する音声 RTP ストリームに影響するのを防ぐため、タイマー設定を 1 秒以下に設定することを推奨します。設定を変更し、フェールオーバーが発生すると、ファイアウォールのフェールオーバーが短縮され RTP ストリームが影響するフェールオーバー時間が削減されるため、RTP ストリームが影響を受ける時間が低減されます。

異なる Unified Communications コンポーネントの間にファイアウォールを設置する場合、コンポーネント間の通信に使用されるすべてのプロトコルについてアプリケーション インスペクションを有効にする必要があります。リモート エージェントの電話とスーパーバイザの電話の間にファイアウォールを設置すると、Unified Communications Manager のサイレント モニタリングなどの機能によって使用されるコール フローのシナリオで、アプリケーション インスペクションが失敗することがあります。

TCP を使用する Unified Communications デバイス（Cisco Unified Communications Manager など）は、パケット損失の場合にデータの転送を高速化するために、TCP SACK オプションをサポートしています。ただし、すべてのファイアウォールが TCP SACK オプションをサポートしているわけではありません。その場合、Unified Communications デバイスが TCP SACK オプションを使用しようとすると、そのようなファイアウォールを経由してデバイス間で確立された TCP セッションに問題が発生し、TCP セッションは失敗する場合があります。そのため、ファイアウォールは TCP SACK オプションを完全にサポートしている必要があります。サポートできない場合、ファイアウォールでは、スリーウェイ ハンドシェイク中に TCP パケットを変更でき、エンドポイントが TCP SACK オプションを使用しないようにこのオプションのサポートを無効にできることが必要です。

ネットワーク上で実行しているアプリケーションがネットワーク内のファイアウォールのバージョンでサポートされているかどうか、および ACL を書き出す必要があるかどうかを判別するには、次の Web サイトで入手可能な適切なアプリケーション マニュアルを参照してください。

http://www.cisco.com

ルーテッド ASA

ルーテッド モードの ASA ファイアウォールは、接続されているネットワーク間のルータとして機能します。各インターフェイスには、異なるサブセット上の 1 つの IP アドレスが必要です。シングル コンテキスト モードでは、ルーテッド ファイアウォールは Open Shortest Path First（OSPF）およびパッシブ モードの Routing Information Protocol（RIP）をサポートしています。マルチ コンテキスト モードは、静的ルートのみをサポートしています。ASA バージョン 8.*x* では、Enhanced Interior Gateway Routing Protocol（EIGRP）もサポートされます。拡張するルーティング要件に対するセキュリティ アプライアンスに依存するのではなく、アップストリーム ルータおよびダウンストリーム ルータの拡張ルーティング機能を使用することを推奨します。ルーテッド モードの詳細については、次の Web サイトで入手可能な『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

利点

ルーテッド ASA ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（「トランスペアレント ASA」（P.4-27）を参照）。ルーテッド設定では、ASA 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

欠点

トランスペアレント モードとは異なり、デバイスはネットワークで参照することができ、それが原因で攻撃ポイントになる場合があります。ルーティングの一部はファイアウォールで実行可能なため、ルーテッド ASA ファイアウォールをネットワークに配置すると、ネットワークのルーティングが変更されます。ファイアウォールに存在する、使用する予定のすべてのインターフェイスでは、IP アドレスも使用可能でなければなりません。そのため、ネットワーク内のルータの IP アドレスを変更する必要が生じる場合もあります。ASA ファイアウォールを経由してルーティング プロトコルまたは RSVP を許可する場合、トラフィックが外側（または信頼性が低い）インターフェイスを通過するのを許可するため、ACL を内側（または最も信頼性が高い）インターフェイス上に配置する必要があります。ACL では、最も信頼性が高いインターフェイスから出るのを許可される、その他のすべてのトラフィックも定義する必要があります。

トランスペアレント ASA

ASA ファイアウォールは、レイヤ 2 ファイアウォール（「Bump In The Wire」または「ステルス ファイアウォール」とも呼ばれる）として設定できます。この設定では、ファイアウォールに IP アドレス（管理目的のものを除く）は与えられず、すべてのトランザクションはネットワークのレイヤ 2 で行われます。ファイアウォールはブリッジとして動作しますが、レイヤ 3 のトラフィックは、拡張アクセス リストで明示的に許可しない限り、セキュリティ アプライアンスを通過できません。アクセス リストなしで許可されるトラフィックは、Address Resolution Protocol（ARP）トラフィックだけです。

利点

この設定には、ファイアウォールが動的ルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。ファイアウォールがトランスペアレント モードでも動作するようにするには、静的ルーティングが必要です。

この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。ファイアウォールはルーティング要求を処理しないので、通常は、**inspect** コマンドと全体のトラフィックを使用したときのファイアウォールのパフォーマンスの方が、同じファイアウォール モデルとソフトウェアがルーティングを実行する場合よりも高くなります。

欠点

トランスペアレント モードでは、ルーティングのためにデータを渡す場合、同じファイアウォールをルーテッド モードで使用する場合とは異なり、トラフィックを許可するためにファイアウォールの内側と外側の両方で ACL を定義する必要があります。Cisco Discovery Protocol（CDP）トラフィックは、デバイスが定義済みの場合でも、デバイスを通過することはありません。直接接続される各ネットワークは、同じサブネット上に置かれている必要があります。コンテキスト間でインターフェイスを共有できません。マルチ コンテキスト モードを実行する計画の場合は、追加のインターフェイスを使用する必要があります。そのトラフィックがファイアウォールを通過するのを許可するには、ACL で、ルーティング プロトコルなどのすべての非 IP トラフィックを定義する必要があります。トランスペアレント モードでは QoS はサポートされていません。マルチキャスト トラフィックは、拡張 ACL が設定されているファイアウォールを通過するのを許可されますが、これはマルチキャスト デバイスではありません。トランスペアレント モードでは、VPN 終端はファイアウォールでサポートされていません。ただし、管理インターフェイス用の終端を除きます。

ASA ファイアウォールを経由してルーティング プロトコルまたは RSVP を許可する場合、トラフィックが外側（または信頼性が低い）インターフェイスを通過するのを許可するため、ACL を内側（または最も信頼性が高い）インターフェイス上に配置する必要があります。ACL では、最も信頼性が高いインターフェイスから出るのを許可される、その他のすべてのトラフィックも定義する必要があります。

トランスペアレント モードの詳細については、次の Web サイトで入手可能な『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

（注）　トランスペアレント モードで NAT を使用する場合は、ASA バージョン 8.0(2) 以降が必要です。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa80/release/notes/asarn80.html の『*Cisco ASA 5500 Series Release Notes*』を参照してください。

ASA Unified Communications Proxy 機能

Cisco ASA 5500 シリーズ アプライアンスの Cisco Unified Communications Proxy 機能には、暗号化および境界セキュリティ サービスのための複数のソリューションが含まれています。TLS プロキシ機能は、セキュリティ ポリシーを終了し、内部的に暗号化された Cisco IP エンドポイントに適用します。電話機プロキシ、モビリティ プロキシ、およびプレゼンス フェデレーション セキュリティ サービスは、企業ネットワークとリモート ユーザ、モバイル ソリューション、およびその他の外部ネットワーク間の安全な通信サービスを可能にします。

これらの機能はすべて、Cisco Unified Communications Proxy 領域の下でライセンスされます。この機能のライセンスおよび配置要件の詳細については、次のマニュアルを参照してください。

- 『*Cisco ASA Unified Communications Proxy Licensing Guide*』
  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/at_a_glance_c45-509624.pdf
- 『*Cisco ASA 5500 Series Unified Communications Deployments*』データ シート
  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet0900aecd8073cbbf.html

利点

Cisco ASA Unified Communications Proxy 機能によって、Unified Communications システムと非信頼ネットワークで接続されたエンドポイント間の安全な通信が可能になります。

欠点

Cisco Unified Communications Proxy 機能は、TLS セッションによってライセンスされます。電話機プロキシまたは TLS プロキシの場合、各 IP Phone に Unified CM サーバへの複数の接続がある場合があります。プライマリ Unified CM への 1 つの接続とバックアップ Unified CM への 1 つの接続です。この場合、2 つの TLS セッションが設定されているため、電話機プロキシは 2 つの Unified Communications Proxy セッションを使用します。モビリティ プロキシおよびプレゼンス フェデレーション プロキシの場合、各エンドポイントは 1 つの Unified Communications Proxy セッションを利用します。

Cisco Unified Communications Proxy 機能を有効にするには、キャパシティについて十分に考慮する必要があります。電話機の登録が失われたり、再登録の試行時に他のトラフィックに影響を与えたりしないように、プロキシ セッションの使用中に ASA での CPU 使用率が 60% 前後を下回るようにする必要があります。

ASA TLS プロキシ

この機能によって ASA ファイアウォールに暗号化音声シグナリングをインスペクションする機能が追加されます。エンドポイント デバイスに暗号化シグナリングが設定されている場合はシグナリングをインスペクションできないため、アプリケーション レイヤ ゲートウェイによって NAT フィックスアップなどの機能を実行できません。シグナリングを TLS プロキシ機能経由で送信することで ASA で TLS セッションに参加できます。これにより、ASA はシグナリング ストリームを解読して必要なフィックスアップなど実行した上で再びシグナリングを暗号化します。

ASA ファイアウォールを IP 電話機と ASA ファイアウォールが登録されている Unified CM の間に設置すると TLS プロキシが TLS セッションに挿入されます。暗号化シグナリングが設定された電話機では TLS を電話機と Unified CM のトランスポートとして使用します。TLS プロキシを使用する場合、1 つの電話機登録に対して 2 つの TLS セッションが存在します。1 つは電話機と ASA の間、もう 1 つは ASA と Unified CM の間です。

ASA はシグナリングのインスペクションが可能なため、アプリケーション インスペクション機能を備えた唯一のファイアウォールで、暗号化シグナリングのコールを制御する方法が装備されています。

TLS プロキシは電話機で使用される Certificate Trust List（CTL）に信頼されるエンティティとして追加されています。CTL ファイルには電話機との信頼関係が求められるすべてのサーバを含む 16 のエントリを格納できます。したがって、特定のクラスタで使用できる設定された TLS プロキシ数は Certificate Trust List のエントリ残数によって制限されます。

ASA フォン プロキシ

Cisco ASA フォン プロキシ機能は、安全なリモート アクセスのために Cisco SRTP/TLS 暗号化エンドポイントの終端を有効にします。電話機プロキシでは、VPN リモート アクセス ハードウェアの大規模な配置がなくても、セキュアな電話機の大規模な配置が可能です。エンド ユーザのインフラストラクチャは IP エンドポイントだけであり、VPN トンネルやハードウェアは必要ありません。Cisco ASA フォン プロキシは、Cisco Unified Phone Proxy の代替製品です。

ASA フォン プロキシは、混合モードとノンセキュア モードの両方で Unified CM クラスタをサポートします。ただし、どちらのシナリオでも、暗号化対応のリモート電話機は常に暗号化モードに強制され、シグナリングとメディアは ASA フォン プロキシで終端されます。

電話機がノンセキュアとして設定されるノンセキュア クラスタ モードまたは混合モードでは、ASA フォン プロキシは、電話機からの TLS 接続を終端し、Unified CM への TCP 接続を開始します。プロキシは、リモート IP Phone からのメディアの変換も行います。内部ネットワーク IP Phone に転送する前に、SRTP から RTP に変換します。

内部 IP Phone が認証されるが暗号化は設定されない混合モード クラスタでは、ASA フォン プロキシは Unified CM の TLS 接続を TCP に変換しませんが、SRTP は RTP に変換されます。内部 IP Phone が暗号化済みとして設定された場合は、TLS 接続も SRTP も変換されません。

（注）　ASA フォン プロキシは、VPN トンネル経由で接続している電話機からのパケットのインスペクションをサポートしません。したがって、VPN トンネルによる電話機プロキシ トラフィックの送信はサポートされません。

（注）　ASA フォン プロキシでは、暗号化された TFTP 設定ファイルおよび電話への HTTP トラフィックがサポートされていません。ASA Phone Proxy に接続されている電話は、設定ファイルの暗号化オプションを無効にする必要があります。

ASA がトランスペアレント モードまたはマルチモードで実行されている場合、ASA フォン プロキシはサポートされません。また、ASA フォン プロキシでは Cisco Unified Personal Communicator はサポートされません。

TLS プロキシ機能と ASA フォン プロキシ機能の違いのリストについては、次の Web サイトで入手可能な『*TLS Proxy vs.Phone Proxy*』を参照してください。

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/white_paper_c11-493584.html

ASA モビリティ プロキシ機能

Cisco ASA モビリティ プロキシは、Cisco Unified Mobile Communicator ソフトウェアと Cisco Unified Mobility Advantage サーバ間のセキュアな接続を容易にします。モビリティ プロキシは、Cisco Unified Mobile Communicator ソフトウェアとサーバ間の TLS 接続を代行受信できます。モビリティ プロキシは、Mobile Multiplexing Protocol（MMP）インスペクション エンジンを使用してポリシーを調べてモビリティ トラフィックに適用し、Blackberry、Symbian、および Windows モバイル デバイス上で実行される Cisco Unified Mobile Communicator のプロトコル準拠を強化します。

Cisco Mobility Advantage を使用した配置の場合、ASA をファイアウォールとモビリティ プロキシの両方として使用することを推奨します。ただし、この機能は、既存のファイアウォールを利用して、モビリティ プロキシとしてだけ実装することもできます。

（注）　Cisco ASA バージョン 8.2(*x*) 以降、モビリティ プロキシ アプリケーションに Cisco Unified Communications Proxy ライセンスは不要になりました。

ASA for Unified Presence

このプロキシ機能は、Cisco Unified Presence と Microsoft Office Communications Server（OCS）プレゼンス ソリューション間のセキュアなプレゼンス フェデレーションを促進します。したがって、Cisco Unified Presence ソリューションを含むネットワークで、プレゼンス情報を他の企業とフェデレーションおよび共有することが可能になります。プレゼンス フェデレーション プロキシは、あるネットワーク内の Cisco Unified Presence サーバと別のネットワーク内の Microsoft Access Proxy サーバ間の TLS 接続の TLS プロキシとして実装されます。

ASA Intercompany Media Engine プロキシ

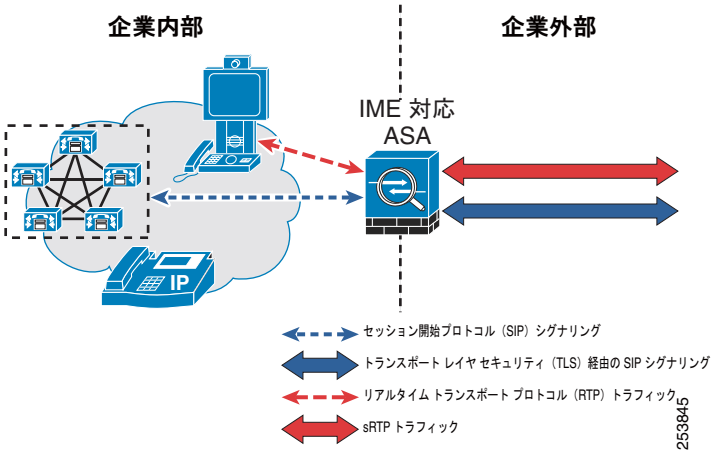
ASA Cisco Intercompany Media Engine（IME）プロキシは、IME コール処理用の Cisco IME ソリューションの必須コンポーネントです。ソリューションの IME コール処理フェーズの詳細については、「Cisco Intercompany Media Engine」（P.5-35）を参照してください。IME 対応 ASA は、非 IME コールのスパム対策ブロッキングなどの境界セキュリティ機能およびフォールバック機能のオーディオ品質モニタリングを提供し、SIP メッセージを検査し、SIP から SIP/TLS および RTP/SRTP への変換のプロキシとして機能します。IME 対応 ASA は接続を終端して再開します。そのことによって SIP メッセージングを検査し、SIP ALG 処理を適用できます。ASA は、Unified CM がセキュアでない場合は SIP/TLS トラフィックを Unified CM に向かう TCP に変換し、Unified CM がセキュアな場合は TLS で接続します。次の配置モデルが IME 対応 ASA に適用されます。

- 基本（インライン）
- オフパス

基本配置

基本（インライン）配置では、IME 機能を使用してインターネット ASA が設定され、Unified CM クラスタからのすべてのインターネット行きのトラフィックは必然的にこの IME 対応 ASA を通過します。図 4-12 に示すように、IME 対応 ASA は企業のエッジにあり、すべての IME 関連 SIP トランク シグナリングおよび音声 / ビデオ RTP メディアをリモート企業にプロキシします。

図 4-12　Intercompany Media Engine ASA の基本（インライン）配置モデル

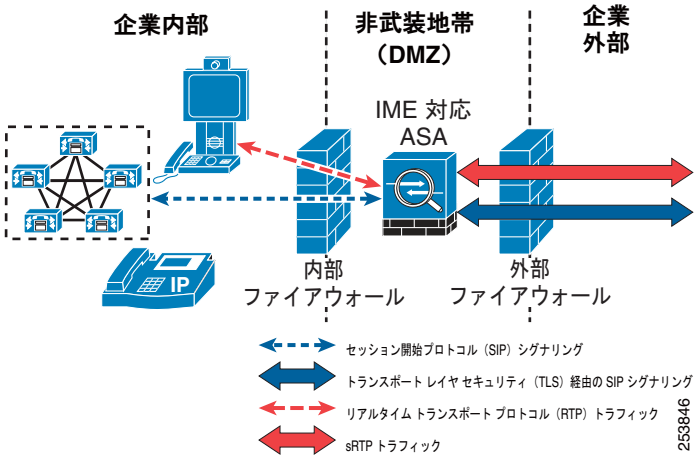


オフパス配置

企業ネットワーク内に既存のファイアウォールがある配置では、IME 機能をサポートするために既存のファイアウォールを置換またはアップグレードすること、またはインターネット ファイアウォールとインラインの IME 対応 ASA を追加して既存のセキュリティ アーキテクチャを変更することが不可能な場合があります。このシナリオでは、IME のオフパス モデルに ASA を実装できます。オフパスは、推奨される配置方式です。

オフパス配置では、図 4-20 に示すように、着信および発信 IME コールは DMZ 内に設置された IME 対応 ASA を通過します。Unified CM は、すべての SIP シグナリングを IME 対応 ASA に転送するように設定されます。その他のすべてのインターネット行きのトラフィックは、IME 対応 ASA を通過しません。

図 4-13　Intercompany Media Engine ASA のオフパス配置モデル



リモート企業からの着信 IME コールは、IME 対応 ASA の外側インターフェイスにアドレス指定されます。IME 対応 ASA は、静的な NAT または PAT を利用して、内側の各 Unified CM ノードへのマッピングを作成します。この動作は、どちらの配置オプションでも同じです。発信 IME コールの場合、オフパス配置では、Unified CM がオフパス IME 対応 ASA にコールを直接送信することが必要です。これは、マッピング サービス プロトコルによって実現されます。Unified CM は、IME 対応 ASA のマッピング サービス リクエストを送信し、宛先 IP アドレスとして使用される内部 IP アドレスおよびポート番号と IME で取得されたルート内のリモート宛先のポート番号を提供します。Unified CM は次に、この IME コールの SIP Invite をこの内部 IP アドレスにアドレス指定します。これにより、パケットが IME 対応 ASA に転送されることが保証されます。IME 対応 ASA はパケットを受信すると、コールを着信側の外部 IP アドレスに転送します。

通話中 PSTN フォールバック

IME ソリューションでは、Quality of Service（QoS）が許容レベルを下回った場合にコールが公衆網にフォールバックするメカニズムも提供されます。発信側と終端側の IME 対応 ASA は、インターネットから着信するすべてのオーディオ ストリーム（ビデオではない）をモニタし、感度調整するアルゴリズムを背景にメディアを分析します。RTP ストリームの検知された損失およびジッタ測定に基づいて、IME 対応 ASA は、コール品質が感度しきい値よりも低下したと判断した場合、SIP Refer メッセージを Unified CM に送信してフォールバックをトリガーします。IME コールはアクティブのままですが、発信側の Unified CM は、リモート企業の特定の IME フォールバック DID（SIP コール セットアップ時に取得）に対してバックグラウンドで公衆網コールをセットアップします。終端側 Unified CM が公衆網コールを IME コールのフォールバック コールとして識別し、接続が確立されると、両方の Unified CM はメディアをそれぞれの公衆網ゲートウェイに切り替えるようにエンドポイントに指示します。この変更はユーザにはシームレスです。ビデオなどの高度な機能は失われますが、コールの音声部分はそのままです。

デフォルトのフォールバック感度レベルから開始し、実際に公衆網接続にフォールバックするコール数を確認した後で変更することを推奨します。IME ソリューションおよび ASA 設定の詳細については、次の Web サイトで入手可能な『*Cisco ASA 5500 Series Configuration Guide using the CLI*』の Cisco Intercompany Media Engine プロキシ情報を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/config.html

設計上の考慮事項

IME 対応 ASA には少なくとも 2 つの外部（グローバル）IP アドレスが必要です。リモート企業からの着信コールに対して PAT が使用される場合、1 つは SIP シグナリング用、1 つはメディア ターミネーション用です。NAT が実装される場合は、さらに必要となる場合があります。IME 対応 ASA 上の SIP シグナリング用外部 IP アドレスは、IME で取得されたルートでアドバタイズされるものです。

IME 対応 ASA には少なくとも 2 つの内部 IP アドレスも必要です。1 つは SIP シグナリング用、1 つはメディア ターミネーション用です。Unified CM からの着信 IME コールに対して PAT が使用されます。

（注）　IME 対応 ASA のインターフェイスを外部および内部と呼んでいますが、ASA が DMZ 内に配置される場合、どちらのインターフェイスも DMZ 内に存在するサブネット上にある場合があります。最低でも、外部インターフェイス サブネットはインターネットからアクセス可能である必要があり、内部インターフェイス サブネットはイントラネットからアクセス可能である必要があります。

ソリューションの 2 つのコンポーネントを分離する、ネットワーク内の非 IME ファイアウォールについて、次のコンポーネント間の IME 通信を許可するために適切なピンホールを開くことが不可欠です。

- IME サーバと Unified CM
- IME サーバと GoDaddy 登録サーバ
- IME サーバとピアツーピア IME サーバ ネットワーク（分散キャッシュ リング）
- IME 対応 ASA（内部）と Unified CM
- IME 対応 ASA（内部）と IME 内部エンドポイント（メディア）
- IME 対応 ASA（外部）とリモート企業の IME 対応 ASA

IME ソリューションのコンポーネントのポートの全リストについては、次の Web サイトで入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

IME 対応 ASA と NAT を実行している Unified CM 間にイントラネット ファイアウォールがある場合は、次の条件を満たす必要があります。

- 着信および発信 SIP メッセージングの正しいフィックスアップを可能にするには、このイントラネット ファイアウォールは SIP ALG 機能に対応する Cisco ASA である必要があります。
- Unified CM の実際の IP アドレスを IME 対応 ASA が到達できるアドレスに変換するには、静的 NAT エントリが必要です。

Cisco IME 対応 ASA には、通常、インターネットのサブネットに到達するためのデフォルト ルートがあります。また、内部エンドポイントを含む潜在的なすべてのサブネットへの IP ルートも必要です。これには、データ サブネット（Cisco Unified Video Advantage カメラを含む場合もあり）も含まれます。

IME ソリューションには、SIP/TLS 接続の確立に使用される ASA 証明書を検証するための独自の認証局が必要です。IME 対応 ASA は、この Certificate Authority（CA; 認証局）に対して SIP SSL 証明書を確認する必要があります。

（注）　GoDaddy.com は、リモート企業とのセキュアな SIP TLS 接続を確立するために認可されている唯一の証明書プロバイダーです。

ハイ アベイラビリティ

IME 対応 ASA は、IME 通信のステートレス フェールオーバーを提供するために、アクティブ/スタンバイ フェールオーバー モードで配置できます。障害が発生した場合、確立されているすべてのコールおよび既存のコールは失われます。ステートフル フェールオーバーはサポートされません。

オフパス配置方式では、Unified CM は、それぞれが独自の IME ファイアウォールを持つ複数の IME サービス（登録 DID と除外 DID のセット）を設定できます。これにより、ソリューションの復元性はさらに向上します。

キャパシティ プランニング

ASA の各モデルは、一定の数の音声コールとビデオ コールの処理について評価されています。ASA の最新の IME コール キャパシティについては、「キャパシティ プランニング」（P.5-43）を参照してください。

オフパス モデルでは、Unified CM で設定された各 IME サービス（登録 DID と除外 DID のセット）は IME 対応 ASA に関連付けられます。複数の IME サービスが Unified CM に存在できるため、管理者は負荷を複数の IME 対応 ASA に分散して、全体のキャパシティを向上させることができます。

利点

IME によってセキュアな企業間通信システムが可能になり、Unified Communications 機能を強化でき、公衆網ネットワークを通過する必要がなくなります。

欠点

IME ソリューションには IME 対応 ASA が必要ですが、これはネットワーク内の既存のファイアウォールでは設定できない場合があります。

IME 対応 ASA は、単一のプロバイダーを Certificate Authority（CA; 認証局）として使用します。このことにより、必要な IME CA が含まれていない CA システムがすでに配置されている組織にとって、特別な考慮事項が発生する場合があります。

データ センター

データ センター内では、IP テレフォニー アプリケーション サーバで必要なセキュリティについて、セキュリティ ポリシーを定義する必要があります。Cisco Unified Communications サーバは IP に基づいているので、データ センター内にある、時間に敏感な他のデータに適用するセキュリティを、これらのサーバにも適用できます。

データ センターの間で WAN でのクラスタリングが使用されている場合、データ センター内とデータ センター間の両方に適用されている追加のセキュリティは、クラスタ内のノード間で許可されている最大往復時間に収まる必要があります。WAN 経由のクラスタリングを使用するマルチサイトまたは冗長なデータ センター実装では、アプリケーション サーバに関する現行のセキュリティ ポリシーでデータ

センターのファイアウォールをまたぐサーバ間のトラフィックを保護するように要求されている場合は、すでに展開済みのインフラストラクチャ セキュリティ システム間のこのトラフィックに対して IPSec トンネルを使用することを推奨します。

データ アプリケーションに適したデータ センター セキュリティを設計するには、次の Web サイトで入手可能な『*Data Center Networking: Server Farm Security SRND*』（『*Server Farm Security in the Business Ready Data Center Architecture*』）のガイドラインに従うことを推奨します。

http://www.cisco.com/go/designzone

ゲートウェイ、トランク、およびメディア リソース

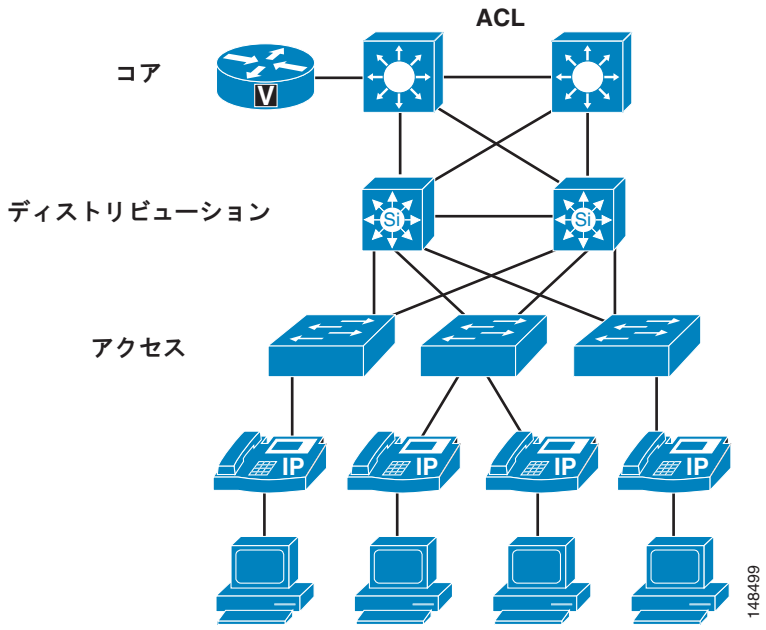
ゲートウェイおよびメディア リソースは、IP テレフォニー コールを公衆網コールに変換するデバイスです。外部コールがかけられた場合、ゲートウェイまたはメディア リソースは、IP テレフォニー ネットワークにおいてすべての音声 RTP ストリームが流れる数少ない場所の 1 つです。

IP テレフォニー ゲートウェイおよびメディア リソースは、ネットワーク内のほぼすべての場所に配置できるので、導入済みのセキュリティ ポリシーによっては、IP テレフォニー ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Unified CM により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御できます。ゲートウェイ（またはメディア リソース）と Unified CM のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合せを使用して、これらのデバイスが保護されています。

H.323 ビデオ会議デバイスでは、ネットワークのどの H.323 クライアントからでも H.225 トランクのためにポート 1720 をブロックするように、ACL を記述できます。この方法では、ユーザが互いに H.225 セッションを直接開始するのをブロックします。シスコ デバイスでは H.225 にさまざまなポートを使用する場合があるので、どのポートが使用されるかを確認するには、使用する機器の製品マニュアルを参照してください。可能であれば、シグナリングの制御に必要な ACL が 1 つだけになるように、ポートを 1720 に変更します。

ここでは、ネットワークのエッジで QoS を使用しているので、攻撃者が Voice VLAN に侵入してゲートウェイおよびメディア リソースの場所を判別できた場合、ポートの QoS により、攻撃者がゲートウェイまたはメディア リソースに送信できるデータの量が制限されます（図 4-14 を参照）。

図 4-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP を有効にしている場合、一部のゲートウェイおよびメディア リソースでは、電話機からのゲートウェイおよびメディア リソースに対する Secure RTP（SRTP）をサポートします。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

IPSec トンネルの詳細については、次の Web サイトで入手可能な『*Site-to-Site IPSec VPN Solution Reference Network Design（SRND）*』を参照してください。

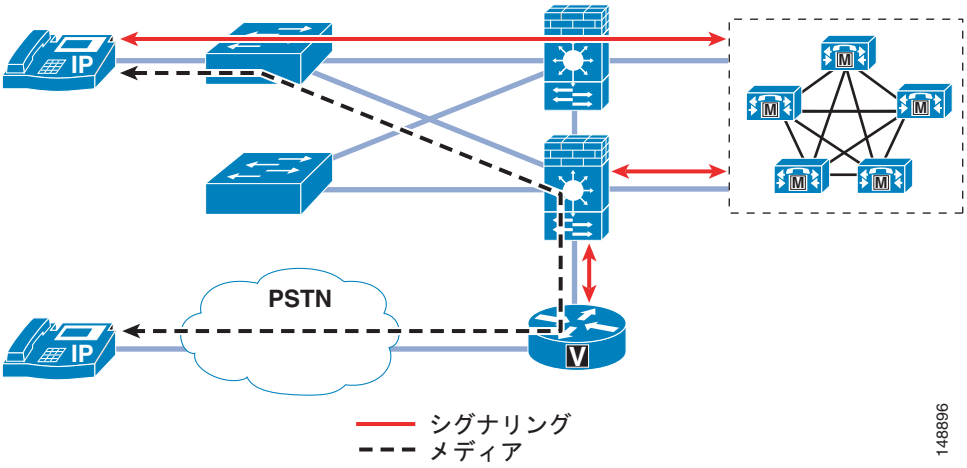
http://www.cisco.com/go/designzone

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、公衆網ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Unified CM、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 4-15 を参照）。

図 4-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番めの方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Unified CM からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Unified CM とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 4-15 を参照）。RTP ストリームはファイアウォールを通過しないので、この配置方式では、ファイアウォールの負荷が低下します。

利点

ACL とは異なり、ほとんどのファイアウォール設定では、シグナリングがファイアウォールを経由している限り、Unified CM が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco Intrusion Prevention System（IPS; 侵入防御システム）シグニチャがあります。

欠点

「ファイアウォール」（P.4-25）の項で説明するように、ファイアウォールが、電話機からゲートウェイへのすべてのシグナリングおよび RTP ストリームを調べる場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率をモニタする必要があります。

ファイアウォールと H.323

H.323 は、エンドポイント間のメディア ストリームのセットアップ、および Unified CM と H.323 ゲートウェイ間でアクティブ状態と要求される接続時間の間、H.245 を利用します。以降のコール フローに対する変更には H.245 を使用します。

デフォルトでは Cisco ファイアウォールによって H.245 セッションと関連するコールの RTP ストリームが追跡されます。また、RTP トラフィックが 5 分以上ファイアウォールを通過しない場合、H.245 セッションのタイムアウトも実行します。1 つ以上の H.323 ゲートウェイと他のエンドポイントがすべてファイアウォールの一方にあるトポロジでは、RTP トラフィックはファイアウォールによって認識されません。H.245 セッションは 5 分後にファイアウォールによってブロックされ、そのストリームの

制御が停止されます。ただし、ストリーム自体には影響しません。この場合、付加サービスなどは利用できなくなります。このデフォルトの動作はファイアウォール設定で、予想される最大コール所要時間が指定されるように変更できます。

利点

デフォルトの値を変更することでエンドポイントすべてがファイアウォールに対して同じ側に存在している場合に H.323 がコールすべての機能を維持できるというメリットがあります。

欠点

タイムアウト機能はファイアウォール側にあるコール エージェントの保護を強化しますが、タイムアウトが増加するとこの機能の価値が低下します。

SAF サービス

Unified CM は、その Call Control Discovery（CCD; コール制御ディスカバリ）機能に対して Cisco Service Advertisement Framework（SAF）ネットワーク サービスを使用します（「Service Advertisement Framework（SAF）」（P.3-64）を参照）。この機能では、コール制御ディスカバリ アドバタイジング サービスに関連付けられた SIP トランクまたは非ゲートキーパー制御 H.323 トランクが使用されます。サービスは、H.323 トランクの動的ポート番号、SIP トランクの標準ポート 5060、SIP ルート ヘッダー情報など、これらのトランクのコール ネゴシエーション情報をアドバタイズします。

Adaptive Security Appliance には、SAF ネットワーク サービスのアプリケーション インスペクションはありません。Unified CM がコールの発信に SAF 対応 H.323 トランクを使用する場合、ASA は H.225 シグナリングで使用されている一時的なポート番号を取得するために SAF パケットを検査できません。そのため、SAF 対応 H.323 トランクからのコール トラフィックが ASA を通過するシナリオでは、このシグナリング トラフィックを許可するために ASA 上で ACL を設定する必要があります。ACL 設定は、H.225 および H.245 シグナリングによって使用されるすべてのポートを指定している必要があります。標準 5060 ポートの SAF 対応 SIP トランクが使用される場合は、ACL 設定は必要ありません。

Cisco Unified Border Element との Unified CM トランク統合

Unified CM トランクによって、企業ネットワークと外部ネットワークの間に IP 接続ポイントが追加されます。これらの相互接続に追加のセキュリティ対策を適用して、データおよび IP テレフォニー アプリケーションに固有の脅威を軽減する必要があります。Unified CM トランクと外部ネットワークの間に Cisco Unified Border Element を実装することが、より柔軟でセキュアな相互運用性オプションとなります。

Cisco Unified Border Element は、音声アプリケーション境界と音声トラフィックとデータ トラフィックの両方に適用できるセキュリティ脅威軽減技術を提供する Cisco IOS ソフトウェア機能です。Cisco Unified Border Element は、Cisco IOS ファイアウォール、認証、および VPN 機能とともに同じデバイス上で設定でき、サービス プロバイダー ネットワークまたはその他の外部ネットワークと統合された Unified CM トランクのセキュリティを強化できます。これらの Cisco IOS セキュリティ機能は、外部の攻撃に対する防御として、およびルータを通過してサービス プロバイダーのネットワークへ出ていく内部トラフィックのチェックポイントとしての役割を果たします。サービス プロバイダーまたはサービス プロバイダーのネットワークに接続されたネットワークから発生した不正アクセス、DoS 攻撃、または Distributed DoS（DDoS; 分散型 DoS）攻撃を防ぐために、および侵入やデータ盗用を防ぐために、インフラストラクチャ Access Control List（ACL; アクセス コントロール リスト）を使用することもできます。

特定の SIP サービス プロバイダーでは、コール サービスが許可される前に、SIP トランクへの登録が必要です。これにより、コールは既知のエンドポイントだけから発生するようになり、企業とサービス プロバイダー間のサービス ネゴシエーションはよりセキュアになります。Unified CM は、ネイティブで SIP トランク上の登録をサポートしていませんが、Cisco Unified Border Element を使用すればこのサポートが可能になります。Cisco Unified Border Element は、Cisco Unified Communications Manager に代わって、企業の電話番号を使用してサービス プロバイダーに登録します。

Cisco Unified Border Element の設定および製品詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

- http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html
- http://www.cisco.com/en/US/products/sw/voicesw/ps5640/products_installation_and_configuration_guides_list.html

利点

シグナリングおよびメディアのネットワーク トポロジを隠蔽する機能を提供する Back-To-Back User Agent（B2BUA; バックツーバック ユーザ エージェント）として動作する Cisco Unified Border Element。ネットワークのセキュリティと処理上の独立性を有効にし、すべてのトラフィックで Cisco Unified Border Element IP アドレスを置き換えることで NAT サービスを提供します。

Cisco Unified Border Element は、ネットワーク間のメディアおよびシグナリング パケットで DSCP QoS パラメータを再マーキングするために使用できます。これにより、トラフィックはネットワーク内で QoS ポリシーに従うようになります。

Cisco IOS ファイアウォール機能は、Cisco Unified Border Element との組み合せで使用され、シグナリング メッセージを一致させてトラフィックを管理するために Application Inspection and Control（AIC）を提供します。これは、SIP トランク DoS 攻撃を防ぐのに役立ち、コンテンツおよびレート制限に基づくメッセージ フィルタリングを可能にします。

Cisco Unified Border Element によって SIP トランク登録が可能です。この機能は、Unified CM SIP トランクでは使用できません。Cisco Unified Border Element は、背後にあるエンドポイントに代わって、企業ネットワークの E.164 DID 番号をサービス プロバイダーの SIP トランクに登録できます。

Cisco Unified Border Element は、外部ネットワーク経由で SRTP を使用して RTP 企業ネットワークを接続できます。これにより、企業内に SRTP を配置しなくても安全な通信が可能になります。

欠点

Cisco Unified Border Element とファイアウォールの使用には複数の設計オプションがありますが、実装の複雑さが増し、追加のソフトウェア機能ライセンスが必要となります。

ネットワークの E.164 DID 番号をプロキシするために Cisco Unified Border Element を使用する場合、実際のエンドポイントのステータスはモニタされません。したがって、登録解除されたエンドポイントが引き続き使用可能として表示される場合があります。

RTP-SRTP インターワーキングがサポートするコーデック数には制限があります（G.711 mulaw、G.711 alaw、G.729abr8、G.729ar8、G.729br8、G.729r8 など）。

アプリケーション サーバ

Unified CM セキュリティ機能のリスト、および有効にする方法については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Security Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

任意の Unified CM セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。詳細については、次の Web サイトにある『*Cisco ASA 5500 Series Release Notes*』を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa80/release/notes/asarn80.html

シングル サインオン

Single Sign-On（SSO; シングル サインオン）機能は、Cisco Unified CM 8.5(1) で導入されました。この機能によりエンド ユーザは、Windows ドメインにログインできるようになり、Unified Communication Manager の User Options ページおよび Cisco Unified Communications Integration for Microsoft Office Communicator（CUCIMOC）アプリケーションに安全にアクセスすることができます。

シングル サインオンの設定には、Cisco Unified CM と サードパーティ製アプリケーションとの統合が必要です。サードパーティ製アプリケーションには、Microsoft Windows Servers、Microsoft Active Directory、および ForgeRock Open Access Manager（OpenAM）も含まれます。設定の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の最新版を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Unified CM およびアプリケーション サーバ上の Cisco Security Agent

Cisco Security Agent は、IP テレフォニーおよび IP テレフォニー サービスを提供するのにシスコが使用するアプリケーション サーバのほとんどで使用されています。Cisco Security Agent ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別する、ホスト侵入防御ソフトウェアです。異常と見なされるものが見つかった場合、Cisco Security Agent ソフトウェアはそのアクティビティが発生するのを阻止します。たとえば、Unified CM にソフトウェア パッケージをインストールすることを試みるウイルスがあり、そのような事態が以前発生したことがない場合でも、ウイルスがインストールを実行することは阻止されます。ただし、Cisco Security Agent は感染を防止するだけで、一度感染したサーバをクリーンにすることはできないので、サーバにはアンチウイルス ソフトウェアが引き続き必要です。

Cisco Security Agent

シスコは、自社サーバ用のデフォルト Cisco Security Agent ポリシーを開発しました。このポリシーにより、IP テレフォニー サーバで必要なすべての機能は正しく機能し、同時に、既知および不明な攻撃が IP テレフォニー サーバに影響することは防止されます。このソフトウェアは、アプリケーションとオペレーティング システムを、ウイルスやワーム攻撃から保護します。これらのタイプの侵入からの最大限の保護を得るには、常に最新バージョンの Cisco Security Agent ソフトウェアがサーバにインストールされていることを確認してください。管理対象外エージェントがサーバにインストールされていると、攻撃のログは、エージェントがインストールされているシステムでのみ参照できます。特定のタイプのアラームが発生したので書き込まれた可能性があるログ ファイルをチェックするには、各システムにログインする必要があります。管理対象外 Cisco Security Agent はデフォルトで Unified CM のインストール時にインストールされます。

利点

管理対象外 Cisco Security Agent は、既知および不明の攻撃、ワーム、およびウイルスから各システムを保護します。

欠点

Cisco Security Agent を管理対象外モードで実行すると、アラームは相関されません。システムのログ ファイルを参照するには、各システムに個別にアクセスする必要があります。

（注）　Cisco Unified CM 8.*x* では現在、管理対象 Cisco Security Agent 機能はサポート*されません*。

サーバに関する一般的なガイドライン

Unified CM およびその他の IP テレフォニー アプリケーション サーバは、通常のサーバとして扱わないでください。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス時間帯で行う必要があります。

アプリケーション サーバ用の標準的なセキュリティ ポリシーは、IP テレフォニー サーバには不十分な場合があります。電子メール サーバや Web サーバとは異なり、音声サーバでは、画面をリフレッシュしたり、メッセージを再送信したりすることは許可されていません。音声通信は、リアルタイムのイベントです。IP テレフォニー サーバ用のセキュリティ ポリシーでは、音声システムの設定または管理に関連付けられていない作業が、IP テレフォニー サーバで決して行われないことを保証する必要があります。ネットワーク内のアプリケーション サーバで通常のアクティビティと見なされるアクティビティ（インターネット サーフィンなど）でも、IP テレフォニー サーバで行うことはできません。

また、シスコは IP テレフォニー サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このパッチ システムを適用する必要があります。シスコシステムズにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコシステムズの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

導入済みのセキュリティ ポリシーで、デフォルト インストールで提供された以上の OS のロック ダウンが要求されている場合は、OS の強化手法を使用する必要があります。

セキュリティの警告を受け取るために、次の Web サイトでシスコの通知サービスに登録できます。

http://www.cisco.com/cisco/support/notifications.html

利点

アプリケーション サーバを他のアプリケーション サーバのようではなく PBX のように扱う場合、一般的なサーバ セキュリティ プラクティスを実施すると、ウイルスやワームを減らすのに役立ちます。

欠点

追加のセキュリティ機能を設定すると、一部の Unified CM 機能が低下する場合があります。また、アップグレードを正常に実行するには、追加のセキュリティで無効になっている一部のサービスを有効にする必要があるため、アップグレード中は特に注意が必要です。

配置例

この項では、ロビーに設置された電話機およびファイアウォールの配置について、セキュリティ面を考慮した実施例を示します。このようなタイプと同様の配置を扱うには、適切なセキュリティ ポリシーを適用する必要があります。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（「電話機の PC ポート」（P.4-17）を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（「アクセス設定」（P.4-19）を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（「IP アドレッシング」（P.4-5）を参照）。また、電話機が抜かれると、ポートの状態が変化し、電話機は Unified CM から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、誰かがネットワークへの接続を試行しているかどうかを判別できます。

電話機のスタティック ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。ダイナミック ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しない限り、MAC アドレスをクリアするためにスイッチ ポートを変更せずに済みます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための Lobby Phone というラベルに置き換えることができます（「スイッチ ポート」（P.4-8）を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（「DHCP スヌーピング：不正な DHCP サーバ攻撃の防止」（P.4-11）を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN でダイナミック ARP インスペクションを有効にして、攻撃者が、ネットワーク上のレイヤ 2 ネイバーの 1 つに関する他の情報を取得するのを防止できます（「ダイナミック ARP インスペクションの要件」（P.4-14）を参照）。

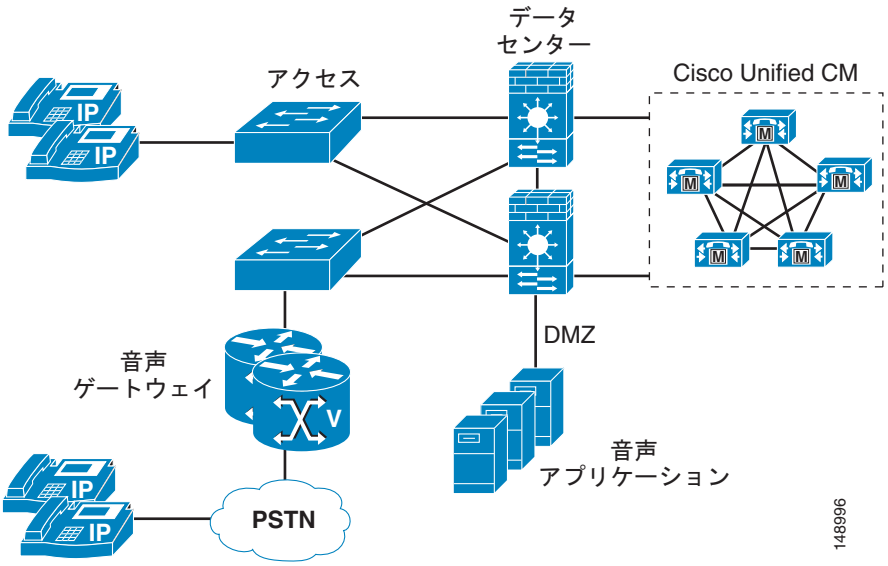
DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソース ガードを使用できます。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（「VLAN アクセス コントロール リスト」（P.4-22）を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（「ルータのアクセス コントロール リスト」（P.4-23）を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への保留音または電話機からの HTTP アクセスは使用しません。

ファイアウォールの配置例（集中型配置）

この項の例は、データ センター内において、背後に Unified CM を配置するファイアウォールの 1 つの展開方法を示しています（図 4-16 を参照）。この例では、Unified CM は、すべての電話機がファイアウォールの外側から 1 つのクラスタに接続される集中型配置として置かれています。この配置内のネットワークには、社内データ センター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての RTP ストリームがファイアウォールを横断しないようにすることが決定されました（「ゲートウェイの周囲へのファイアウォールの配置」（P.4-37）を参照）。ゲートウェイはファイアウォールの外側に配置されています。Unified CM でゲートウェイとの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（「IP アドレッシング」（P.4-5）を参照）。音声アプリケーション サーバは DeMilitarized Zone（DMZ; 非武装地帯）に配置されています。Unified CM との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用します。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小限に抑えられます。

図 4-16　　ファイアウォールの配置例



ネットワーク仮想化の保護

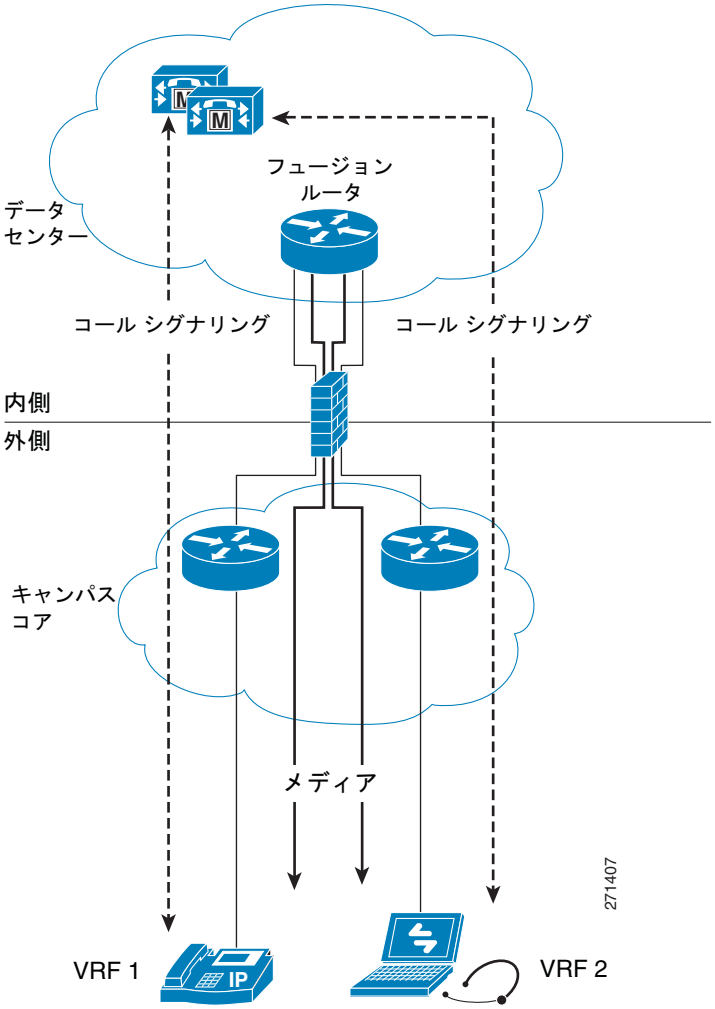
ここではバーチャル ネットワーク間の通信に同種接続を提供するのに伴う問題と、この問題を解決するための手法について説明します。バーチャル ルート フォワーディングとネットワーク仮想化についての知識が必要です。これらのテクノロジーに関するネットワーク設計原理については、http://www.cisco.com/go/designzone で入手可能なネットワーク仮想化の資料を参照してください。

ここで紹介する内容は、仮想化を使用した Unified Communication ソリューションのセキュリティの強化を保証するものではありません。既存のインフラストラクチャに Unified Communications レイヤに配置できる内容を説明することを目的としています。仮想化テクノロジーのメリットとデメリットを評価するには、ネットワーク仮想化に関する資料を参照してください。

仮想化テクノロジーに基づいたネットワークでは、トラフィックがレイヤ 3 で論理的に区別され、バーチャル ネットワークにはそれぞれルーティング テーブルが存在します。ルーティング情報の欠如により、異なるバーチャル ネットワーク間では通信できません。この環境はユーザ エンドポイントがデータ センター内のデバイスとのみ通信するクライアントサーバ配置に最適ですが、ピアツーピア通信では問題が発生します。部門別、場所別、トラフィックのタイプ（データまたは音声）別など、バーチャル ネットワークの配置にかかわらず、異なるバーチャル プライベート ネットワーク ルーティングおよび転送（VRF）テーブルのエンドポイントに相互に通信する機能が備えられていないという問題の中核は変わりません。図 4-17 で示されているソリューションでは、ある VRF に設置されたソフトウェア ベースの電話機と別の VRF に設置されたハードウェア電話機の通信にデータ センターに設置された共有 VRF を使用しています。このソリューションは、他の異なる状況にも適用できる場合があります。ネットワーク仮想化では、データ センターとキャンパス ネットワーク間の境界に対する、データ センターの防御を実装することが要求されます。以降では、この実装方法について説明します。

シナリオ 1：単一のデータ センター

図 4-17　単一のデータ センター



このシナリオは最も簡単に実装できます。通常のネットワーク仮想化実装への増設として実装します。この設計では、パケットを任意の VRF にルーティングできる機能を備えたデータ センター ルータが組み込まれています。このルータはフュージョン ルータと呼ばれます（フュージョン ルータの構成に関する詳細については、ネットワーク仮想化の資料を参照してください）。このピアツーピアの通信トラフィックを可能にする配置シナリオは、VRF 間のルーティングとデータ センターのセキュアなアクセスを実現するファイアウォール機能の役割をフュージョン ルータが担います。

このシナリオには、次の主な要件が適用されます。

- キャンパス ルータによってパケットがデフォルトのルーティング経由でフュージョン ルータに向けて他のキャンパス VRF に送信されます。つまり、すべてのルータ ホップはデフォルトでフュージョン ルータにルーティングされる必要があります。データ センターで共有されている VRF にはそれぞれのキャンパス VRF に関するルート情報が保持されています。共有 VRF を除くすべての VRF は直接接続されていません。
- Unified CM はデータ センターの共有 VRF に配置されています。共有 VRF 内の通信が妨げられることはありません。

- 共有 VRF はデータ センターに設置されています。複数のデータ センターが存在している場合は、共有 VRF はデータ センターすべてを網羅します。

データ センター側のアプリケーション レイヤ ゲートウェイによって TFTP と SCCP または外部から送信された SIP セッションをデータ センターの Unified CM クラスタ宛てに送信するポートを開放するアクセス リストが指定されます。TFTP は電話機が TFTP サーバから設定とソフトウェア イメージをダウンロードするのに必要です。また、電話機を Unified CM クラスタに登録するため、SCCP または SIP が必要です。使用される特定のソフトウェア バージョンに適切なポート番号については Unified CM の製品マニュアルを参照してください。

このシナリオでは、VRF それぞれの通信デバイスから送信されたコール シグナリングは、すべてアプリケーション レイヤ ゲートウェイを経由してシグナリングをインスペクションすることでアプリケーション レイヤ ゲートウェイが動的に必要な VRF それぞれの UDP ピンホールを開き、ファイアウォール外部から送信された RTP トラフィックをフュージョン ルータ宛てに通します。ファイアウォールでインスペクションされないと、外部エンドポイントから送信された RTP ストリームそれぞれはファイアウォールを通過できません。呼制御シグナリングのインスペクションにより、ファイアウォールを通じた UDP トラフィックのフォワーディングが可能になります。

利点

この配置モデルは、VRF 対応ネットワーク上で通信デバイスのピアツーピア接続を可能にします。アプリケーション レイヤ ゲートウェイによって共有 VLAN とフュージョン ルータに安全にアクセスできます。

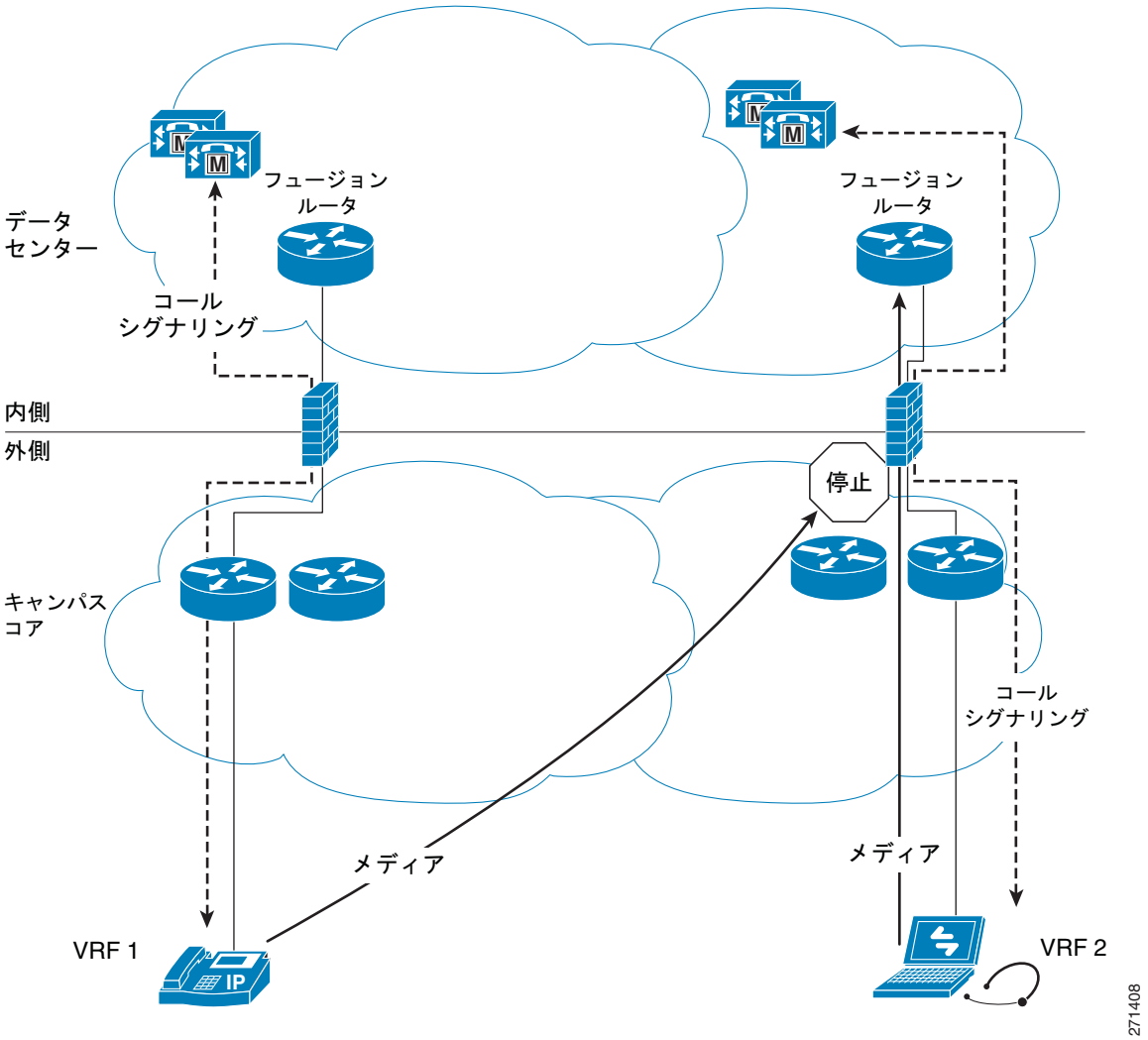
欠点

エンドポイント間の異なる VRF のメディア ストリームはすべて、最短パスを通過しません。メディアはフュージョン ルータ経由でルーティングされるためデータ センターにバックホールされます。

シナリオ 2：冗長なデータ センター

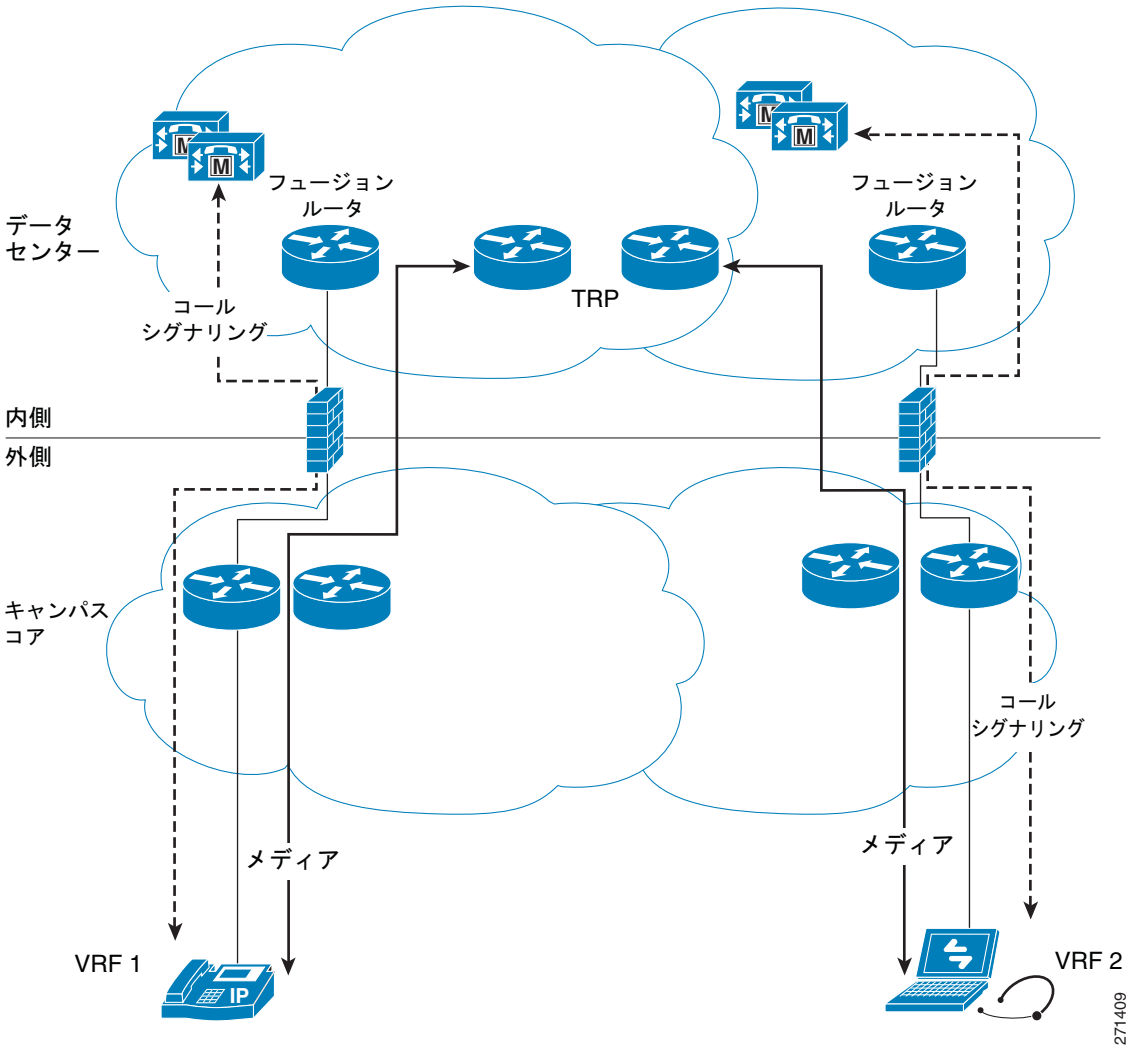
冗長なデータ センターの場合、シナリオは複雑化します。コール セットアップ シグナリングが対応する RTP ストリームによって使用される同一のアプリケーション レイヤ ゲートウェイを確実に通過するようにします。シグナリングとメディアが異なるパスを通過すると、UDP ピンホールが開かれません。図 4-18 は問題を抱えるシナリオの例を示します。左のハードウェア電話機は左のデータ センターのサブスクライバによって制御されています。対応する呼制御シグナリングは左のファイアウォールを通過します。RTP ストリームを通過させるため、このファイアウォールのピンホールが開かれています。しかし、このルーティングでは RTP メディア ストリームが必ず同じパスを通過するとは限りません。また、右のファイアウォールによってストリームはブロックされます。

図 4-18　異なるパスを通過するコール シグナリングとメディア



この問題を解決するには、Trusted Relay Point（TRP）機能を使用します（図 4-19 を参照）。データ センターそれぞれのサブスクライバは メディアを固定する TRP を起動して、メディア ストリームが適切なファイアウォールを確実に通過するようにします。左のデータ センター内のサブスクライバによって制御されている電話機が左データ センターの TRP を起動し、右のデータ センター内のサブスクライバによって制御されている電話機が右データ センターの TRP を起動する必要があります。TRP は、コール シグナリングとまったく同じルーティング パスを通過することを保証するメディアに対して、特定のホスト ルートを有効にする IP アドレスを提供します。このアドレスを使用してシグナリングとメディアは同じファイアウォールを通過するため、問題を解決できます。

図 4-19　TRP を備えた冗長なデータ センター



TRP は、デバイスが利用されるコールでデバイス レベルで起動されるメディア ターミネーション ポイント リソースです。デバイスにはそれぞれ TRP を起動するかどうかを設定するチェックボックスがあります。

まとめ

この章では、ネットワーク内の音声データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。

CHAPTER 5

Unified Communications の配置モデル

この章では、Cisco Unified Communications システムの配置モデルについて説明します。

この章の旧版では、Cisco Unified Communications Manager（Unified CM）向けのコール処理配置モデルに基づいて、配置モデルを説明しました。これに対して、この章の最新版では、Cisco Unified Communications システムの構成技術に関する設計ガイドラインについてサイトベースで説明します。その目的は、Cisco Unified Communications システム全体の設計ガイドラインを示し、コール処理サービスにとどまらず豊富な情報を提供することです。

以前のリリースの Cisco Unified Communications での設計ガイドラインについては、次の Web サイトで入手可能な Cisco Unified Communications ソリューション リファレンス ネットワーク デザイン（SRND）のマニュアルを参照してください。

http://www.cisco.com/go/ucsrnd

この章の新規情報

表 5-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Unified CMBE 3000 ローカル PSTN ブレークアウトの考慮事項	「集中型コール処理を使用するマルチサイト」（P.5-9）	2011 年 6 月 30 日
Cisco Unified CMBE 6000 での WAN を介したクラスタリング	「WAN を介した Unified CMBE 6000 クラスタリング」（P.5-58）	2011 年 6 月 2 日
ファイバ チャネル プロビジョニングとストレージ アレイ論理ユニット番号に関する項は、この章から削除されました。これらの情報は、他のシスコの資料で詳しく説明されています。	http://www.cisco.com/go/uc-virtualized http://www.cisco.com/en/US/netsol/ns747/networking_solutions_sub_program_home.html	2011 年 6 月 2 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）3000、5000、および 6000	この章の各項で説明	2011 年 2 月 28 日
Enhanced Survivable Remote Site Telephony（E-SRST）	「Enhanced Survivable Remote Site Telephony」（P.5-19）	2010 年 11 月 15 日

表 5-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ファイバ チャネルのプロビジョニングとハイ アベイラビリティ、Logical Unit Number（LUN; 論理ユニット番号）のパーティション、Input/Output Operations Per Second（IOPS）、および論理ハード ディスク RAID スキーム	「B シリーズ ブレード サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項」（P.5-62）	2010 年 11 月 15 日
Intercompany Media Engine（IME）PSTN フェールオーバー	「PSTN のフェールオーバー」（P.5-41）	2010 年 11 月 15 日
Cisco UCS C シリーズ ラックマウント	「Cisco UCS C シリーズ ラックマウント」（P.5-62） 「C シリーズ ラックマウント サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項」（P.5-64）	2010 年 7 月 23 日
Cisco Unified Communications Manager Session Management Edition	「Session Management Edition を配置する場合の設計上の考慮事項」（P.5-31）	2010 年 7 月 23 日
Cisco Intercompany Media Engine	「Cisco Intercompany Media Engine」（P.5-35）	2010 年 4 月 2 日
Cisco IOS Service Advertisement Framework（SAF）	「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）	2010 年 4 月 2 日
サイトベースの設計ガイドライン	「サイトベースの設計」（P.5-3）	2010 年 4 月 2 日
仮想サーバでの Unified Communications アプリケーション	「仮想サーバでの Unified Communications の配置」（P.5-59）	2010 年 4 月 2 日

配置モデル アーキテクチャ

一般に、配置モデル アーキテクチャは、サービスを提供する企業のアーキテクチャに従います。配置モデルは、企業の代表的なトポロジにおける Unified Communications ニーズを満たす参照アーキテクチャを記述します。たとえば、集中型コール処理配置モデルは、1 箇所または数箇所の中央集中型の本社に接続された多数のサイトで業務の大部分が行われる企業に向いたモデルです。

場合によっては、技術的制約のために技術の配置モデルが企業の配置モデルから逸脱することがあります。たとえば、企業に 1 つあるキャンパスのスケールが 1 つのサービス インスタンス（Cisco Unified Communications Manager が提供するコール処理サービスなど）のスケールを超えている場合、1 つのキャンパスに複数のコール処理クラスタ インスタンスまたは複数のメッセージング製品が必要になることがあります。

配置モデルのハイ アベイラビリティ

Unified Communications サービスは、ハイ アベイラビリティを実現するための機能を数多く備えています。その実装には、次のようにさまざまな方法があります。

- フェールオーバー冗長性

  不可欠なサービスの場合、設計に単一障害点が存在しないように冗長な要素を配置します。2 つ（またはそれ以上）の要素間の冗長性が自動的に確保されます。たとえば、Cisco Unified Communications Manager（Unified CM）に使用されているクラスタリング技術では、最大 3 台のサーバがお互いをバックアップできます。このタイプの冗長性は、技術的境界を越えて実現される

場合があります。たとえば、1 台の電話機に対して、優先順位 3 番めまでの呼制御エージェントとして、同じコール処理クラスタに属する 3 台の独立した Unified CM サーバを設定できます。そして 4 番めの選択肢として、Cisco IOS ルータを利用してコール処理サービスを提供するように電話機を設定することもできます。

- リンクの冗長性

  1 つの WAN リンクでの障害に対処するために、IP WAN リンクなどの冗長な IP リンクを配置すると有益な場合があります。

- 地理的多様性

  一部の製品は、冗長なサービス ノードを WAN リンク越しに分散させて、（あらかじめ設定しておいた UPS および発電バックアップ システムの機能を超えて長時間停電が発生するなど）サイト全体がオフラインになっても、別の場所にある別のサイトで事業を継続できるようにしています。

配置モデルのキャパシティ プランニング

さまざまな配置モデルのキャパシティは、一般にその基となる製品のキャパシティと切り離すことができません。この章では、適宜キャパシティについて説明します。サービスをサポートしている製品をこのドキュメントの他の項で詳しく取り上げている場合、その項でその製品のキャパシティについて説明します。

サイトベースの設計

Cisco Unified Communications システムを構成するどの技術でも、設計時に検討する基準として次のものがあります。

サイズ

このコンテキストでのサイズとは一般にユーザ数を指し、これが IP 電話、ボイスメールボックス、プレゼンス ウォッチャなどの数量に読み換えられます。また、データセンターなど、ユーザがほとんど（あるいはまったく）存在しないサイトでは、処理キャパシティの点からサイズを考えることもできます。

ネットワーク接続

サイトをシステムの他の部分への接続を設計する際に考慮が必要な主な要素が 3 つあります。

- Quality of Service（QoS）を確保できる帯域幅
- 遅延
- 信頼性

多くの場合、Local Area Network（LAN; ローカル エリア ネットワーク）ではこれらの要素は十分達成されています。すべての LAN 機器で QoS が達成されており、帯域幅は一般にギガビット範囲、遅延は最小限（数ミリ秒程度）で、優れた信頼性が標準で確保されています。

Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）では、3 つの要素とも LAN に近いものとなっています。帯域幅は一般にまだ数メガビット範囲、遅延は一般に数十ミリ秒で、優れた信頼性が確保されています。一般にパケット処理ポリシーが MAN プロバイダーから提供されるため、エンドツーエンドの QoS を実現できます。

Wide Area Network（WAN; ワイド エリア ネットワーク）では、これらの要素に特に注意する必要があります。帯域幅はコストが何よりも重視され、遅延は実効的な送出速度だけでなく物理的な距離にかかわる実際の伝搬遅延にも左右されることがあり、信頼性はさまざまな要因の影響を受けます。また、QoS 実現のために、余分な運用コストと設定作業が必要になることもあります。

帯域幅は、サイトで利用できる Unified Communications サービスのタイプおよびサービスの提供方法に大きな影響を与えます。たとえば、20 人のユーザにサービスを提供するサイトがシステムの他の部分に 1.5 Mbps の帯域幅で接続している場合、サイトの音声、プレゼンス、インスタント メッセージング、電子メール、およびビデオ サービスをリモートのデータセンター サイトに問題なくホストできます。その同じサイトが 1000 人のユーザをホストしている場合、比較的限られた帯域幅がシグナリングおよびメディア フローで飽和状態になるのを避けるために、サービスの一部をローカルにホストするのが最善です。これ以外にもう 1 つ、リモートのデータセンター サイトから WAN 全体にサービスを配信できるよう帯域幅を拡大する方法もあります。

遅延が設計に与える影響は、リモートに配置する Unified Communications サービスのタイプに応じて異なります。たとえば、片方向の遅延が 200 ms である WAN 全体に音声サービスを提供する場合、ダイヤルトーン遅延やメディア カットスルー遅延増大などの問題が発生することがあります。プレゼンスなど他のサービスでは、200 ms の遅延があっても問題が発生しない可能性があります。

サイトからネットワークの他の部分への接続の信頼性は、技術に適した配置モデルを決定する際の基本的な考慮事項です。信頼性が高い場合は、ほとんどの Unified Communications コンポーネントではリモート サイトからホストされるサービスを配置できます。信頼性が安定しない場合、一部の Unified Communications コンポーネントはリモートからホストされる際に正しく実行されないことがあります。信頼性が低いと、サイトに Unified Communications サービスのコロケーションが必要になることがあります。

ハイ アベイラビリティ要件

サービスのハイ アベイラビリティは常に設計の目標となるものです。信頼性の必要性とその実現に伴うコストとのバランスを保つには、実際的な設計の判断が必要です。次のいずれの要素も、設計がハイアベイラビリティを実現できるかどうかに影響を与えます。

- 帯域幅の信頼性。Unified Communications サービスの配置モデルに直接影響を与えます。
- 電源の可用性

  停電は、どんなシステムでも極めて破壊的な事象です。停電中はサービスが利用できなくなるだけでなく、電力復旧によってリプル効果がもたらされるためです。電力の可用性が高いサイト（たとえば、Uninterruptible Power Supply（UPS; 無停電電源装置）および発電装置によるバックアップを備えて、電力グリッド接続が安定しているサイト）は、一般に Unified Communications サービスのホストに選択できます。サイトの電力可用性に一貫性がない場合、そのサイトをホスト用のサイトとして使用するのは賢明な判断ではありません。
- 熱、湿度、振動などの環境要因
- 能力ある人材の確保

  一部の Unified Communications サービスは、サーバなど定期的な保守を必要とする機器を使用して配信されます。Unified Communications コール エージェント サーバのホストなど、一部の Unified Communications 機能は、能力ある人材が配属されているサイトに配置するのが最善です。

サイトベースの設計ガイドライン

このドキュメント全体を通して、さまざまな Unified Communications サービスおよび技術の系列に沿って設計ガイドラインを編成しています。たとえば、コール処理の章では、コール処理サービスを実際に説明するだけでなく、サイトのサイズ、ネットワーク接続、およびハイ アベイラビリティの要件

に基づいて IP Phone および Cisco Unified Communications サーバを配置するための設計ガイドラインも示します。同様に、コール アドミッション制御の章では、技術自体の説明に焦点を当てるだけでなく、サイトベースの設計考慮事項も示します。

一般に、特定の Unified Communications サービスまたは技術のほとんどの側面が、サイトのサイズまたはネットワーク接続とは関係なく、すべての配置に関係しています。必要に応じて、サイトベースの設計考慮事項について説明します。サービスは集中化、分散化、インターネットワーク化、および地理的多様化が可能です。

サービスの集中化

企業の支店サイトが地理的に分散し、ワイド エリア ネットワークで相互接続されている用途では、Cisco Unified Communications サービスを中央に配置しつつ、WAN 接続でエンドポイントにサービスを提供できます。たとえば、コール処理サービスを集中的に配置できます。テレフォニー サービスの配信に必要なのは、リモート サイトとの IP 接続だけです。同様に、Cisco Unity Connection プラットフォームから提供されるようなボイス メッセージ サービスも中央にプロビジョニングして、IP WAN で接続されたリモートからサービスをエンドポイントに配信できます。

中央にプロビジョニングした Unified Communications サービスは、WAN 接続中断の影響を受けます。そのため、サービスごとに、ローカル サバイバビリティ オプションを計画すべきです。たとえば、Cisco Unified CM から提供されるようなコール処理サービスには、SRST や Cisco Unified Communications Manager Express（Unified CME）などのローカル サバイバビリティ機能を設定できます。同様に、Cisco Unity Connection のような集中型ボイス メッセージ サービスは、SRST または Unified CME で運用するリモート サイトから中央サイトのボイス メッセージ サービスへ公衆網経由でアクセスできるようにプロビジョニングできます。

すべての Unified Communications サービスでサービスの集中化を統一する必要はありません。たとえば、複数のサイトが 1 つの集中型コール処理サービスを利用する場所にシステムを配置し、一方で Cisco Unity Express などの非集中型（分散型）ボイス メッセージ サービスでそのシステムをプロビジョニングすることもできます。同様に、Cisco Unity Connection などの集中型ボイス メッセージ サービスとともに、Cisco Unified Communications Manager Express を使用してコール処理が各サイトでローカルにプロビジョニングされる形態で Unified Communications システムを配置することもできます。

多くの場合、各サービスの設計時に考慮すべき主要な基準は、サイト間の IP ネットワークの可用性と品質です。サイト間の IP 接続が次の特性を備えている場合、Unified Communications サービスの集中化は、機器のホストと運用に伴う資本費用と運用費用のどちらの面でもスケールメリットが得られます。

- 予想されるトラフィック負荷に十分対応できる帯域幅。ボイスメールへのアクセス、集中型の公衆網接続へのアクセス、音声やビデオを含むサイト間オンネット通信などによって発生する、ピーク時のアクセス負荷も含めます。
- ハイ アベイラビリティ。WAN サービス プロバイダーがサービス レベル契約に従って接続を迅速に保守および復旧することによりもたらされます。
- 低遅延。主要な中央サイトへのラウンドトリップ時間のためにシステムの応答時間に遅延が発生しても、リモート サイトのローカルなイベントは損害を受けません。

また、特定のサービスを中央に配置して複数のサイトのエンドポイントにサービスを提供した場合、複数のサイトでユーザに同じ処理リソースを使用することから、機能の透過性という利点が得られます。たとえば、2 つのサイトに同じ集中型 Cisco Unified Communications Manager クラスタからサービスを提供する場合、ユーザは 2 つのサイト間でライン アピアランスを共有できます。各サイトに異なる（分散した）コール処理システムからサービスを提供する場合には、この利点は得られません。

機能の透過性およびスケール メリットという利点は、Unified Communications トラフィックの需要に応えるために WAN ネットワークを構築および運用する際の相対的コストに照らして評価する必要があります。

サービスの分散化

Unified Communications サービスは、複数のサイトに分散させて個別に配置することもできます。たとえば、2 つ（またはそれ以上の）のサイトを独立したコール処理 Cisco Unified CME ノードでプロビジョニングできます。同じ場所にあるエンドポイントに対するサービスの可用性を確保するために WAN を利用する必要はありません。同様に、サイトを Cisco Unity Express などの独立したボイス メッセージ システムでプロビジョニングできます。

Unified Communications サービスを分散させた場合の主な利点は、配置方法が WAN 接続の相対的な可用性およびコストに依存しないことです。たとえば、WAN 接続が使用できないか、極めて費用がかかるか、または信頼性が高くないリモートの場所でサイトを運用している場合、そのリモート サイト内で Cisco Unified Communications Manager Express などの独立したコール処理ノードをプロビジョニングすると、WAN がダウンしてもコール処理の中断が回避されます。

サービスのインターネットワーク化

2 つのサイトを独立したサービスでプロビジョニングした場合でも、両サイトを相互接続してサイト間で機能の透過性をある程度実現できます。たとえば、Cisco Unified Communications Manager Express でプロビジョニングした分散コール処理サービスを H.323 トランクまたは SIP トランクでインターネットワーク化して、サイト間で IP コールを許可できます。同様に、Cisco Unity Connection または Cisco Unity Express の独立したインスタンスを同じメッセージング ネットワークに参加させることによって、ユニファイド メッセージ ネットワーク内でメッセージをルーティングしたり、サブスクライバ情報およびディレクトリ情報を交換したりできます。

Unified Communications サービスの地理的多様性

一部のサービスを IP WAN 越しで複数の冗長なノードにプロビジョニングすると、停電やネットワーク障害でサイトが中断したり、火事や地震などの災害でサイトの物理的な整合性が損なわれたりしても、サービスを継続できます。

このような地理的多様性を実現するには、個々のサービスが冗長なノードをサポートするだけでなく、IP WAN の遅延と帯域幅の制約を越えてこれらのノードを配置できる必要があります。たとえば、ノード間のエンドツーエンドの合計ラウンドトリップ時間が 80 ms を超えず、適度な容量の QoS 対応帯域幅をプロビジョニングしている限り、Unified CM のコール処理サービスは単一クラスタのコール処理ノードを IP WAN 越しに配置できます。これに対して、Unified CME は冗長性を備えていないため、地理的に多様な構成に配置できません。

表 5-2 に、各 Cisco Unified Communications サービスを上記の方法で配置できるかどうかをまとめます。

表 5-2　Cisco Unified Communications サービスに使用可能な配置オプション

サービス	集中型	分散型	インターネットワーク化	地理的多様性
Cisco Unified CM	可	可	可	可
Cisco Unified CME	不可	可	可	不可
Cisco Unified CMBE 6000	可	可	可	可

表 5-2　Cisco Unified Communications サービスに使用可能な配置オプション（続き）

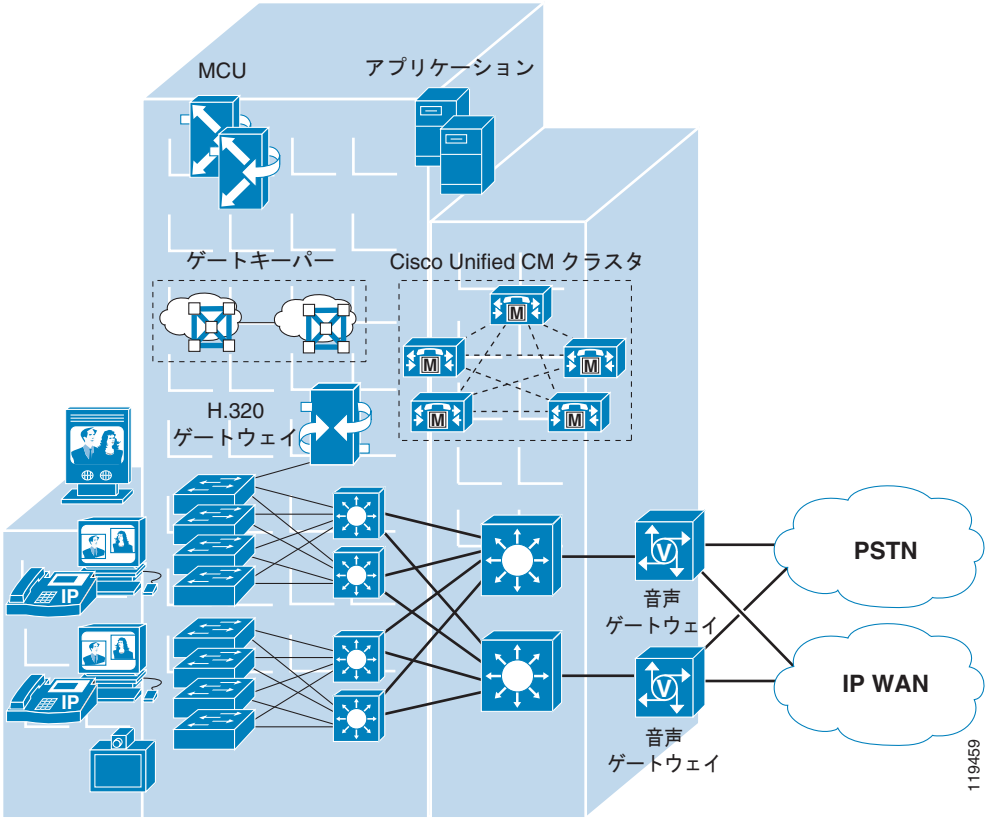
サービス	集中型	分散型	インターネットワーク化	地理的多様性
Cisco Unified CMBE 5000	可	可	可	不可
Cisco Unified CMBE 3000	可	不可	不可	不可
Cisco Unity Express	不可	可	可（Cisco Unified Messaging Gateway を使用）	不可
Cisco Unity	可	可（サイトごとに 1 つの Cisco Unity）	可（Cisco Unified Messaging Gateway を使用）	可
Cisco Unity Connection	可	可（サイトごとに 1 つの Cisco Unity Connection）	可（Cisco Unified Messaging Gateway を使用）	可
Cisco Emergency Responder	可	可（サイトごとに 1 つの Emergency Responder グループ）	可（Emergency Responder クラスタリングを使用）	可
Cisco Unified Presence	可	可（サイトごとに 1 つの Cisco Unified プレゼンス）	可（ドメイン間フェデレーションを使用）	不可
Cisco Unified Mobility	可	可（Unified CM シングル ナンバー リーチとして）	不可	可

コール処理は基本的なサービスであるため、この章では基本コール処理配置モデルについて説明します。Cisco Unified Communications Manager コール処理の技術的詳細については、「コール処理」（P.8-1）の章を参照してください。

キャンパス

このコール処理配置モデルでは、Unified Communications サービスとエンドポイントはキャンパスの同じ場所にあります。サービス ノード、エンドポイント、およびアプリケーション間の QoS 対応ネットワークは高い可用性を実現しており、帯域幅は事実上無制限で、エンドツーエンドの遅延は 15 ms 未満です。同様に、電源の品質および可用性は極めて高く、サービスは適切なデータセンター環境にホストされます。エンドポイント間の通信は、LAN または MAN を通過し、企業外部の通信は公衆網などの外部ネットワークを経由します。企業は、一般に LAN または MAN で接続された 1 つまたは複数のまとまったビルにキャンパス モデルを配置します。

図 5-1　キャンパス配置の例



キャンパス モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CM クラスタ。一部のキャンパス コール処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- 一方、小規模な配置では、Cisco Unified Communications Manager Business Edition（Unified CMBE）3000、CMBE 5000、または CMBE 6000 をキャンパスに配置できます。
- 1 つの Unified CM クラスタあたり最大 40,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone あるいは SCCP ビデオ エンドポイント。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- キャンパスの外部にある宛先へ向かうすべてのコール用のトランクやゲートウェイ（IP または公衆網）。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対応する、同じ場所のデジタル シグナル プロセッサ（DSP）リソース。
- メッセージング（ボイスメール）、プレゼンス、モビリティなどその他の Unified Communications サービスも一般に同じ場所に設置されます。
- PBX やボイスメール システムなど従来の音声サービスへのインターフェイスがキャンパス内に接続されるため、帯域幅または接続に運用コストがかかりません。

- マルチポイント ビデオ会議には、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323 および H.320 ビデオ ゲートウェイが必要です。
- サイト内のデバイス間では、広帯域オーディオ（G.722 や Cisco Wideband Audio など）が使用できます。
- サイト内のデバイス間では、広帯域ビデオ（384 kbps 以上など）が使用できます。7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec もサポートされます。

キャンパス モデルのベスト プラクティス

単一サイト モデルを実装する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- インフラストラクチャがハイ アベイラビリティで、QoS に対応し、復元性、高速コンバージェンス、およびインライン パワーを備えていることを確認します。
- 自社内のコール パターンを知っておく必要があります。キャンパス モデルは、大部分のコールが社内の同一サイトから発信されている場合、または社外の公衆網ユーザ宛てに発信されている場合に適用します。
- すべてのエンドポイントに G.711 コーデックを使用します。この方式を実施すると、トランスコーディングに対してデジタル シグナル プロセッサ（DSP）リソースを消費する必要がなくなり、その分のリソースは、会議や Media Termination Point（MTP; メディア ターミネーション ポイント）などの他の機能に割り当てることができます。
- ハイ アベイラビリティ、電話機用の接続オプション（インライン パワー）、Quality of Service（QoS）メカニズム、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています（「ネットワーク インフラストラクチャ」（P.3-1）を参照）。
- 「コール処理」（P.8-1）の章にリストされているプロビジョニングの推奨事項を実行します。

集中型コール処理を使用するマルチサイト

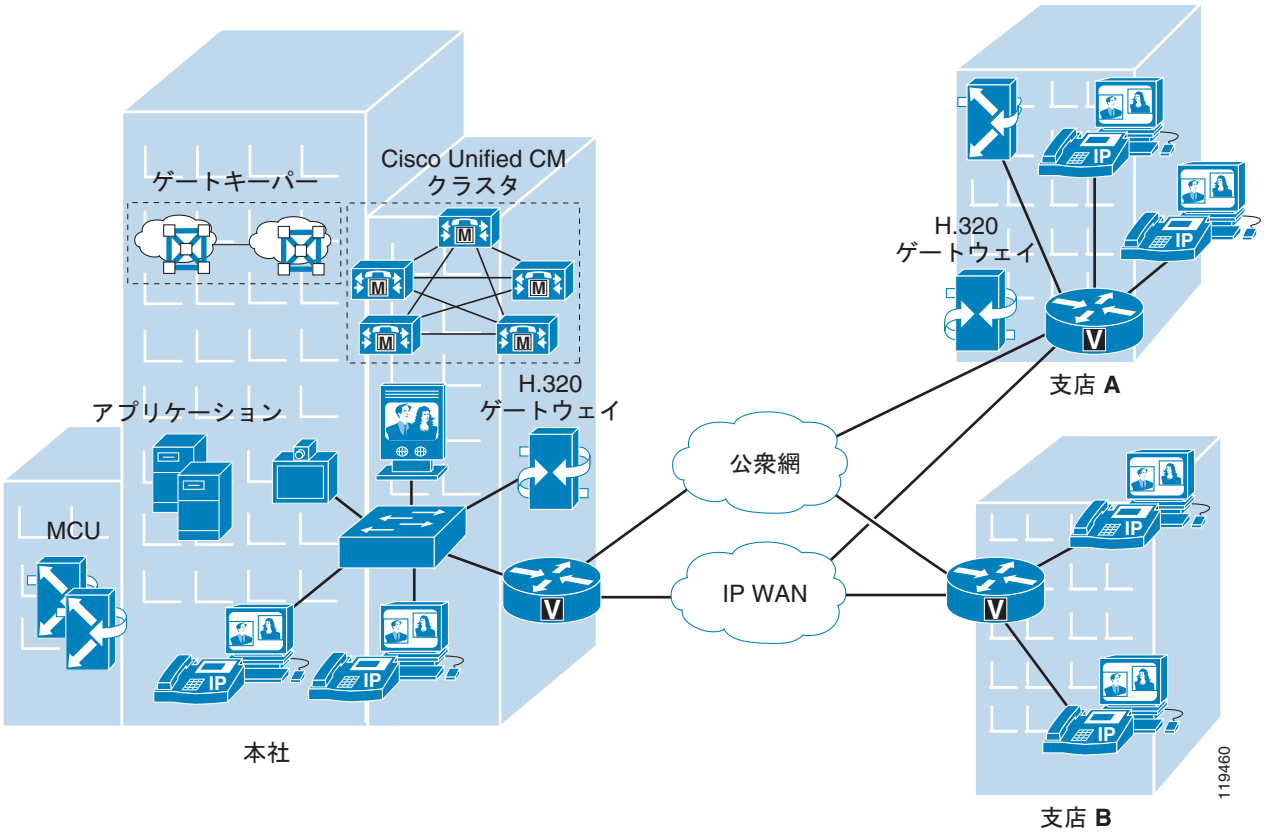
このコール処理配置モデルでは、エンドポイントは QoS 対応のワイド エリア ネットワークを越えてコール処理サービスとは離れた場所に置かれます。WAN 全体で利用できる帯域幅の容量が限られているため、特定の WAN リンクで認められるコールの数を管理して、負荷を使用可能な帯域幅の制限内に収めるには、コール アドミッション制御メカニズムが必要です。エンドポイント間のオンネット通信は、LAN/MAN（エンドポイントが同じサイトにある場合）または WAN（エンドポイントが異なるサイトにある場合）のいずれかを通過します。企業外部の通信は、エンドポイントと同じ場所または別の場所（たとえば、メイン サイトで集中型ゲートウェイを使用している場合や、企業ネットワーク全体で Tail End Hop Off（TEHO; テールエンド ホップオフ）を行っている場合）に配置できるゲートウェイを介して、公衆網などの外部ネットワークを経由します。

IP WAN は、中央サイトとリモート サイト間のコール制御シグナリングも伝送します。図 5-2 は、一般的な集中型コール処理配置を示しています。この配置では、中央サイトのコール処理エージェントとして Unified CM クラスタを使用し、すべてのサイトを接続するために、QoS 対応の IP WAN を使用します。この配置モデルでは、管理と保守全体のコストを削減するために、ボイス メッセージ、プレゼンス、モビリティなど他の Unified Communications サービスも中央サイトにホストすることがよく

あります。WAN の信用性が低い場合や、WAN 帯域幅のコストが高い場合には、サービスの可用性が WAN の障害の影響を受けないように、ボイス メッセージ（ボイスメール）など一部の Unified Communications サービスを分散させることができます。

（注）　このマニュアルで説明する集中型コール処理モデル用のソリューションでは、さまざまなサイトが QoS に対応した IP WAN に接続されます。

図 5-2　集中型コール処理を使用するマルチサイト配置



集中型コール処理を使用するマルチサイト モデルの設計上の特長は、次のとおりです。

- 単一の Unified CM クラスタ。一部の集中型コール処理配置では、複数の Unified CM クラスタが必要になる場合があります。たとえば、コールの対象となるエンドポイントの数が多すぎて単一のクラスタでは対応できない場合や、クラスタをコール センターなどの用途に限る必要がある場合などです。
- 小規模な配置では、Unified CMBE 3000 を最大 9 つのリモート サイトに対応する集中型コール処理構成で配置できます。
- Unified CMBE 5000 は、最大 19 のリモート サイトに対応する集中型コール処理構成で配置できます。
- Unified CMBE 6000 は、最大 49 のリモート サイトに対応する集中型コール処理構成で配置できます。
- 1 つのクラスタあたり最大 40,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone あるいは SCCP ビデオ エンドポイント。
- Unified CM クラスタあたり最大 2,000 のロケーションまたは支店サイト。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべてのオフネット コールのための公衆網接続。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）用のデジタル シグナル プロセッサ（DSP）リソースを各サイトにローカルに分散させて、DSP を必要とするコールが消費する WAN 帯域幅の容量を削減します。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。PBX やボイスメール システムなど従来の音声サービスへのインターフェイスを中央サイト内に接続できるため、帯域幅または接続に運用コストがかかりません。リモート サイトにある従来のシステムに接続するには、余分な WAN 帯域幅のプロビジョニングに伴う運用費が必要になる場合があります。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパーに登録することが必要です。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要です。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースが中央サイトに存在していても、ローカル会議リソースが必要な場合はリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイは中央サイトにあっても、ローカル ISDN アクセスが必要な場合はリモート サイトに分散していてもかまいません。
- サイト内のデバイス間では広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）を自動的に選択し、一方異なるサイトのデバイス間では狭帯域オーディオ（G.729 や G.728 など）を選択できます。
- 同じサイト内のデバイス間では広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間では狭帯域ビデオ（128 kbps など）を自動的に選択できます。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。
- WAN でビデオを発信するときには、WAN リンク速度を最低でも 768kbps 以上にする必要があります。

- Unified CM ロケーション（静的または RSVP 対応）では、コール アドミッション制御を提供します。
- 音声コールおよびビデオ コールの場合、帯域幅不足のためにコール アドミッション制御がコールを拒否したときには、Automated Alternate Routing（AAR; 自動代替ルーティング）により、公衆網を介して自動的にコールを再ルーティングできます。AAR は、ゲートウェイを利用して発信側電話機から公衆網へ向かうコールをルーティングし、着信側電話機に接続される別のゲートウェイを利用してリモート サイトで公衆網からのコールを受け付けます。
- リモート WAN リンク障害のためにエンドポイントが未登録であると見なされたときには、Call Forward Unregistered（CFUR）機能により、公衆網経由で自動的にコールを再ルーティングできます。CFUR は、ゲートウェイを利用して呼び出し元の電話機から公衆網へ向かうコールをルーティングし、呼び出し先の電話機に接続される別のゲートウェイを利用してリモート サイトで公衆網からのコールを受け付けます。
- ビデオ用 Survivable Remote Site Telephony（SRST）。WAN 接続で障害が発生すると、リモート サイトにある SCCP ビデオ エンドポイントが音声だけのデバイスになります。
- SRST ルータの代わりに Cisco Unified Communications Manager Express（Unified CME）を使用して、リモート サイトのサバイバビリティ（コール処理の継続）を確保することもできます。
- Cisco Unified Communications Manager Express（Unified CME）は、支店またはリモート サイトで Cisco Unity サーバと統合可能。Cisco Unity サーバは、中央サイトの Unified CM に通常モードで登録され、Unified CM が到達不能の場合や WAN の障害時は、Unified CME に SRST モードでフォール バックできます。これにより支店のユーザは、MWI を使用してボイスメールにアクセスできます。
- マルチサイト集中呼処理をサポートするその他の呼処理タイプと同様に、Cisco Unified CMBE 3000 でも中央サイトゲートウェイおよびリモート サイト ゲートウェイの両方を経由した PSTN ルーティングが可能です。ローカル PSTN ブレークアウト用にリモート サイトでローカル ゲートウェイを提供することは、リモート サイトのユーザに緊急サービスを提供する国では必要な要件です。リモート サイトのローカル ゲートウェイは、リモート サイト ロケーションのローカル PSAP にコール ルーティングを提供します。IP テレフォニー ネットワークと PSTN の分離を要件とする厳しい規制のある国では、リモート サイトのローカル PSTN ブレークアウトも必要または必須である場合があります。規制で許可されていれば、リモート サイト ゲートウェイを経由するローカル PSTN ブレークアウトを使用して、トール バイパスまたは Tail-end Hop Off（TEHO; テールエンド ホップ オフ）をイネーブルにできます。Unified CMBE 3000 は、設定された PSTN ゲートウェイへのルーティングをイネーブルにするための国ベースのダイヤル プラン設定、および PSTN アクセス制限を制御するポリシー メカニズムを提供します（当該国の規制に基づきます）。Unified CMBE 3000 は、MGCP で制御された Cisco 2901 Integrated Services Router（ISR; サービス統合型ルータ）を経由するローカル PSTN ブレークアウトのみをサポートします。
- Unified CMBE 3000 は、SRST またはリモート サイトのサバイバビリティはサポートしません。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- Multiprotocol Label Switching（MPLS）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）
- Voice and Video Enabled IP Security Protocol（IPSec; IP セキュリティ プロトコル）VPN（V3PN; 音声およびビデオ対応 IPSec VPN）

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの Quality of Service（QoS）メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。加えて、音声トラフィックによる WAN リンクのオーバーサブスクリプションや確立されたコールの品質低下を防止するために、コール アドミッション制御方式が必要です。集中型コール処理配置の場合は、Unified CM 内に設定された *ロケーション*（静的または RSVP 対応）でコール アドミッション制御が行われます（ロケーションの詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください）。

リモート サイトでは、さまざまな Cisco ゲートウェイにより、公衆網を介したアクセスが可能です。IP WAN で障害が発生した場合や、IP WAN 上で使用可能な帯域幅がすべて消費されてしまった場合でも、リモート サイトのユーザからのコールは、公衆網経由で再ルーティングできます。Cisco Unified Survivable Remote Site Telephony（SRST）機能は、SCCP および SIP 電話機の両方で使用可能です。Cisco Unified IP Phone が、リモートの 1 次、2 次、および 3 次 Unified CM への接続を失った場合、または WAN 接続がダウンした場合に、支店でのコール処理を提供します。Cisco Unified SRST 機能は、SRST 機能を実行する Cisco IOS ゲートウェイ、または SRST モードで動作する Cisco Unified CME で使用できます。SRST モードで動作する Unified CME では、Cisco IOS ゲートウェイの SRST よりも多くの機能が電話機に提供されます。

集中型コール処理モデルのベスト プラクティス

マルチサイトの集中型コール処理配置を実装する際は、次のガイドラインおよびベスト プラクティスに従ってください。

- 音声のカットスルー遅延（クリッピングとも呼ばれます）を減らすために、Unified CM とリモート ロケーション間の遅延を最小限に抑えます。
- Unified CM 内のロケーション（静的または RSVP 対応）でリモート支店との間のコール アドミッション制御が行われるように設定する。このメカニズムをさまざまな WAN トポロジに適用する方法については、「コール アドミッション制御」（P.11-1）の章を参照してください。
- 各リモート サイトでの Survivable Remote Site Telephony（SRST）モードでサポートされている IP Phone およびライン アピアランスの数は、その支店内にあるルータのプラットフォーム、取り付け済みメモリ容量、および Cisco IOS リリースにより異なります。Cisco IOS ゲートウェイの SRST では最大 1,500 台の電話機がサポートされますが、SRST モードで動作する Unified CME の場合は、最大 350 台です（SRST または Unified CME プラットフォームおよびコード仕様に関する詳細は、http://www.cisco.com から入手できる SRST および Unified CME の文書を参照してください）。ただし、一般的には、特定サイトに対して集中呼処理または分散型コール処理のいずれの方法を採用するかの選択は、次に示す種々の要素によって異なります。
  - IP WAN 帯域幅、または遅延制限
  - 音声ネットワークに関する臨界状況
  - 機能セットの必要性
  - スケーラビリティ
  - 管理の容易性
  - コスト

  お客様のビジネス ニーズに分散型コール処理モデルがふさわしいと判断する場合は、2 つの選択肢があります。各サイトに Unified CM クラスタをインストールする方法と、リモート サイトで Unified CME を稼動する方法です。

- リモート サイトでは、次の機能を使用して、WAN 障害が発生した場合のコール処理のサバイバビリティを確保します。
  - SCCP 電話機の場合は、Cisco IOS ゲートウェイの SRST を使用するか、SRST モードで動作する Unified CME を使用します。
  - SIP 電話機の場合は、SIP SRST を使用します。
  - MGCP 電話機の場合は、MGCP ゲートウェイ フォールバックを使用します。

  SRST または SRST モードの Unified CME、SIP SRST、および MGCP ゲートウェイ フォールバックは、同一の Cisco IOS ゲートウェイに相互に存在することができます。

リモート サイトのサバイバビリティ（コール処理の継続）

集中型コール処理モデルで WAN を介した Cisco Unified Communications を配置する場合、リモート サイトのデータ サービスと音声サービスのハイ アベイラビリティを確保するために、追加の処置が必要です。表 5-3 では、リモート サイトでのハイ アベイラビリティを実現するためのさまざまな方法をまとめています。これらの方法のいずれを選択するかは、ビジネスまたはアプリケーションの特殊な要件、可用性が高いデータ サービスと音声サービスに関連した優先順位、コストの考慮事項などの複数の要素によって異なります。

表 5-3　リモート サイトのハイ アベイラビリティを実現する方法

方法	データ サービスのハイ アベイラビリティ	音声サービスのハイ アベイラビリティ
支店ルータにおける冗長 IP WAN リンク	あり	あり
支店ルータの冗長プラットフォーム + 冗長 IP WAN リンク	あり	あり
データのみの ISDN バックアップ + SRST または Unified CME	あり	あり
データと音声の ISDN バックアップ	あり	あり（下記の規則を参照）
Cisco Unified Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME	なし	あり

表 5-3 にリストされている最初の 2 つのソリューションは、IP WAN アクセス ポイントに冗長性を追加して、リモート IP Phone と中央の Unified CM との間の IP 接続を常に保持することによって、ネットワーク インフラストラクチャ層に高い可用性を提供します。これらのソリューションは、データ サービスと音声サービスの両方に適用され、コール処理層からはまったく見えません。このオプションは、支店ルータでの冗長 IP WAN リンクの追加から、冗長 IP WAN リンクを備えた別の支店ルータ プラットフォームの追加までにわたります。

表 5-3 の 3 番めと 4 番めのソリューションでは、ISDN バックアップ リンクを使用して、WAN 障害時の存続可能性を提供します。ISDN バックアップ用には、次の 2 つの配置オプションがあります。

- データのみの ISDN バックアップ

  このオプションでは、ISDN はデータのみの存続可能性の確保に使用され、一方 SRST または SRST モードの Unified CME は音声のサバイバビリティの確保に使用されます。Skinny Client Control Protocol（SCCP）、H.323、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）、Session Initiation Protocol（SIP; セッション開始プロトコル）などのテレフォニー シグナリング プロトコルからのトラフィックが ISDN インターフェイスに入らないように支店ルータにアクセス コントロール リストを設定して、IP Phone からの信号が中央

サイトの Unified CM に到達しないようにする必要があることに注意してください。これにより、支店にあるテレフォニー エンドポイントは WAN の障害を検出し、ローカル SRST リソースを利用するようになります。

- データと音声の ISDN バックアップ

  このオプションでは、ISDN はデータと音声の両方の存続性を確保するのに使用されます。この場合、IP Phone は常に Unified CM クラスタとの IP 接続を保持するので、SRST または SRST モードの Unified CME は使用されません。しかし、データと音声のトラフィックの転送に ISDN を使用するのは、次の条件がすべて満たされる場合だけにすることをシスコは推奨します。

  - ISDN リンク上で音声トラフィックに割り当てられた帯域幅が、IP WAN リンク上で音声トラフィックに割り当てられた帯域幅と同じである。
  - ISDN リンクの帯域幅が固定されている。
  - 必要なすべての QoS 機能が、ルータの ISDN インターフェイスに配置されている。QoS の詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。

表 5-3 にリストされている 5 番めのソリューションでは、WAN 障害が検出された場合、Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME が、リモート オフィスのルータ内でコール処理機能のサブセットを提供し、IP Phone を拡張して、ローカル ルータ内のコール処理機能に「re-home」機能を提供することによって、音声サービスのみの高い可能性を提供します。図 5-3 では、SRST または SRST モードの Unified CME を使用した典型的なコールのシナリオを示しています。

図 5-3　Survivable Remote Site Telephony（SRST）または SRST モードの Unified CME

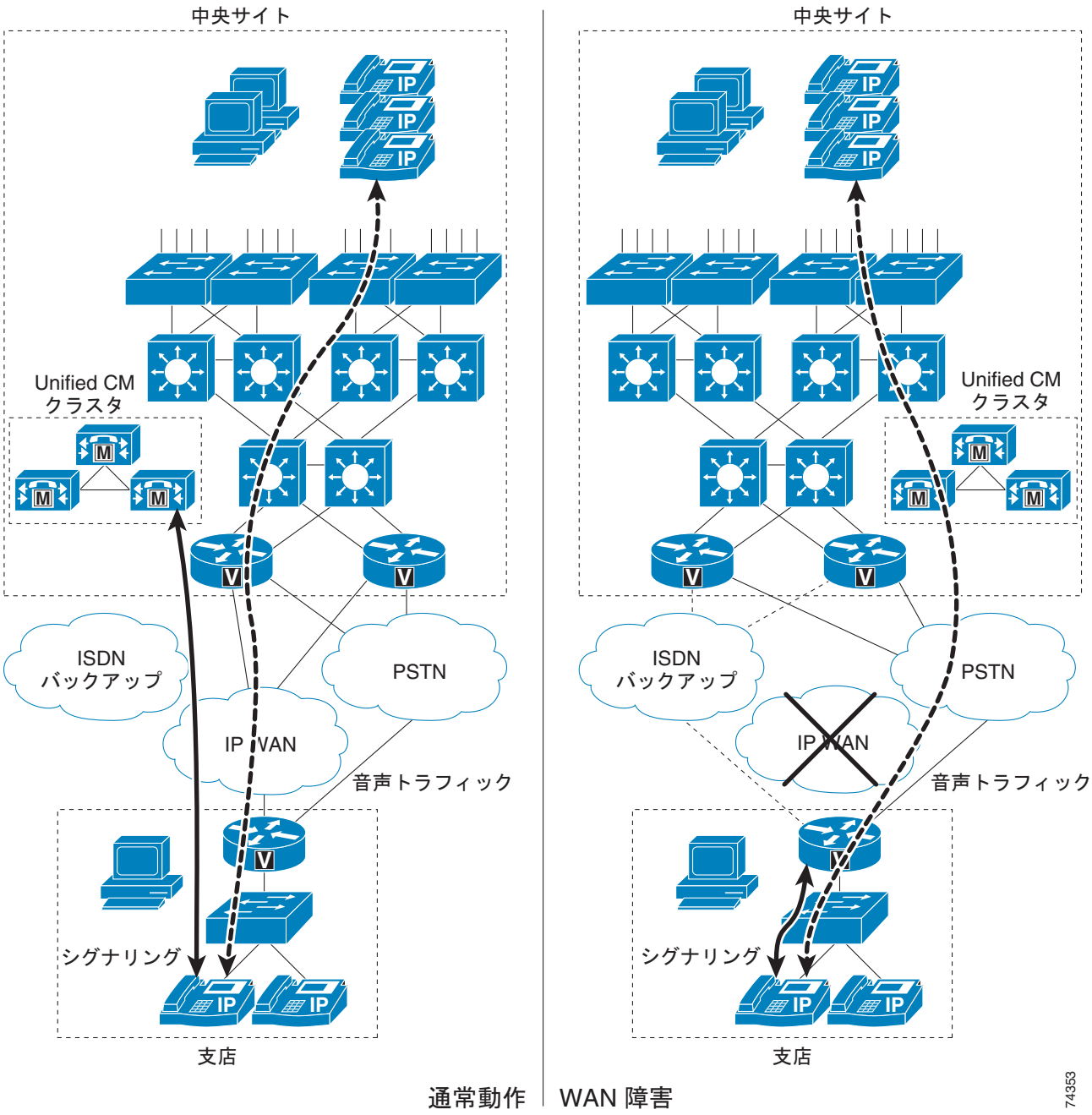


図 5-3 の左側に表示されている通常の動作では、支店は、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。支店の IP Phone は、中央サイトの Unified CM クラスタとコール シグナリング情報を交換し、IP WAN を介してコールを発信します。支店のルータまたはゲートウェイは、両方のタイプのトラフィック（コール シグナリングと音声）を透過的に転送し、IP Phone を認識しません。

支店との WAN リンクに障害が起きた場合、またはその他の何らかのイベントにより、Unified CM クラスタとの接続が失われた場合、支店の IP Phone は支店のルータに SRST モードで再登録されます。支店のルータ、SRST、または SRST モードで動作する Unified CME は、設定について IP Phone に照

会し、この情報を使用して独自の設定を自動的に作成します。支店の IP Phone は、支店のネットワーク内か、または公衆網を介してコールの発信と受信を行うことができます。電話機は「Unified CM fallback mode」というメッセージを表示し、Unified CM の一部の拡張機能が利用不能になり、電話機のディスプレイでグレー表示されます。

中央サイトとの WAN 接続が再度確立されると、支店の IP Phone は、Unified CM クラスタに自動的に再登録され、正常な動作に戻ります。支店の SRST ルータは、IP Phone についての情報を削除し、標準のルーティングまたはゲートウェイ設定に戻ります。SRST モードで動作する支店の Unified CME では、自動プロビジョニング オプションを使用することで、取得した電話機および回線の設定を、Unified CME ルータの実行設定に保存できます。**auto-provision none** が設定されている場合、自動でプロビジョニングされた電話機または回線の設定情報は、Unified CME ルータの実行設定に保存されません。そのため、IP Phone を交換して MAC アドレスが変更された場合でも、Unified CME での設定変更は必要ありません。

（注） 中央サイトとの WAN 接続が再度確立された場合、または Unified CM が再度到達可能になった場合でも、アクティブ コールを持つ SRST モードの電話機がただちに Unified CM に再登録されるわけではありません。再登録されるのは、そのようなアクティブ コールが終了してからです。

（注） 上記で説明したリモート サイトのサバイバビリティ機能は、Unified CMBE 3000 ではサポートされていません。

SRST モードの Unified CME

Unified CME が SRST モードで使用されている場合、ルータの SRST で使用できる機能よりも多くのコール処理機能が IP Phone に提供されます。コール プリザベーションや自動プロビジョニング、フェールオーバーといった SRST の機能に加え、SRST モードの Unified CME では、SCCP 電話機用に用意されている次のような Unified CME テレフォニー機能のほとんどを使用できます。

- ポケットベルによる呼び出し
- 会議
- ハント グループ
- Basic Automatic Call Distribution（B-ACD; 基本自動着信呼分配）
- コール パーク、コール ピックアップ、コール ピックアップ グループ
- オーバーレイ DN、ソフトキー テンプレート
- Cisco IP Communicator
- Cisco Unified Video Advantage
- MWI をサポートする Cisco Unity とのリモートサイトでの統合、および分散型の Microsoft Exchange または IBM Lotus Domino サーバとの統合

SRST モードの Unified CME では、WAN 障害が発生した場合に、SCCP 電話機に対するコール処理がサポートされます。ただし、SRST モードの Unified CME では、MGCP 電話機またはエンドポイントに対するフォールバックはサポートしていません。SIP プロキシ サーバまたは Unified CM への接続が失われた場合や、WAN 接続に障害が発生した場合に、SIP 電話機および MGCP 電話機がフォールバックできるようにするために、SRST フォール バック サーバとして動作している Unified CME サーバに、SIP SRST 機能と MGCP ゲートウェイ フォールバック機能の両方を追加で設定できます。

SRST モードの Unified CME のベスト プラクティス

- Unified CM での SRST 参照の IP アドレスとして、Unified CME の IP アドレスを使用します。
- Connection Monitor Duration は、SRST から Unified CM へのフォールバックを開始するまでに、電話機が WAN リンクをモニタする時間を指定するタイマーです。ほとんどの場合は、デフォルト設定の 120 秒を使用します。ただし、SRST モードの電話機が、フラッピングが発生しているリンクで Unified CM にフォールバックしたり復帰したりするのを防ぐために、Unified CM の Connection Monitor Duration パラメータをより長い期間に設定できます。これにより、電話機が SRST ルータと Unified CM の間で登録と再登録を繰り返すことがなくなります。電話機が長期間にわたって SRST から Unified CM にフォールバックしなくなるため、この値を極端に長い期間に設定しないでください。
- SRST フォールバック モードの電話機は、アクティブ状態になっても Unified CM に復帰しません。
- SRST フォールバック モードの電話機は、セキュア会議から非セキュア モードに戻ります。
- **auto-provision none** を設定し、取得された ephone-dn または ephone 設定が、Unified CME ルータの実行設定に書き込まれないようにします。これにより、IP Phone が交換された場合や、MAC アドレスが変更された場合に、設定を変更する必要がなくなります。

SRST モードの Unified CME の使用に関する詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html

SIP SRST の詳細については、次の Web サイトで入手可能な『*Cisco Unified SIP SRST System Administrator Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

MGCP ゲートウェイ フォールバックの詳細については、次の Web サイトで入手可能な『*Cisco CallManager and Cisco IOS Interoperability Guide*』の MGCP ゲートウェイに関する情報を参照してください。

http://www.cisco.com/en/US/docs/ios/12_3/vvf_c/interop/ccm_c.html

SRST ルータのベスト プラクティス

次の配置シナリオでは、SRST モードの Unified CME ではなく、Cisco Unified SRST ルータを使用します。

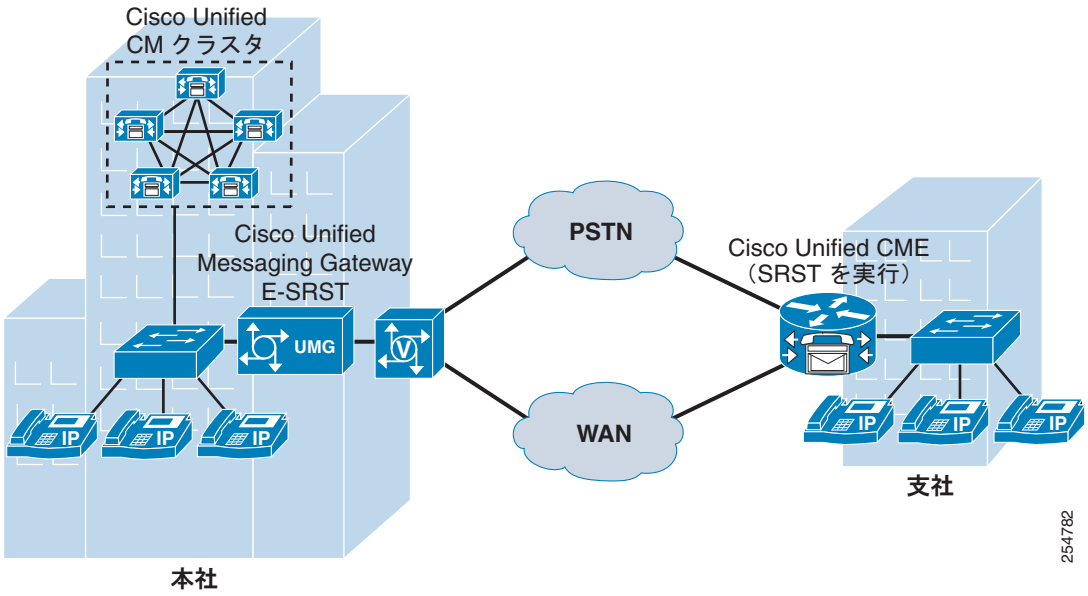
- 1 台の SRST ルータで、最大 1,500 台の電話機をサポートする場合。
- 最大 3,000 台の電話機をサポートする場合は、2 台の SRST ルータを使用します。各 SRST ルータ間でコールが相互にルーティングされるように、ダイヤル プランを正しく設定する必要があります。
- 基本的な SRST 機能の、単純な 1 回限りの設定を行う場合。
- Cisco Unified SRST（セキュア SRST）でのみ使用可能な SRTP メディア暗号化を使用する場合。
- Cisco VG248 音声ゲートウェイをサポートする場合。

到達不能または SRST ルータに登録されていない電話機のコールをルーティングする場合は、**alias** コマンドを使用。

Enhanced Survivable Remote Site Telephony

Enhanced Survivable Remote Site Telephony（E-SRST）によって、SRST を実行する Cisco Unified CME を支社に展開する作業が簡単になります。E-SRST アーキテクチャは Survivable Remote Site Voicemail（SRSV）に基づいて構築されています（図 5-4 を参照）。通常の操作時には、E-SRST は本社サイトにある Cisco Unified Messaging Gateway E-SRST を利用して、Cisco Unified CM から設定（コーリング サーチ スペース、パーティション、ハント グループ、コール パーク、コール ピックアップなど、設定されている場合）を定期的に取得し、同様の機能を持つ支社ルータにプロビジョニングして SRST モードで使用するためにその設定をアップロードします。E-SRST を使用すると、結果として SRST を実行する Unified CME で必要な手動の設定が減り、SRST モードでも通常モードでも同様のコール操作を実現できます。

図 5-4　Enhanced Survivable Remote Site Telephony の展開



E-SRST では、Unified CM 設定をアップロードして支社ルータにプロビジョニングするときに、WAN リンクからの帯域幅を消費します。E-SRST ソフトウェアではパケットのマーキングが実行されないため、E-SRST トラフィックはネットワーク上でベストエフォートとして伝送されます。シスコでは、このベストエフォート型マーキングを維持することを推奨します。これは IP Precedence 0（DSCP 0 または PHB BE）であり、リアルタイムの高優先度音声トラフィックに干渉しません。E-SRST トラフィックによる輻輳の発生を回避し、パケットのドロップ率を軽減するために、ピーク時以外の間（夜間や週末など）に設定のアップロードをスケジュールすることを推奨します。設定のアップロードは、Unified Messaging Gateway E-SRST Web インターフェイスで設定できます。

E-SRST の展開時には、次のガイドラインを考慮してください。

- Unified Messaging Gateway E-SRST では、最大で 1000 の SRST ノードがサポートされます。
- E-SRST がサポートされるのは、SRST を実行する Unified CME が搭載された支社ルータの場合のみです。
- E-SRST は、Cisco Unified Communications 500 シリーズ プラットフォームまたは Cisco Unified CM Business Edition ではサポートされません。
- 支社の音声ゲートウェイと SRST は、同じルータ内に設定されている必要があります。

- Unified Messaging Gateway E-SRST による設定のアップロードの場合、ハイ アベイラビリティのサポートはありません。Unified Messaging Gateway を使用可能な場合、設定のアップロードは実行できません。
- E-SRST および SRSV の展開には、同じ Unified Messaging Gateway および SRST を実行する Unified CME を使用する必要があります。この場合、SRST と SRSV は、合計で 1,000 ノードまでサポートできます。
- 本社と支社の間に NAT が使用されている展開では、E-SRST はサポートされません。
- セキュア Unified CME 接続は E-SRST ではサポートされません。

（注）　上記で説明したリモート サイトの拡張サバイバビリティ機能は、Cisco Unified CMBE 3000 ではサポートされていません。

集中型コール処理のバリエーションとしての Voice Over the PSTN

集中型コール処理配置は、サイト間音声メディアが WAN の代わりに公衆網を介して送信されるように調整できます。このように設定された場合、すべてのテレフォニー エンドポイントのシグナリング（呼制御）は、引き続き中央の Unified CM クラスタによって制御されます。したがって、この Voice over the PSTN（VoPSTN）モデル バリエーションでも、シグナリング トラフィック用に設定された適切な帯域幅を持つ、QoS 対応の WAN が必要になります。

VoPSTN は、次のいずれかの方法で実装できます。

- Automated Alternate Routing（AAR; 自動代替ルーティング）機能を使用する（AAR の詳細については、「Automated Alternate Routing」（P.9-103）の項を参照してください）。
- Unified CM と公衆網ゲートウェイの両方のダイヤル プラン構成要素を組み合せて使用する。

VoPSTN が魅力的なオプションとなる可能性があるのは、IP WAN 帯域幅が不足しているか、または公衆網料金と比較して高価である配置や、Cisco Unified Communications システムがすでに配置されている状況で IP WAN 帯域幅のアップグレードを計画している配置です。

（注）　VoPSTN 配置では、Unified CM 機能セットの一部を削減した基本的な音声機能が提供されます。

システム設計者は、実装時の選択内容に関係なく、特に次の問題に対処する必要があります。

- 集中型ボイスメールには、次の要件があります。
  - 配置に含まれているすべてのロケーションに対して Redirected Dialed Number Identification Service（RDNIS）エンドツーエンドをサポートする、テレフォニー ネットワーク プロバイダー。RDNIS は、ボイスメールにリダイレクトされるコールがリダイレクト元の DN を搬送するために必要となります。その結果、ボイスメール ボックスが正しく選択されることが保証されます。
  - ボイスメール システムが MGCP ゲートウェイを介してアクセスされる場合、ボイスメールのパイロット番号は完全修飾 E.164 番号である必要があります。
- エクステンション モビリティ機能は、単一の支店サイトにある IP Phone に制限されます。
- オンネット（クラスタ内）コールはすべて、オフネット（公衆網）コールと同じコール トリートメントによって宛先の電話機に送信されます。この対象には、Missed Calls や Received Calls などのコール ディレクトリに送信される桁数も含まれます。

- 支店間コールはそれぞれ、2 つの独立した Call Detail Record（CDR; コール詳細レコード）を生成します。1 つは、発信側の電話機から公衆網へのコール レッグに対応するもので、もう 1 つは、公衆網から着信側の電話機へのコール レッグに対応するものです。
- オンネット コールとオフネット コールの呼出音タイプを区別する手段はありません。
- 宛先の電話機すべてにおいて、直接発信できる完全修飾 Direct Inward Dial（DID; ダイヤルイン方式）の公衆網番号が必要になります。DID 以外の DN に別の支店サイトから直接到達することはできません。
- VoPSTN を使用する際、Music On Hold（MoH; 保留音）は、保留側が MoH リソースと同じ場所にある場合に限り使用されます。MoH サーバが中央サイトに配置されている場合は、中央サイトのデバイスによって保留にされたコールのみが保留音を受信します。
- 支店サイトの外部の宛先に着信転送すると、支店のゲートウェイを介したヘアピン コールが発生します。支店のゲートウェイのトラフィック エンジニアリングを、必要に応じて調整する必要があります。
- 支店のゲートウェイに着信するコールを支店サイトの外部の宛先にコール転送すると、ゲートウェイを介したヘアピン コールが発生し、2 つのトランク ポートが使用されます。この動作は、次の場合に発生します。
  - 支店の外部にあるボイスメール システムにコールが転送される場合
  - 別の支店にあるオンネットの内線番号にコールが転送される場合

  支店と公衆網を接続するトランクのサイジングを行うときは、このコール転送フローによるゲートウェイ ポートの使用率を考慮する必要があります。
- 会議リソースは、会議を開始する電話機と同じ場所にある必要があります。
- VoPSTN は、中央サイトに IP オーディオのストリーミングを要求する（つまり、ゲートウェイを通過しない）アプリケーションをサポートしません。このアプリケーションには、次のようなものがあります。
  - 集中型 Music On Hold（MoH; 保留音）サーバ
  - Interactive Voice Response（IVR）
  - CTI ベースのアプリケーション
- 中央サイトの外部で Attendant Console を使用する場合、リモート サイトがキャッシングしないで大規模なユーザ アカウント ディレクトリにアクセスする必要があるときは、かなり大きな帯域幅が必要になることがあります。
- 支店間メディア（着信転送を含む）はすべて公衆網を介して送信されるため、支店間トラフィック、着信転送、および集中型ボイスメール アクセスのすべてを収容できるように、ゲートウェイ トランク グループの回線数を調整する必要があります。
- シェアドラインを支店間に配置して、回線を共有するデバイスを別々の支店に配置することは避けるよう推奨します。

このような一般的な考慮事項のほか、以降の項では、次の実装方法のそれぞれに固有の推奨事項や問題について説明します。

- 「AAR を使用する VoPSTN」（P.5-22）
- 「ダイヤル プランを使用する VoPSTN」（P.5-23）

AAR を使用する VoPSTN

この方法では、Unified CM ダイヤル プランを従来の集中型コール処理配置として設定し、さらに Automated Alternate Routing（AAR; 自動代替ルーティング）機能を正しく設定します。コール アドミッション制御のロケーション メカニズムによって、新たなコールを受け入れるのに十分な WAN 帯域幅がないと判別された場合、AAR は、サイト間コールを公衆網を介して透過的に再ルーティングします。

公衆網をプライマリ（および唯一の）音声パスとして使用するには、各ロケーション（支店サイト）のコール アドミッション制御の帯域幅を 1 Kbps に設定します。この設定により、すべてのコールが WAN を通過することが防止されます。このように設定されている場合、サイト間コールはすべて AAR 機能をトリガーし、AAR 機能は公衆網を介してコールを再ルーティングします。

VoPSTN の AAR 実装方法には、次の利点があります。

- 完全な Cisco Unified Communications の配置に簡単に移行できます。WAN を介した音声メディアをサポートする帯域幅が使用可能になった場合、ダイヤル プランはそのまま保持できるため、変更作業としては、サイトごとにロケーション帯域幅の値をアップデートするだけで済みます。
- 通話中のコールバックなど、一部の付加機能がサポートされます。

AAR 実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

- AAR 機能を正しく設定する必要があります。
- 一般に、サポートされているデバイスには、IP Phone、ゲートウェイ、およびアナログ電話機を収容するゲートウェイがあります。
- 支店間コールが AAR を使用できるのは、宛先デバイスが IP Phone または Cisco Unity ポートの場合のみです。
- 他のエンドポイントに対する支店間コールは、完全修飾 E.164 番号を使用する必要があります。
- すべてのオンネット支店間コールでは、「Network congestion, rerouting」というメッセージが表示されます。
- 宛先の電話機が（WAN 接続の通信断などのため）登録から外れている場合、AAR 機能が呼び出されないため、短縮ダイヤルは Call Forward Unregistered（CFUR）が設定されている場合にだけ使用できます。宛先の電話機が SRST ルータに登録されている場合は、その公衆網 DID 番号を直接ダイヤルすることで、宛先に到達することもできます。
- 発信側の電話機が（WAN 接続の通信断などのため）登録から外れている場合、その電話機は SRST（または SRST として機能する Unified CME）モードに移行します。このような条件の下でも短縮ダイヤルを機能させるには、SRST（または SRST として機能する Unified CME）ルータに、宛先の短縮ダイヤル形式を照合して公衆網が宛先へコールをルーティングするのに必要な形式に変換するという変換ルールを設定します。
- 同じ支店内のシェアドラインは、その支店のコーリング サーチ スペースのみに含まれているパーティション内に設定される必要があります。シェアドラインへのサイト間アクセスには、次のどちらかの操作が必要です。
  - 発信側サイトでシェアドラインの DID 番号をダイヤルします。
  - シェアドラインへのサイト間短縮ダイヤルが必要な場合は、ユーザがダイヤルした短縮ストリングをシェアドラインの DID 番号へと変換するトランスレーション パターンを使用します。

（注） この場合、シェアドラインの DN を別の支店から直接ダイヤルすると、AAR ベースの公衆網コールが複数トリガーされます。

ダイヤル プランを使用する VoPSTN

この方法は、Unified CM 内の特定のダイヤル プラン設定と公衆網ゲートウェイを利用して、すべてのサイト間コールを公衆網を介してルーティングします。ダイヤル プランでは、各サイトの IP Phone の DN を別のパーティションに配置する必要があります。また、その DN のコーリング サーチ スペースは、サイトの内部パーティションと、ローカル公衆網ゲートウェイが関連付けられているルート パターンのみにアクセスする必要があります。

サイト間短縮ダイヤルは、各支店サイトの変換セット（支店サイトごとに 1 セット）からも使用可能です。この変換は、Cisco IOS 内の H.323 ゲートウェイと変換ルールを使用して行うのが最適です。

VoPSTN のダイヤル プラン実装方法には、次の利点があります。

- AAR が必要ないため設定が容易になります。
- 発信側または宛先側のどちらかで WAN 障害が発生した状態でも、短縮ダイヤルは自動的に動作します。これは、H.323 ゲートウェイ内の Cisco IOS 変換ルールが SRST モードで有効になるためです。

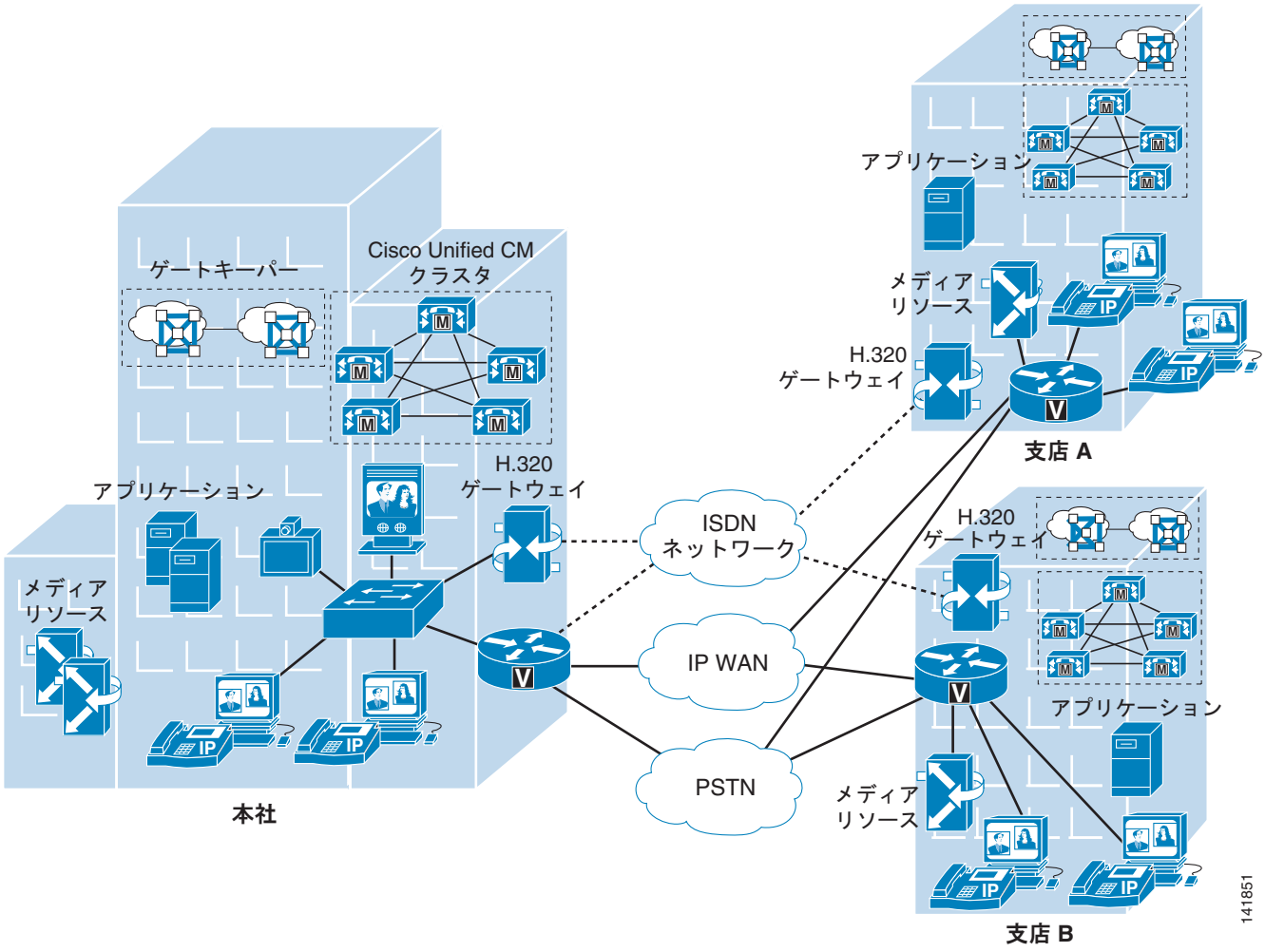
ダイヤル プラン実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

- 通話中のコールバックなど、付加機能はサポートされません。
- CTI ベースのアプリケーションの中には、重複している内線番号（つまり、別々のパーティションにあるが、同じ DN が設定されている複数の電話機）をサポートしないものがあります。
- 完全な Cisco Unified Communications の配置に簡単に移行することはできません。これは、ダイヤル プランの再設計が必要になるためです。

分散型コール処理を使用するマルチサイト

分散型コール処理を使用するマルチサイト配置のモデルは、複数の独立したサイトから構成されています。各サイトには独自のコール処理エージェント クラスタがあり、そのエージェント クラスタは、分散されたサイト間の音声トラフィックを伝送する IP WAN に接続されます。図 5-5 は、標準的な分散型コール処理配置を示しています。

図 5-5　分散型コール処理を使用するマルチサイト配置



分散型コール処理モデルの各サイトは、次のいずれかになります。

- 独自のコール処理エージェントを使用する単一サイト。コール処理エージェントは、次のいずれかになります。
  - Cisco Unified Communications Manager（Unified CM）
  - Cisco Unified Communications Manager Business Edition（Unified CMBE）5000 および Unified CMBE 6000
  - Cisco Unified Communications Manager Express（Unified CME）
  - その他の IP PBX

- 集中型コール処理サイトと、それに関連したすべてのリモート サイト。
- Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX。

分散型コール処理を使用するマルチサイト モデルの設計上の特長は、次のとおりです。

- 1 つのクラスタあたり最大 40,000 の設定済みおよび登録済み Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone あるいは SCCP ビデオ エンドポイント。
- Unified CM クラスタごとに最大 2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）用のデジタル シグナル プロセッサ（DSP）リソースを各サイトにローカルに分散させて、DSP を必要とするコールが消費する WAN 帯域幅の容量を削減します。
- ボイスメール、ユニファイド メッセージング、および Cisco Unified Presence の各コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパーに登録することが必要です。Unified CM は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。Cisco IOS ゲートキーパーを使用して、分散した Unified CM クラスタ間でコール ルーティングおよび帯域幅管理を提供することもできます。多くの場合、Unified CM クラスタごとに専用のエンドポイント ゲートキーパーを持ち、それとは別のゲートキーパーを使用してクラスタ間コールを管理することを推奨します。状況によっては、ネットワークのサイズやダイヤル プランの複雑さに応じて、同じゲートキーパーを両方の機能に使用することもできます（詳細については、「ゲートキーパー」（P.12-25）を参照してください）。
- マルチポイント ビデオ会議のクラスタごとに MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースがリージョン サイトに存在していても、ローカル会議リソースが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網上で H.320 ビデオ会議デバイスと通信するために H.323/H.320 ビデオ ゲートウェイが必要です。これらのゲートウェイはリージョン サイトにあっても、ローカル ISDN アクセスが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。ただし、Cisco VT Camera Wideband Video Codec はクラスタ間トランクでサポートされていません。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。
- コール アドミッション制御は、同じ Unified CM クラスタで制御されるサイト間のコールに対しては Unified CM のロケーションから提供。Unified CM クラスタ間のコールに対しては Cisco IOS ゲートキーパーから提供されます（クラスタ間トランク）。

IP WAN は、分散型コール処理のサイトをすべて相互接続します。一般に、公衆網は、IP WAN 接続に障害が起きたか、使用可能な帯域幅がすべて消費されてしまった場合に、サイト間のバックアップ接続の役目を果たします。公衆網のみで接続されているサイトは、独立サイトであり、分散型コール処理モデルには含まれません（「キャンパス」（P.5-7）を参照）。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- Multiprotocol Label Switching（MPLS）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）
- Voice and Video Enabled IP Security Protocol（IPSec; IP セキュリティ プロトコル）VPN（V3PN; 音声およびビデオ対応 IPSec VPN）

分散型コール処理モデルのベスト プラクティス

分散型コール処理を使用するマルチサイト配置には、単一サイトと同じ、または集中型コール処理を使用するマルチサイト配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください（「キャンパス」（P.5-7）および「集中型コール処理を使用するマルチサイト」（P.5-9）を参照）。

ゲートキーパーまたは Session Initiation Protocol（SIP）プロキシ サーバは、マルチサイトの分散型コール処理配置の重要な要素です。どちらもダイヤル プランの解決を行います。さらに、ゲートキーパーは、コール アドミッション制御も行います。ゲートキーパーは、コール アドミッション制御と E.164 ダイヤル プラン解決を実行する H.323 デバイスです。

ゲートキーパーの使用には、次のベスト プラクティスが適用できます。

- Cisco IOS ゲートキーパーを使用して、各サイトとのコール アドミッションを制御します。
- ゲートキーパーの有効性を高めるには、Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）ゲートキーパー ペア、ゲートキーパーのクラスタリング、および代替ゲートキーパー サポートを使用します。さらに、ネットワーク内の冗長性を確実にするために複数のゲートキーパーを使用します（「ゲートキーパーの設計上の考慮事項」（P.8-46）を参照）。
- プラットフォームの規模を適切に調整して、パフォーマンスとキャパシティの要件が満たされることを確認します。
- WAN 上のコーデックは 1 つのタイプに限定して使用します。これは、H.323 仕様では、レイヤ 2、IP、UDP（User Data Protocol）、または RTP（Real-time Transport Protocol）ヘッダーのオーバーヘッドが、帯域幅要求で許可されないからです（ヘッダーのオーバーヘッドは、パケットのペイロードまたは符号化された音声部分のみで許可されます）。WAN 上で使用するコーデックを 1 つのタイプに限定すると、最悪のシナリオに備えて IP WAN を過剰にプロビジョニングする必要がなくなるので、キャパシティ プランニングが簡単になります。
- ゲートキーパー ネットワークは、数百単位のサイトにスケーラブルです。また、設計上の制限は WAN トポロジからしか受けません。

ゲートキーパーが実行する各種機能の詳細については、次の項を参照してください。

- ゲートキーパーのコール アドミッション制御については、「コール アドミッション制御」（P.11-1）を参照してください。
- ゲートキーパーのスケーラビリティと冗長性については、「コール処理」（P.8-1）を参照してください。

- ゲートキーパーのダイヤル プラン解決については、「ダイヤル プラン」（P.9-1）を参照してください。

SIP デバイスは、E.164 番号と SIP ユニフォーム リソース識別子（URI）を解決して、エンドポイント間で相互にコールを発信できるようにします。Unified CM は、E.164 番号の使用のみをサポートします。

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

- SIP プロキシの適切な冗長性を確保します。
- SIP プロキシのキャパシティが、ネットワークに必要なコール レートおよびコール数に対応していることを保証します。
- コール アドミッション制御のプランニングは、このドキュメントの対象外です。

分散型コール処理モデルのコール処理エージェント

コール処理エージェントの選択は、多くの要素によって異なります。設計での主な要素は、サイトの規模および機能要件です。

分散型コール処理配置の場合、各サイトには独自のコール処理エージェントがあります。各サイトの設計は、コール処理エージェント、必要な機能、および必要な耐障害性によって変わります。たとえば、500 台の電話機を備えたサイトでは、2 台のサーバを含む Unified CM クラスタは、1 対 1 の冗長性を提供することができ、バックアップ サーバは、パブリッシャおよび Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）サーバとして使用されます。

IP ベース アプリケーションの要件も、コール処理エージェントの選択に大きな影響を与えます。これは、多くの Cisco IP アプリケーションをサポートするのは、Unified CM だけであるからです。

表 5-4 は、推奨されるコール処理エージェントを示しています。

表 5-4　推奨されるコール処理エージェント

コール処理エージェント	推奨規模	備考
Cisco Unified Communications Manager Express（Unified CME）	最大 450 台の電話機	• 小規模なリモート サイト用 • キャパシティは Cisco IOS プラットフォームに依存する
Cisco Unified Communications Manager Business Edition（Unified CMBE）5000	最大 575 台の電話機	• 小規模なサイト用 • 集中型または分散型コール処理をサポートする
Cisco Unified Communications Manager Business Edition（Unified CMBE）6000	最大 1,200 台の電話機	• 小中規模サイト用 • 集中型または分散型コール処理をサポートする
Cisco Unified Communications Manager（Unified CM）	50 ～ 40,000 台の電話機	• Unified CM クラスタの規模に応じて、小規模から大規模までのサイト • 集中型または分散型コール処理をサポートする
VoIP ゲートウェイを備えた従来の PBX	PBX に依存する	• IP WAN コール数と機能は、PBX と VoIP ゲートウェイを接続するプロトコルおよびゲートウェイ プラットフォームによって異なる

同じシステムに複数のコール処理エージェントが存在する場合は、他のエージェントを認識するように各エージェントを手動で設定できます。また、Cisco Service Advertisement Framework（SAF）を使用して、コール エージェント間でコール ルーティングおよびダイヤル プラン情報を自動的に共有することもできます。SAF の詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）を参照してください。

Unified CM Session Management Edition

Cisco Unified Communications Manager Session Management Edition を使用するユニファイド コミュニケーションの配置は、マルチサイトの分散型コール処理配置モデルのバリエーションであり、一般に、1 つのフロントエンド システム（この場合は Unified CM Session Management Edition）を介して多数のユニファイド コミュニケーション システムを相互接続するために採用されます。この項では、Unified CM Session Management Edition の配置に関する設計上の考慮事項について説明します。

Cisco Unified CM Session Management Edition は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフ システムと呼ばれる、複数のユニファイド コミュニケーション システムを集約できます。

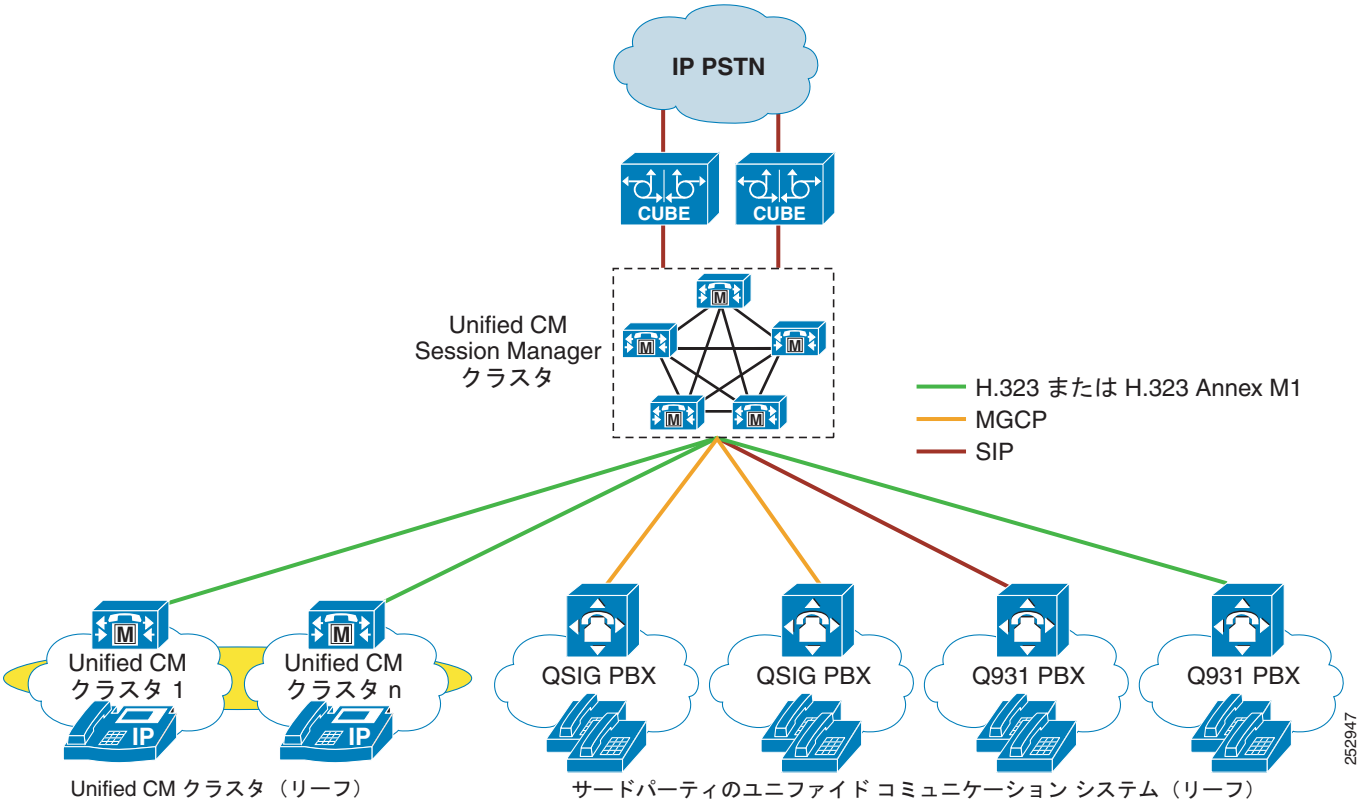
Session Management Edition の配置は、複数の PBX 配置とそれに関連する電話を、IP 電話があり比較的少数のトランクを持つ Unified CM クラスタに移行するために使用できます。Session Management Edition クラスタをサードパーティの PBX を相互接続する多数のトランクで開始し、何千もの IP 電話を持つ Unified CM クラスタ配置に徐々に移行することも可能です。

Cisco Unified CM 8.0 以降のリリースでは、Unified CM Session Management Edition で次の機能がサポートされています。

- H.323 Annex M1 クラスタ間トランク
- SIP クラスタ間トランク
- SIP トランク
- H.323 トランク
- MGCP トランク
- 音声コール
- ビデオ コール
- 暗号化されたコール
- FAX コール

また、Unified CM Session Management Edition を使用して、IP 公衆網接続、PBX、集中型のユニファイド コミュニケーション アプリケーションなど、サードパーティのユニファイド コミュニケーション システムに接続できます（図 5-6 を参照）。ただし、標準の Unified CM クラスタと同様に、サードパーティ デバイスからの Unified CM Session Management Edition への接続は、実稼動環境で使用する前に相互運用性をテストしたシステムである必要があります。

図 5-6　Unified CM Session Management Edition を使用したマルチサイト配置



Unified CM Session Management Edition を配置する状況

次のいずれかの操作を行う場合は、Unified CM Session Management Edition を配置することを推奨します。

- 集中型ダイヤル プランを作成および管理

  他のすべてのユニファイド コミュニケーション システムに接続するために各ユニファイド コミュニケーション システムに別個のダイヤル プランおよびトランクを設定するのではなく、Unified CM Session Management Edition を使用すると、Session Management クラスタを指す簡潔なダイヤル プランおよびトランクをリーフのユニファイド コミュニケーション システムに設定できます。Unified CM Session Management Edition には、集中型ダイヤル プランと、他のすべてのユニファイド コミュニケーション システムに到達するためのこのプランに対応する情報が含まれています。

- 集中型公衆網アクセスを提供

  Unified CM Session Management Edition を使用すると、1 つ（または複数）の IP 公衆網トランクに公衆網アクセスを集約できます。集中型公衆網アクセスには一般に、支店ベースの公衆網回線の削減または排除を伴います。

- アプリケーションを集中化

  Unified CM Session Management Edition の配置によって、会議やビデオ会議などの一般に使用されるアプリケーションを直接 Session Management クラスタに接続できるため、複数のトランクの管理によるリーフ システムへのオーバーヘッドが軽減されます。

- Unified Communications システムに移行するために PBX を集約

  Unified CM Session Management Edition は、レガシー PBX から Cisco Unified Communications システムへの移行の一環として、複数の PBX の集約ポイントを提供できます。

Unified CM Session Management Edition と標準の Unified CM クラスタの相違

Unified CM Session Management Edition ソフトウェアは、Unified CM と同じです。ただし、このソフトウェアは、この新しい配置モデルの要件と制約を満たすために大幅に強化されています。Unified CM Session Management Edition は、多数のトランクツートランク接続をサポートするように設計されているため、次に示す設計上の考慮事項に従う必要があります。

- キャパシティ

  Unified CM Session Management クラスタは、リーフの Unified Communications システム間（Unified CM クラスタと PBX など）、集中型 IP 公衆網接続間、および集中型アプリケーションへの予想される BHCA トラフィック ロードに基づいて正確にサイジングすることが重要です。使用している Unified Communications システムでのユーザの平均的な BHCA およびコール保持時間を判断し、その情報をシスコ アカウント システム エンジニア（SE）またはシスコ代理店と共有して、Unified CM Session Management Edition クラスタの規模を適切に決定してください。

- トランク

  可能な場合は、Unified CM トランクに静的な MTP を使用しないでください（つまり、リーフまたは Session Management Unified CM SIP または H.323 トランクに対する [MTP required] チェックボックスをオフにします）。[MTP required] を使用しないトランクの場合、コーデックの選択の幅が広がり、音声、ビデオ、および暗号化がサポートされ、トランク コールは MTP リソースに固定されません。トランクでは、動的に挿入された MTP を使用できます（たとえば、インバンドからアウトオブバンドに DTMF を変換する場合など）。サードパーティのユニファイド コミュニケーション システムで CM Early Offer が必要とされる場合は、Unified CM SIP トランクで [Early Offer support for voice and video calls (insert MTP if needed)] を使用するか、Cisco Unified Border Element と一緒に [Delayed Offer to Early Offer] 機能を使用します。トランクでは、動的に挿入された MTP を使用できます（たとえば、インバンドからアウトオブバンドに DTMF を変換する場合など）。

- Unified CM バージョン

  Unified CM Session Management Edition と Unified CM リーフ クラスタの両方とも、Cisco Unified CM 7.1(2) 以降のリリースと一緒に配置する必要があります。それよりも前のバージョンの Unified CM も配置できますが、クラスタを Unified CM 7.1(2) 以降のリリースにアップグレードしないと解決できない問題が発生する可能性があります。

- 相互運用性

  ほとんどのベンダーが標準に準拠していますが、各ベンダーによるプロトコルの実装には相違があります。標準の Unified CM クラスタの場合と同様に、実稼動環境にシステムを配置する前に、サードパーティの未検証のユニファイド コミュニケーション システムとのエンドツーエンドの相互運用性テストを実施することを強く推奨します。相互運用性テストでは、Unified CM Session Management クラスタを介したシスコおよびサードパーティのリーフ システムからのコール フローと機能を検証します。シスコの相互運用性チームによってテストされたサードパーティのユニファイド コミュニケーション システムの情報を得るには、次の Cisco Interoperability Portal サイトで提供している情報を参照してください。

  http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/interOp_ucSessionMgr.html

- 着信コールと発信コールのロード バランシング

  Session Management クラスタ内の Unified CM サーバ間に着信コールと発信コールが均等に分散されるよう、Unified CM Session Management Edition およびリーフのユニファイド コミュニケーション システムのトランクを設定します。トランク コールのロード バランシングの詳細については、「Cisco Unified CM トランク」（P.14-1）の章を参照してください。

- 設計のガイドラインとサポート

  Unified CM Session Management Edition の設計と展開の詳細については、次の URL の『*Cisco Unified Communications Manager Session Management Edition Deployment Guide*』を参照してください。

  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/session_mgmt/deploy/8_5_1/cucmse-851-deploy.html

  Unified CM Session Management Edition の設計は、担当のシスコ SE が Cisco Unified CM Session Management チームと一緒に確認します。Unified CM Session Management Edition の設計確認プロセスの詳細について、シスコ代理店および従業員は次の Web サイトにある資料を参照できます。

  http://docwiki.cisco.com/wiki/Unified_Communications_Manager_-_Session_Manager_Edition

Session Management Edition を配置する場合の設計上の考慮事項

ここで示す設計上の考慮事項とガイドラインは、Cisco Unified CM Session Management Edition の配置に当てはまるものです。

Session Management Edition と SAF CCD Deployments

Session Management Edition の配置は、内部ダイヤル プランの集約を提供します。Cisco Service Advertisement Framework（SAF）Call Control Discovery（CCD; コール制御ディスカバリ）の配置は、内部ダイヤル プランと対応する外部「To PSTN」ダイヤル プランの両方を、参加している SAF CCD Unified Communications システムに分散させます。Session Management Edition と SAF CCD を組み合せることにより、Session Management Edition がすべてのリーフ Unified Communications システムに対して中央のセッション マネージャとして機能する中で、SAF CCD を使用して内部ダイヤル プランと外部「To PSTN」ダイヤル プランの両方を SAF CCD に参加しているすべての Unified CM リーフ クラスタに分散させることが可能になります。

Session Management Edition と SAF のハイブリッド配置では、リーフ クラスタ間のすべてのコールが Session Management Edition クラスタを通じてだけルーティングできるようにするために、SAF CCD の特定の設定を使用します。この SAF 設定は、次の 2 つの部分から成ります。

- Session Management Edition からまたはそれを通じた SAF CCD ルートのリーフ クラスタへのアドバタイジング
- SAF CCD ルートのリーフ クラスタから Session Management Edition へのアドバタイジング

（注）　ここの説明では、Unified CM 上ですでに Cisco IOS SAF フォワーダと基本的な SAF CCD 設定（アドバタイズ サービス、要求サービス、SAF 対応トランクなど）が設定されていることを前提としています。この設計は、単一の SAF Autonomous System（AS; 自律システム）を使用します。

Session Management Edition からまたはそれを通じた SAF CCD ルートのリーフ クラスタへのアドバタイジング

Session Management Edition クラスタ上で、各 SAF 対応リーフ クラスタでホストされる内部の番号範囲および外部「To PSTN」番号のための DN パターン、DN グループ、および対応する「to DID」ルールを作成します。これらの DN パターンを 1 つまたは複数の SAF 対応トランクおよびアドバタイジング サービスに関連付けることにより、SAF AS にパブリッシュします。これらの DN パターンと、

Session Management Edition への対応するルートが、すべての SAF 対応リーフ クラスタによって学習されます。Session Management Edition が IP WAN を介して到達可能な間は、すべてのクラスタ間コールが Session Management Edition を通じてルーティングされます。Session Management Edition が到達不能なときは、クラスタ間コールは、学習済みの DN パターンの「to DID」規則を使用して着信番号が修正された後に、リーフ クラスタのローカル PSTN ゲートウェイを通じてルーティングされます。

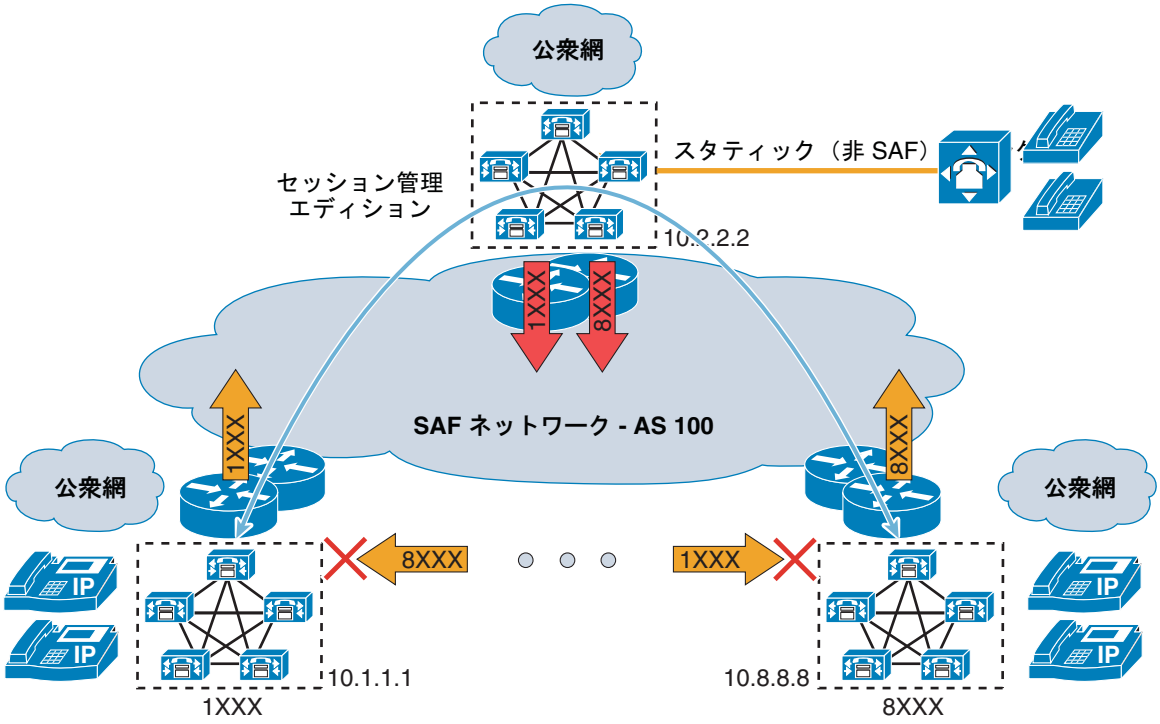
SAF CCD ルートのリーフ クラスタから Session Management Edition へのアドバタイジング

各リーフ クラスタのホストされている DN 範囲を SAF AS にアドバタイズすることの目的は、Session Management Edition クラスタにこれらの DN 範囲およびリーフ クラスタの到達可能性について学習させることです。これらの番号範囲は、その他のすべてのリーフ クラスタにも学習されます（図 5-7 を参照）。リーフ間の直接ルートが使用されるのを避けるために、各リーフ クラスタ内で、他のすべてのリーフ クラスタから学習されたルートをブロックします。ルートは、それがリーフ クラスタ内の SAF ノードの IP アドレスか、または（可能であれば）各リーフ クラスタの Remote Call Control Entity Name に一致するかどうかに基づいてブロックできます（後者、Unified CM の [Enterprise Parameters] メニューの [Unified CM Cluster ID] です）。

図 5-7　Session Management Edition の配置での SAF CCD ルートのアドバタイジング

セッション管理エディション SAF CCD ルーティング テーブル

DN パターン	「to DID」規則	IP アドレス	プロトコル
1XXX	0:+1212444	10.1.1.1	SIP
8XXX	0:+1408902	10.8.8.8	SIP



リーフ 1 SAF CCD ルーティング テーブル

DN パターン	「to DID」規則	IP アドレス	プロトコル
1XXX	0:+1212444	10.2.2.2	SIP
8XXX	0:+1408902	10.2.2.2	SIP
~~8XXX~~	~~0:+1408902~~	~~10.8.8.8~~	~~SIP~~

リーフ 8 SAF CCD ルーティング テーブル

DN パターン	「to DID」規則	IP アドレス	プロトコル
1XXX	0:+1212444	10.2.2.2	SIP
~~1XXX~~	~~0:+1212444~~	~~10.1.1.1~~	~~SIP~~
8XXX	0:+1408902	10.2.2.2	SIP

254275

Session Management Edition と SAF CCD の配置の運用上の考慮事項

ここで示す運用上の考慮事項は、Service Advertisement Framework（SAF）Call Control Discovery（CCD）を備えた Cisco Unified CM Session Management Edition の配置に当てはまるものです。

リーフ クラスタによる自身の DN 範囲の Session Management Edition からの学習

図 5-7 の SAF CCD ルーティング テーブルからわかるように、リーフ クラスタは、自身の DN 範囲の到達可能性について Session Management Edition から学習します。これらの DN 範囲は、クラスタ間の DN 範囲およびルートをブロックするのと同じ方法でブロックできます。これらの Session Management Edition SAF CCD ルートがブロックされていない場合、発信デバイスのコーリング サーチ スペースが内部 DN のパーティションの上に順序付けられた、SAF CCD で学習されたルート パー

ティションを持っていれば、これらはクラスタ内コールにだけ選択されます。ほとんどの場合、内部 DN パーティションが SAF CCD パーティションの上に順序付けられるため、内部クラスタ コールは Session Management Edition を通じてはルーティングされません。

Session Management Edition からのリーフ クラスタへの IP ルートが使用できない場合の公衆網へのルーティング コール

コールを公衆網に再ルーティングする場合に、次の 2 つの設定オプションが使用できます。

- Session Management Edition に関連付けられた公衆網ゲートウェイを通じての公衆網へのコールの再ルーティング

  Session Management Edition クラスタが公衆網アクセスを持っており、Session Management Edition からの IP パスを通じてでは接続先リーフ クラスタに到達しないコールを再ルーティングしたい場合は、各リーフ クラスタが、アドバタイズされる各 DN 範囲またはグループについて、必ず「to DID」規則を Session Management Edition にアドバタイズするようにしてください。この「to DID」規則は、Session Management Edition が着信番号に変更を加え、インバウンド トランクの Automated Alternate Routing（AAR; 自動代替ルーティング）コーリング サーチ スペース（CSS）を通じてコールをルーティングするために使用されます。

- 発信側リーフ クラスタから公衆網へのコールの再ルーティング

  Session Management Edition クラスタが公衆網アクセスを持っておらず、Session Management Edition から接続先リーフ クラスタに到達できないコールを発信側リーフ クラスタでの公衆網を通じて再ルーティングしたい場合は、各リーフ クラスタが、アドバタイズされる各 DN 範囲またはグループの「to DID」規則を決して Session Management Edition にアドバタイズしないようにしてください。この場合、Session Management Edition から接続先リーフ クラスタへのシグナリング パスが確立できないと、Session Management Edition は、コールが失敗したことを発信側リーフ クラスタに通知します。これを受けて、発信側リーフ クラスタはその「to DID」規則（Session Management Edition から学習したもの）を使用して、着信番号を修正し、発信側デバイスの自動代替ルーティング（AAR）コーリング サーチ スペース（CSS）を通じてコールをルーティングします。

Static Session Management Edition トランクを介した非 SAF ユニファイド コミュニケーション システムへのコール

Session Management Edition は、SAF CCD を使用して、非 SAF ユニファイド コミュニケーション システムの DN 範囲をすべての SAF 対応リーフ クラスタにアドバタイズできます。リーフ クラスタから非 SAF ユニファイド コミュニケーション システムへの Session Management Edition クラスタを介したコールは、Session Management Edition に到達するために SAF トランクを使用します。次に、Session Management Edition は、設定されているルート パターンと対応するスタティック（標準）トランクを使用して、非 SAF ユニファイド コミュニケーション システムに到達します。

非 SAF ユニファイド コミュニケーション システムへのコールの公衆網フォールバック

非 SAF ユニファイド コミュニケーション システムが Session Management Edition からのスタティック トランクを通じて到達できない場合の公衆網フォールバックには、次の 2 つのオプションがあります。

- 発信側リーフ クラスタから公衆網へコールを再ルーティングします。

  このオプションでは、Session Management Edition から接続先ユニファイド コミュニケーション システムへの単一のトランクが設定されます。Session Management Edition から接続先のユニファイド コミュニケーション システムへのシグナリング パスが確立できないと、Session Management Edition は、コールが失敗したことを発信側リーフ クラスタに通知します。これを受けて、発信側リーフ クラスタはその「to DID」規則（Session Management Edition から学習したもの）を使用して、着信番号を修正し、発信側デバイスの自動代替ルーティング（AAR）コーリング サーチ スペース（CSS）を通じてコールをルーティングします。

- Session Management Edition から公衆網へコールを再ルーティングします。

  このオプションでは、ルート リストとルート グループの一部として 2 つのトランクが作成されます。最初に選択されるトランクは、Session Management Edition から接続先ユニファイド コミュニケーション システムへと設定し、2 つめに選択されるトランクは、Session Management Edition からそのローカル公衆網ゲートウェイへと設定します。Session Management Edition から接続先ユニファイド コミュニケーション システムへのシグナリング パスが確立できない場合、Session Management Edition は公衆網への 2 つめのトランクを選択します。公衆網トランクを含むルート グループを使用して、内部着信番号をその公衆網での相当する番号に変更できます。

Cisco Intercompany Media Engine

Cisco Intercompany Media Engine（IME）は、分散コール処理を使用したマルチサイト展開の一例ですが、IME を使用する場合、各サイトは個別の企業組織です。Unified Communications では、この技術を説明するために*境界なし*という用語が使用されます。高忠実度のコーデック、拡張発信者 ID、企業ネットワーク外部のビデオ テレフォニーなどの Unified Communications 機能を企業間に広げていくことができるためです。ソリューションは、動的かつ安全な方法でルートを学習し、インターネットを介して組織同士が安全に通信できるようにします。他の組織と密接に連携し、高度な企業間通信を備えた組織であれば、IME が提供する拡張通信の恩恵を最大限に享受できます。ここでは、ソリューションのコンポーネントと高度なアーキテクチャについて説明し、あわせて IME を配置するための設計上の考慮事項も示します。

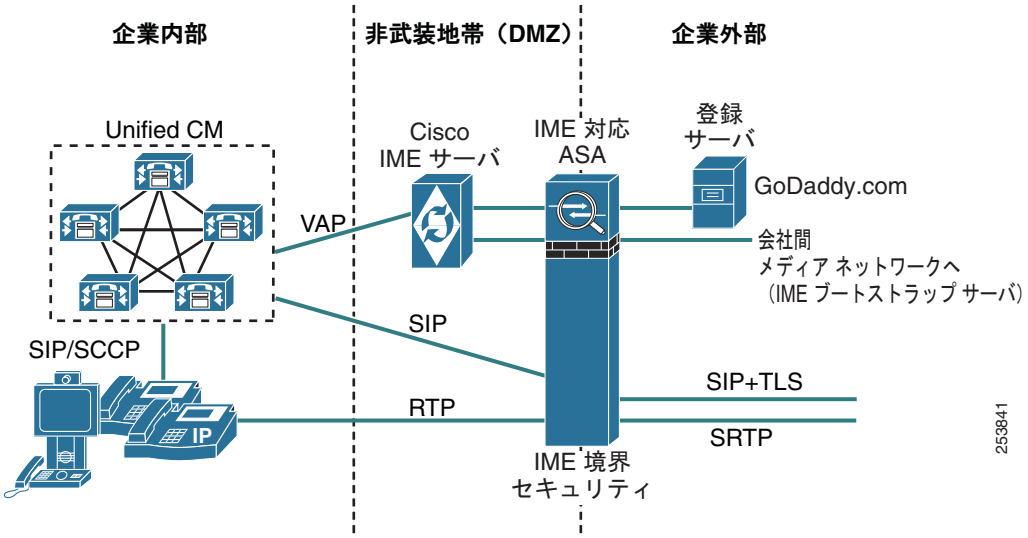
IME のコンポーネント

IME ソリューションは、IME ルートの動的学習と、組織間でのコール シグナリングおよびメディアの安全な暗号化を実現する複数のコンポーネントで構成されています。このうち 2 つの要素はインターネットにホストされます。GoDaddy.com 登録サーバと Intercompany Media Engine Bootstrap サーバで、GoDaddy.com と Cisco がそれぞれホストします。これ以外に次の必須コンポーネントがオンプレミスで配置されます。

- Cisco Intercompany Media Engine サーバ
- Cisco Unified Communications Manager（Unified CM）
- Cisco Adaptive Security Appliance（ASA）

図 5-8 に、配置したコンポーネントの概要図を示します。

図 5-8　Cisco Intercompany Media Engine コンポーネント



GoDaddy.com 登録サーバ

GoDaddy.com 登録サーバは、IME サーバを必ず検証してから、インターネットに形成された IME サーバのリングに加えます。適切な GoDaddy.com 証明書とともにインストールして登録した IME サーバだけがそのリングに参加できます。この登録サーバにアクセスするのは、リングに参加させる前と、または証明書が期限切れになって IME サーバを再登録する必要があるときだけです。

Intercompany Media Engine ブートストラップ サーバ

IME ブートストラップ サーバはグローバルにアクセスしやすいひとまとまりの IME サーバで、Cisco が所有し、運用しています。（分散型キャッシュ リングとも呼ばれる）リングに参加している各 IME サーバは、IME ブートストラップ サーバにまず接続してネットワークに参加します。登録プロセスで取得したピアツーピア証明書は、ブートストラップ サーバへの初めての接続を含め、すべてのピアツーピア TLS 接続に使用されます。

Intercompany Media Engine サーバ

各組織が、それぞれのネットワークで 1 つ以上の IME サーバを所有および運用します。IME サーバは、組織が所有するディレクトリ番号を分散型キャッシュ リングに公開し、コール レコードを検証し、リモートの企業へのルートを学習して、IME 学習ルートを Unified CM にプッシュします。このような役割は、ソリューションの IME 学習サイクルにだけかかわるもので、リアルタイム シグナリング通信およびメディア通信では機能しません。

Unified Communications Manager および Session Management Edition

組織が IME に参加するには、Cisco Unified CM 8.*x* または Unified CM Session Management Edition 8.*x* が必要です。Unified CM は、IME サーバと通信して IME 指定のディレクトリ番号を分散型キャッシュ リングにアップロードし、そのディレクトリ番号から発信された公衆網コールのコール レコード

を IME に送信します。また、Unified CM は IME サーバが検証した IME 学習ルートを受信し、その IME 学習ルートでリモートのディレクトリ番号への動的 SIP トランク コールを開始します。SIP トランク シグナリングは、常に IME 対応の Adaptive Security Appliance（ASA）を経由します。

Adaptive Security Appliance

IME コールは常に IME 対応の Adaptive Security Appliance（ASA）を経由する必要があります。これで、境界のセキュリティが確保されます。IME 対応の ASA は、SIP シグナリング通信（Unified CM からの発信またはリモートの企業からの着信）を受信し、IME チケットを検証し、アドレス変換を実行して、インターネット経由での安全なシグナリングのために SIP と SIP+TLS との変換を提供します。組織間のオーディオおよびビデオ メディアも、IME 対応の ASA を経由します。その際、RTP-to-Secure RTP（sRTP）変換と、インターネットから着信したオーディオ ストリームの音声品質モニタリングが行われます。配置オプションには、オフ パスと基本（インライン）があります。このような配置オプションの詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-31）を参照してください。

IME のアーキテクチャ

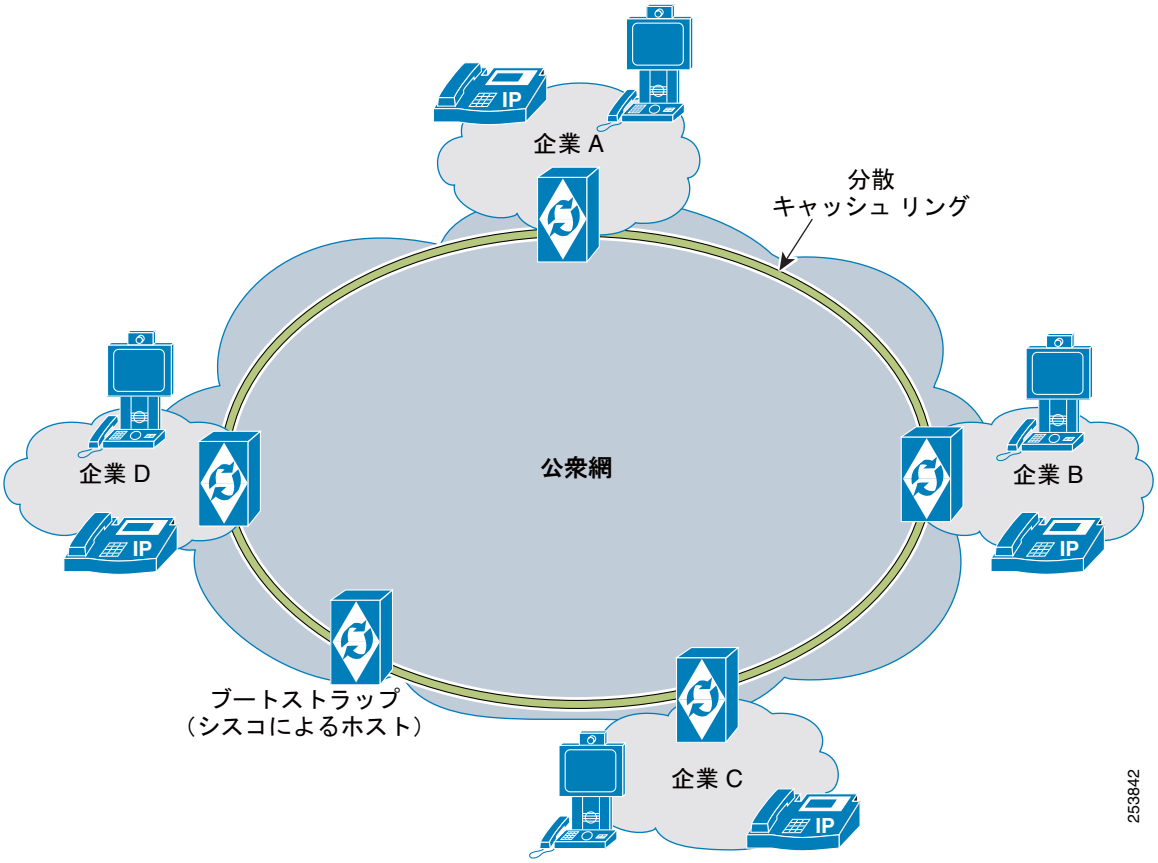
IME のアーキテクチャは、IME の運用方法に反映されます。IME の動作は、次の上位段階にかかわってきます。

- 「IME 学習ルート」（P.5-37）
- 「IME コール処理」（P.5-40）

IME 学習ルート

GoDaddy.com 登録サーバに登録し、IME ブートストラップ サーバによる検証が完了すると、IME サーバがピアツーピア リングでアクティブなサーバになります。IME に参加しているすべての組織の IME サーバが、インターネット上のリングに加わり、Resource Location And Discovery（RELOAD）プロトコルに基づく安全なピアツーピア技術を使用して通信します。IME サーバは、IME 固有の情報を 1 つ格納する分散ハッシュ テーブルを作成します。公開済みのすべての +E.164 ディレクトリ番号と、その番号を所有する IME サーバ ピア ID を収めた一方向ハッシュです。この情報はすべての IME サーバに分散され、ピアツーピア技術のアーキテクチャは IME サーバがリングの機能を低下させることなくリングへの参加または脱退を動的に行えるようになっています。IME サーバをリング上に確立し、企業が IME に登録したディレクトリ番号を公開することが、IME ルートの学習に向けた最初の手順となります。図 5-9 に、Distributed Cache Ring（DCR; 分散キャッシュ リング）の論理構成図を示します。

図 5-9　Intercompany Media Engine 分散キャッシュ リング

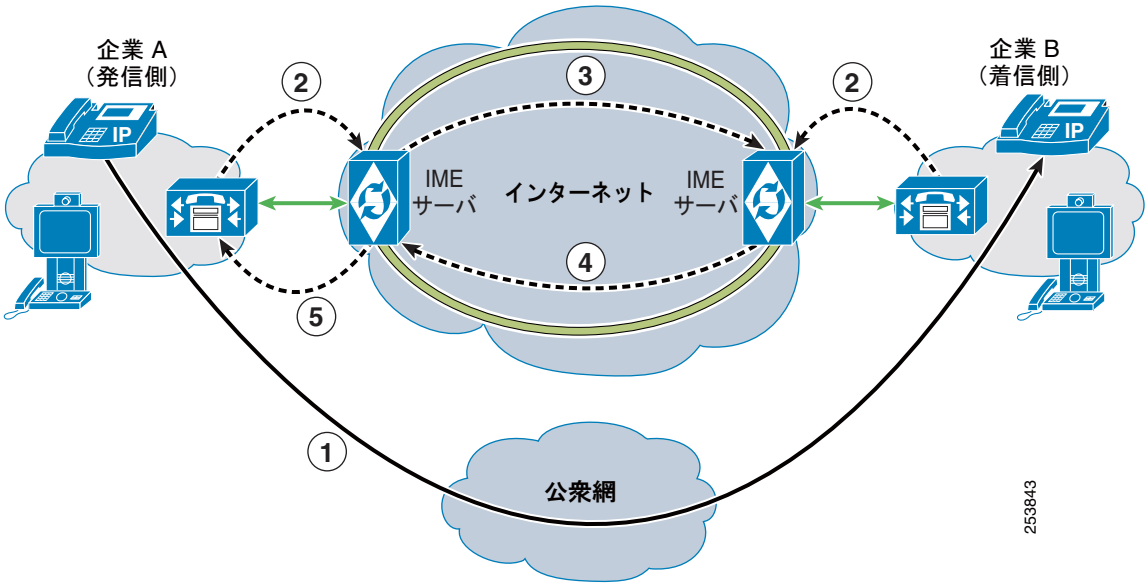


（注）　IME サーバ ピアツーピア プロトコルの標準化を目指して、IETF 機関にドラフトが提出されています。詳細については、http://datatracker.ietf.org/doc/draft-rosenberg-dispatch-vipr-reload-usage/ を参照してください。

（注）　IME では、国際番号に付く + プレフィックス（+14085551212 など）を含め、Intercompany Media Network に関連付けられたすべてのディレクトリ番号を E.164 形式にする必要があります。このドキュメントでは、これを +E.164 形式と呼びます。

図 5-10 に、IME 学習ルート プロセスを示します。

図 5-10　Intercompany Media Engine 学習ルート プロセス



組織に IME ソリューションを配置した後、選択したディレクトリ番号を登録して IME で管理できます。このように登録した +E.164 番号は、分散型キャッシュ リングに公開されます。IME ディレクトリ番号からの最初のコールは、事前に定めたとおりに公衆網を使用します（図 5-10 のステップ 1）。コール元が IME ディレクトリ番号であるため、コールが完了すると、そのコールに関する情報が Voice Call Record（VCR; 音声コール レコード）という IME に固有の CDR のようなレコードで作成され、Validation Access Protocol（VAP）によって IME サーバにアップロードされます（図 5-10 のステップ 2）。

音声コール レコードには、+E.164 形式の発着信番号やコールの開始時間と終了時間などの情報が含まれています。（リアルタイムではなく）その後のある時点で、コールの発信側の企業の IME サーバはこの +E.164 着信番号を所有する企業を見つけるために、DCR 上のピアに照会します（図 5-10 のステップ 3）。この着信番号のオーナーが検出されると（このディレクトリ番号は別の企業によって IME にすでに登録されているものとします）、検証プロセスが始まります。IME サーバ間のすべての通信が 128 ビット AES TLS で行われます。着信側 IME サーバは、発信側 IME サーバの VCR に記載された着信側 / 発信側番号および開始 / 終了時間が着信側の対応する VCR のものと一致することを確認します。一致を確認すると、着信側 IME サーバが、正常完了の返信を発信側 IME サーバに送信します（図 5-10 のステップ 4）。返信には、「チケット」（着信側の ASA だけが「IME コール処理」（P.5-40）の要領で解読できるセキュリティ ハッシュ）と、この +E.164 番号に対応する IME SIP トランク コールの送信先の外部 IP アドレスが含まれています。これが、IME 学習ルートとなります。発信側 IME サーバはこの学習ルートを受信し、その後のある時点で VAP を使用して Unified CM に公開します（図 5-10 のステップ 5）。Unified CM は、この IME 学習ルートを受信すると、そのルートを Unified CM データベースに挿入します。この時点で、発信側の企業にある IME 対応のディレクトリ番号が IME 学習ルート リストにある番号にコールを発信すると、そのコールは IME コールになります。IME ルートの学習にはリアルタイムの通信は関与しないことに留意してください。学習ルートの詳細な例については、次の URL で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10669/prod_maintenance_guides_list.html

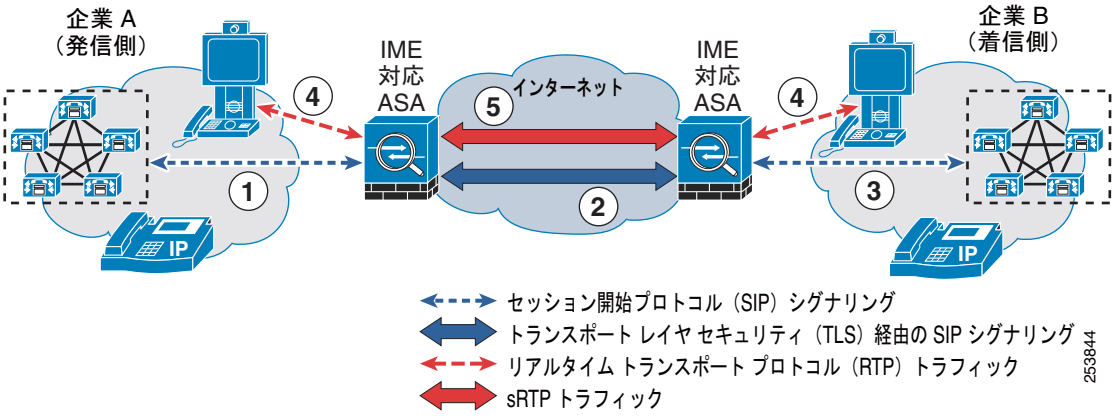
（注）　Unified CM には、定義済みのプレフィックスまたはドメインについては IME 学習ルートを Unified CM データベースに挿入しないようにする機能があります。

（注）　Unified CM には、グローバル化されたダイヤル プランが実装されていない場合でも、発着信の番号を IME VCR に固有のグローバル化された +E.164 形式に変換する方法が用意されています。VCR のための +E.164 変換の詳細については、「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）を参照してください。

IME コール処理

IME 学習ルートが Unified CM データベースに存在していると、IME コールをセットアップするときにルートの情報が使用されます。ただし、IME サーバ自体はコール処理段階に関与しません。図 5-11 に、IME コール処理の概要図を示します。

図 5-11　Intercompany Media Engine のコール処理



（注）　IME では、IME 対応の ASA と Unified CM との間で TLS 経由で安全な SIP シグナリングも使用できます。

IME コールを開始するには、着信番号がデータベース内の IME 学習ルート パターンに一致し、発信側のエンドポイントのディレクトリ番号が IME に登録されている必要があります。これらの基準が満たされた場合、Unified CM は IME 学習ルートに含まれていた着信側の企業の外部 IP アドレスまたは Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）宛ての IME SIP トランクを動的に呼び出します。IME 学習ルート パターンは +E.164 形式です。ただし、グローバル化された Unified CM ダイヤル プランが配置されていない場合でも、IME 固有の VCR 用に着信番号を +E.164 形式に変換する場合と同じプロセスを使用して、IME 固有の分析用にゲートウェイで着信番号が分析されて +E.164 形式に変換されます。E.164 変換プロファイルの詳細については、「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）を参照してください。

IME 対応の ASA は、リモートの組織との間で行われるすべての IME 通信のプロキシとして機能します。ASA は、Network Address Translation（NAT; ネットワーク アドレス変換）および SIP Application Layer Gateway（ALG; アプリケーション レイヤ ゲートウェイ）機能を備えており、SIP

メッセージング自体の内部でアドレッシングを変換できます。IME 対応の ASA 向けの配置オプションが 2 つあります。基本（インライン）とオフパスです。Unified CM が IME トラフィックを DMZ 内の IME 対応の ASA に送信できるようになるため、オフパスが推奨のオプションです。このオプションでは、ネットワークにすでに配置されている既存の ASA を使用して、インターネットへ向かうすべての Unified CM トラフィックがこの ASA を経由するように構成できます。基本とオフパスによる ASA 配置の詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-31）を参照してください。

発信側の Unified CM が、IME 対応の ASA に到達する SIP INVITE を開始します（図 5-11 のステップ 1）。この SIP INVITE の SIP ヘッダーには、学習ルートから取得したセキュリティ ハッシュ チケットが属性として含まれています。ASA は、SIP レベルでパケットを整えます。INVITE の送信元として外向きの IP アドレスが表示され、安全な（256 ビット AES）TLS 接続上でリモートの企業の外部 IP アドレスへ送信されます（図 5-11 のステップ 2）。IME 学習ルートに記載されている外部 IP アドレスは、Unified CM クラスタに代わって着信 SIP シグナリングを受信する IME 対応 ASA の外部アドレスと関連付けられています。着信側の ASA は、SIP INVITE を受信して解読し、チケットを検証します。有効なチケットがない要求はブロックされます。チケットの検証が完了すると、ASA は NAT 機能および ALG 機能を実行してから、チケットを着信側の Unified CM に転送します（図 5-11 のステップ 3）。

（注）　IME サーバおよび IME 対応 ASA は直接には通信しませんが、どちらも同じ**エポック チケット パスワード**で設定されており、チケットの検証を正常に完了できます。

SIP シグナリングのネゴシエートが正常に完了すると、各 IME 対応 ASA はそれぞれの Unified CM に指示し、エンドポイントが RTP メディアを内部メディア ターミネーション アドレスに直接ストリーミングするようにします（図 5-11 のステップ 4）。ASA は、この RTP ストリームを取得して暗号化し、NAT を実行して、オーディオ メディアやビデオ メディアなどの外部メディア ターミネーション アドレスから発生した sRTP としてストリームをリモート ASA に送信します（図 5-11 のステップ 5）。この時点で、2 つのエンドポイントにアクティブな IME コールができあがります。

IME ソリューションには、オーディオ ストリームの音声品質が許容レベルを下回った場合に、コールを公衆網にフォールバックするためのメカニズムもあります。ビデオなどの高度な機能は失われますが、コールの音声部分は元の状態のままであるため、ユーザには変更が明示されません。

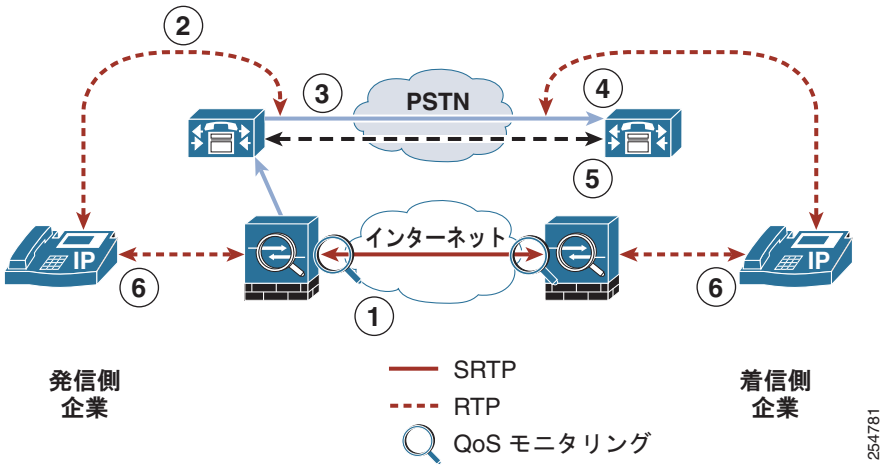
IME フォールバック機能および IME 対応 ASA の設定の詳細については、次の URL で入手可能な『*Cisco ASA 5500 Series Configuration Guide using the CLI, 8.3*』にある、Cisco Intercompany Media Engine プロキシの設定に関する説明を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/config.html

PSTN のフェールオーバー

Cisco IME では、企業間トラフィックの伝送にはパブリック インターネットが使用されます。パブリック ネットワークでのパケット損失によってユーザの使用感が低下しないように、コールに関係する IME 対応の ASA では、着信 SRTP ストリームが継続的にモニタされ、RTP の統計情報がリアルタイムに計算されます。IME 対応の ASA では、ランダムなパケット損失、パケット損失の小規模なバースト、およびパケット損失の大規模なバーストが検索されます。これら 3 つの条件は、定義した最低限のコール品質に達しているかどうかを判断するために使用されます。リアルタイムの RTP 統計情報の計算値によって定義される測定品質が、定義済みの品質制限を下回る場合、IME 対応の ASA は、影響を受けるコールに対して PSTN のフォールバックを開始します（図 5-12 を参照）。QoS 管理アルゴリズムでは、多様なパケット障害のしきい値を使用して 5 段階の感度レベルを保守することで、PSTN フォールバックの感度をより細かく制御できます。フォールバック QoS 感度レベルは、全体的に、または IME 登録グループごとに設定できます。

図 5-12　IME PSTN のフェールオーバー



IME コールの確立後、RTP パケットが ASA を出入りするときに ASA は RTP パケットを検査します。ASA はシーケンス番号とタイムスタンプを検査し、観測されたパケット損失に基づいて、フォールバックが必要かどうかをアルゴリズムで決定します。このアルゴリズムでは、フォールバック QoS 感度レベルを使用して、各 QoS 感度レベルのパケット損失しきい値を作成します。アルゴリズムでフォールバックが必要と示された場合（図 5-12 の手順 1）、ASA は Out-Of-Dialog REFER を Cisco Unified Communications Manger に送信し、PSTN にフォールバックするように求めます（図 5-12 の手順 2）。

終端 Unified CM は REFER を受信すると、既存のダイアログで Mid-Dialog REFER を発信元の Unified CM に発行します。この REFER は、必要なフォールバックについて発信元の Unified CM に通知するために必要です。PSTN フォールバックに必要な PSTN コールは、フォールバックをトリガーした IME 対応 ASA が発信側か終端側かに関係なく、常に IME コールの発信元である Unified CM から開始されます。

次に、発信元の Unified CM は、SIP コール セットアップの一環として、終端 Unified CM からアドバタイズされた Fallback Directory E.164 Number に対して PSTN コールを発信します（図 5-12 の手順 3）。Fallback Directory E.164 Number は、グローバルな [Fallback Feature Configuration Settings] と [Fallback Profile Configuration Settings] の両方で設定できるため、IME Enrolled Group ごとに異なる Fallback E.164 Number を設定できます。

デフォルトで、Fallback Directory E.164 Number に対するコールは、発信元デバイスの AAR コーリング サーチ スペースを使用してルーティングされます。グローバルな [Fallback Feature Configuration Settings] と [Fallback Profile Configuration Settings] のいずれでも、発信元デバイスの再ルーティング コーリング サーチ スペースを使用できます。

PSTN コールが設定済みの Fallback Directory E.164 Number にルーティングされると、Unified CM は着信コールを正しい IME コールに関連付ける必要があります。最初の手順は、この PSTN コールの発信者 ID を、最初の VoIP コールの SIP INVITE に含まれる発信元 Unified CM からの発信者 ID シグナリングと対応付けることです（図 5-12 の手順 4）。十分な桁数（グローバルな [Fallback Feature Configuration Settings] または [Fallback Profile Configuration Settings] の [Number of Digits for Caller ID Partial Match] で定義）が一致する場合、PSTN フォールバック コールを終端する Unified CM は、単一の DTMF 番号 1 を送信して、PSTN コールの発信元 Unified CM に通知します。発信元 Unified CM はただちに VoIP コールを分割し、PSTN レグを電話に接続し、VoIP レグを終了します。発信者 ID が一致しない場合、終端 Unified CM は単一の DTMF 番号 2 を送信します（図 5-12 の手順 5）。

発信元 Unified CM は DTMF 番号の着信を待ち受けます。1 を受信した場合、発信元 Unified CM はただちに VoIP コールを分割し、PSTN レグを電話に接続し、VoIP レグを終了します（図 5-12 の手順 6）。

2 を受信した場合、終端 Unified CM が PSTN フォールバック コールを一意な既存の IME VoIP コールに関連付けられなかったことを示すため、発信元 Unified CM は、コールを一意に識別する DTMF シーケンスをパルス出力します。この DTMF シーケンスは、最初の IME VoIP コールの確立時に行われる SIP 交換の一環として、終端 Unified CM から通知されます。DTMF シーケンスの送信後に、発信元 Unified CM は VoIP コールを分割し、PSTN レグを電話に接続し、VoIP レグを終了します（図 5-12 の手順 6）。

Unified CM は、PSTN フォールバック手順の一環として受信される DTMF 番号を受信し、それがアウトオブバンドで配信されると想定しています。

キャパシティ プランニング

IME サーバの規模は、サーバに公開する登録済み DID の数に従って調整します。表 5-5 に、プラットフォームごとの現在サポートされているキャパシティ制限を示します。

表 5-5　IME サーバでサポートしているキャパシティ

プラットフォーム	登録 DID の最大数
Cisco MCS 7825-H2/I2 と 7825-H4/I4	20,000
Cisco MCS 7845-H2/I2 と 7845-I3	40,000

すべての IME コール メディア（オーディオおよびビデオ）が IME 対応の ASA を経由するため、キャパシティは ASA を経由するコールのタイプおよび数によって異なります。IME 対応の ASA は、音声品質確保のためインターネットから着信したオーディオ ストリームだけをモニタします。ビデオ メディアは音声品質確保の目的でモニタされることはありませんが、RTP と sRTP 間の変換のため IME 対応の ASA を経由します。そのため、ビデオの帯域幅は処理できるセッションの数に直接影響を与えます。表 5-6 に、ASA-5550 および ASA-5580 のキャパシティ制限を示します。その他の ASA モジュールのパフォーマンス制限は、まだ検証されていません。

表 5-6　タイプおよび ASA モデルごとのコールの最大数

ASA モデル	Voice G.711	Video 300 kbps	Video 800 kbps	Video 1 Mbps
ASA-5550 4 GB	480 コール	240 コール	120 コール	80 コール
ASA-5580-20 4 GB	900 コール	600 コール	300 コール	200 コール

Unified CM では、処理できる IME コールの数に制限はありませんが、クラスタが提供するコール キャパシティに対する IME コールの影響を考慮する必要があります。シスコ代理店またはシスコのシステム エンジニアが、Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、大量のコール トラフィックを処理する設計をすべて検証する必要があります。サイジング ツールでは、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定できます。

ハイ アベイラビリティ

IME ルート学習段階には、ハイ アベイラビリティの側面がいくつか含まれています。Distributed Cache Ring（DCR; 分散型キャッシュ リング）自体にはピアツーピア技術による高度な冗長性があり、IME サーバがリングに加入したりリングから脱退したりすると、DCR ピアに保存される情報が調整されます。また、有効な IME サーバがいつでもリングに参加できるようにするために、シスコでは複数の IME ブートストラップ サーバをホストしています。これらの側面は、このソリューションが本質的に備えているものです。

Unified CM では、（一連の登録済み DID、除外済み DID、および IME サーバなどのパラメータを定義する）各 IME サービスはプライマリ IME サーバとセカンダリ IME サーバからなります。どちらのサーバも稼動しており、Unified CM は登録済み DID および着信側コール VCR を両サーバにアップロードします。ただし、発信側コール VCR はプライマリ IME サーバにだけアップロードされます。このため、プライマリだけが検証要求を開始しますが、どちらのサーバも着信側コール VCR があるため他の企業から受信した検証要求を処理できます。VCR に関してプライマリとセカンダリの IME サーバとが直接通信することはないため、停電になると、検証のためにプライマリに格納した発信側コール VCR が失われます。推奨するオプションは、登録済み DID を 2 つの範囲に分割し、2 つの IME サービスを作成して、サービス A のプライマリ IME サーバがサービス B のセカンダリ IME サーバになったり、あるいはその逆になったりできるようにすることです。これにより、発信側コール検証負荷が IME サーバ全体にバランスよく配分されるほか、停電時に失われる発信側 VCR の数を最小限に抑えることができます。

Unified CM 側では、IME サービスを設定した後に、IME サービスに関連付けられた IME SIP トランクのデバイス プールによって、プライマリ IME サーバとの VAP 通信を開始する Unified CM が決まります。デバイス プールに関連付けられた Unified CM Group 属性によって、サービスを担当する 1 次、2 次、および 3 次の Unified CM が決まります。1 次 Unified CM がダウンした場合には、2 次 Unified CM がアクティブな IME サーバとの VAP 通信を引き継ぎます。

コール処理については、IME サービスの IME SIP トランクに関連付けられた Unified CM Group によって、どの Unified CM サブスクライバが IME コールを開始するかが決まります。このため、IME SIP トランクの 1 次 Unified CM がオフラインであっても、IME コールは続行します。コールを受信する場合、各 IME サービスはクラスタ内の Unified CM コール処理サブスクライバに対して外部 IP アドレスとポートのペアを設定できます。各外部 IP アドレスとポートのペアは、実際には IME 対応の ASA 上に設定された IP アドレスとポートであり、Unified CM コール処理ノードと 1:1 で対応しています。IME ルートに複数の外部 IP アドレスおよびポートがあるときは、Unified CM はこの IME ルートへのコールを順繰りに送信して、コールの負荷がリモートの企業の Unified CM サーバにバランスよく配分されるようにします。リモートの Unified CM がオフラインの場合、発信側 Unified CM はリストの次に掲載されている外部 IP アドレスおよびポートを試します。応答がなく、このリストの末尾に達した場合、コールは IME がない場合と同じように公衆網に送信されます。

2 台の IME 対応の ASA をアクティブ スタンバイ モードで配置できます。ただし、ステートフル フェールオーバーは提供されません。フェールオーバーの場合には、アクティブ コールは切断されますが、後続の IME コールはスタンバイ（今はアクティブな）ASA によって接続されます。オフパス IME 対応 ASA を使用した配置の場合、Unified CM での IME サービス設定によって、1 つの IME ファイアウォールを関連付けることができます。異なる登録済み DID 範囲ごとにいくつか IME 対応の ASA を配置して、IME コールを処理できます。このため、キャパシティの増大に加え、IME コールの負荷をバランスよく配分するメカニズムを実現できます。

（注）　IME 対応の ASA では、アクティブ/アクティブ フェールオーバー モードはサポートされません。

IME コールが接続されている間、IME 対応の ASA はコールの品質をモニタできます。品質が特定の感度レベルを下回ると、コールは公衆網に戻されます。詳細については、「ASA Intercompany Media Engine プロキシ」（P.4-31）を参照してください。

設計上の考慮事項

IME ソリューションでは、IME サーバと IME 対応の ASA にパブリックに到達可能な IP アドレスが付与されている必要があります。このため、どちらも組織の DMZ に配置する例が最も多く見られます。そのために、組織内でセキュリティを担当するグループと Unified Communications を担当するグループとが緊密に連携することが必要になる場合があります。セキュリティと Unified Communications の両チームが IME プロジェクトの早期設計段階からかかわることが重要です。また、自社の IME ソリューションを設計するときは、次のガイドラインおよび考慮事項に従ってください。

- すべての Unified CM サーバ、IME サーバ、および IME 対応の ASA にネットワーク タイム プロトコルを使用する必要があります。いずれも、信頼できる上位層のクロック ソースに同期する必要があります。IME ルート学習段階では、そのようなクロック ソースが音声コール レコードの開始時間と終了時間に不可欠です。
- ホスト型 IME ソリューション配置モデルもサポートされます。ホスト型 IME 配置では、IME サーバが複数の Unified CM または Unified CM Session Management Edition クラスタに代わって、登録済みディレクトリ番号を公開し、VCR を検証します。詳細については、次の URL で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』のホスト型 IME ソリューションの情報を参照してください。

  http://www.cisco.com/en/US/products/ps10669/prod_maintenance_guides_list.html

IME サーバ

- デフォルトでは、Unified CM と IME サーバとの VAP 通信では認証だけが行われます。DMZ に IME サーバを配置する場合は、VAP 通信を認証および暗号化の対象として設定することを推奨します。このように設定すると、通信が強制的に TLS 経由で行われます。そのためには、セキュリティ証明書を共有するための追加の設定が必要です。

Unified CM および Unified CM Session Management Edition

- Intercompany Media Network では、公開するすべての番号を +E.164 形式にして、グローバルな一意性を確保する必要があります。発信側と着信側の番号は、IME 固有の Voice Call Record（VCR; 音声コール レコード）が IME サーバにアップロードされたときに正しい形式になるように、+E.164 形式に変換する必要があります。Unified CM には、IME だけのために発信側と着信側の番号を +E.164 形式に変換する機能が用意されています。これは通常のダイヤル プラン番号分析には影響を与えません。詳細については、次の URL で入手可能な『*Cisco Intercompany Media Engine Installation and Configuration Guide*』の E.164 変換プロファイルの情報を参照してください。

  http://www.cisco.com/en/US/products/ps10669/prod_maintenance_guides_list.html

- 公衆網接続に使用されるゲートウェイまたはトランクでは、[PSTN Access] チェックボックスをオンにして、IME 参加のために発信側と着信側の番号を分析する必要があります。Unified CM 8.*x* へのアップグレード時に、このパラメータはすべてのゲートウェイおよびトランクでデフォルトで有効になります。このチェックボックスが必要ない場合にはオフにできます。
- 内部エンドポイントと IME SIP トランク間のリージョンで Unified CM をどのように設定するかによって、IME コールに許可されるオーディオとビデオの機能が決まります。
- IME 対応の ASA でキャパシティを制限するために、Unified CM ロケーション ベースのコール アドミッション制御を IME SIP トランクに適用して、ASA 経由で送信されるオーディオ コールおよびビデオ コールの数を制御することを推奨します。帯域幅の制限に達すると、後続のコールは IME を配置する前と同じように公衆網でルーティングされます。
- IME で通信しようとしているリモートの企業のドメインを明示的に信頼することを推奨します。信頼グループを設定すると、VCR を検証しようとする他のすべてのドメインはデフォルトで拒否となります。

- ユーザが開始した保留および転送シナリオでは、ユニキャスト Music On Hold（MoH; 保留音）がサポートされます。ファイアウォールを正しく機能させるには、MoH full-duplex streaming サービス パラメータを有効にする必要があります。
- IME サーバの登録済み DID グループからアナログおよび FAX ステーションのディレクトリ番号を除外することを推奨します。そのようなディレクトリ番号は拡張 Unified Communications のメリットを受けず、IME では FAX コールがサポートされていないためです。

IME 対応の ASA

- 基本およびオフパスの ASA 配置の詳細と、ネットワーク内にある他のファイアウォールのセキュリティを確保するための考慮事項については、「ASA Intercompany Media Engine プロキシ」（P.4-31）を参照してください。
- （384 kbps 以上の）高帯域幅ビデオがサポートされます。ただし、IME 対応の ASA を経由するコールのキャパシティに直接影響を与えます。
- フォールバック感度レベルは、初期 IME 配置のデフォルト設定のままにしてください。フォールバックは使用し始めてから数か月間モニタし、その結果に応じて調整します。コール詳細レコードを表示して、IME またはフォールバックのために生成されたコールを探すことを推奨します。適切なフォールバック感度レベルは、企業によって異なります。
- IME 登録済み DID があるエンドポイントをリモートに配置して企業へ VPN 接続している場合、そのようなエンドポイントではコールの遅延およびジッタ特性が増幅され、その結果 IME 対応の ASA が公衆網にトリガーするフォールバックの頻度が高くなることがあります。特定のエンドポイントにおいてフォールバックが頻繁に発生する場合、このようなデバイスにデバイス プールを設定してそのフォールバック プロファイルでフォールバックを無効にするか、フォールバック感度レベルを下げるか、または IME から登録済み DID を削除することが必要になる場合があります。

IP WAN を介したクラスタリング

QoS 機能に対応している IP WAN によって相互接続される複数サイト間で、単一の Unified CM クラスタを配置できます。ここでは、WAN を介したクラスタリングの概要を簡潔に説明します。詳細については、「コール処理」（P.8-1）の章を参照してください。

WAN を介したクラスタリングでは、次の 2 種類の配置方法がサポートされます。

- 「ローカル フェールオーバー配置モデル」（P.5-51）

  ローカル フェールオーバーでは、Unified CM サブスクライバ サーバとバックアップ サーバを同じサイトに配置し、これらのサーバ間に WAN を置かないことが必要です。このタイプの配置は、Unified CM を備えた 2 ～ 4 つのサイトに理想的です。

- 「リモート フェールオーバー配置モデル」（P.5-57）

  リモート フェールオーバーでは、WAN を介して分割されたプライマリとバックアップのコール処理サーバを配置できます。このタイプの配置を使用すると、Unified CM サブスクライバを備えた最大 8 つのサイトを、別のサイトにある Unified CM サブスクライバでバックアップすることが可能です。

（注）　リモート フェールオーバーの配置では、サブスクライバ サーバ間で大量のクラスタ内トラフィックが流れるため、広い帯域幅が必要になる場合があります。

また、2 つの配置モデルを組み合せて、特定のサイト要件を満たすことも可能です。たとえば、2 つのメイン サイトにプライマリ サブスクライバとバックアップ サブスクライバを配置し、別の 2 つのサイトにはそれぞれプライマリ サーバのみを配置し、2 つのメイン サイトにある共用バックアップまたは専用バックアップのどちらかを使用できます。

WAN を介したクラスタリングの主な利点として、次のようなものが挙げられます。

- クラスタ内の全サイトに対してユーザを 1 箇所で管理
- 機能の透過性
- シェアドライン アピアランス
- クラスタ内のエクステンション モビリティ
- 統一ダイヤル プラン

これらの機能により、このソリューションは、ビジネスが継続して行われるサイトのディザスタ リカバリ プランとして、または最大 8 つの中小規模サイト用の単一ソリューションとして理想的なものになります。

WAN の考慮事項

WAN を介したクラスタリングが成功するには、WAN 自体のさまざまな特性を慎重に計画し、設計し、実装する必要があります。Unified CM サーバ間の Intra-Cluster Communication Signaling（ICCS）は、複数のトラフィック タイプから構成されます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。さまざまなタイプの ICCS トラフィックについては、「クラスタ内通信」（P.5-48）で説明されています。この項では、プロビジョニングについてのさらに詳しいガイドラインも記述されています。WAN の特性には、次の設計上のガイドラインが適用されます。

- 遅延

  任意の 2 台の Unified CM サーバ間の片方向の最大遅延は 40 msec、つまり 80 msec Round-Trip Time（RTT; ラウンドトリップ時間）以下でなければなりません。遅延の測定については、「遅延のテスト」（P.5-50）を参照してください。2 つのサイト間の伝搬遅延は、他のネットワーク遅延を考慮しない場合、1 キロメートルあたり 6 マイクロ秒になります。これは、20 ms 遅延に対して理論的な最大距離約 3000 km、つまり約 1860 マイルに相当します。この距離は、相対的なガイドラインとしてのみ記載されています。実際には、ネットワーク内の他の遅延により、これより短くなります。

- ジッタ

  ジッタは、処理、キュー、バッファ、輻輳、またはパス変動遅延により、パケットがネットワークを介して受ける変動遅延です。IP Precedence 3 ICCS トラフィックのジッタは、Quality of Service（QoS）機能を使用して最小限に抑える必要があります。

- パケット損失とエラー

  ネットワークは、すべての ICCS トラフィック、特に優先 ICCS トラフィックに対して、十分な優先順位付き帯域幅を提供するように設計される必要があります。標準的な QoS メカニズムを実装して、輻輳とパケット損失を回避する必要があります。回線エラーや他の「現実的な」状況によってパケットが損失した場合、ICCS パケットは再送信されます。これは、高信頼性伝送のために TCP プロトコルが使用されているからです。再送信が行われると、セットアップ、接続解除（終了）、または他の付加サービスの実行中に、コールが遅延する場合があります。パケット損失の状

況によっては、コールが失われる可能性があります。ただし、このシナリオ以上に、T1 または E1 上でエラーが発生することが考えられます。このエラーは、トランクを介した公衆網/ISDN へのコールに影響を及ぼします。

- 帯域幅

  予想されるコール ボリューム、デバイスのタイプ、およびデバイス数に対して、各サーバ間で適切な帯域幅を提供してください。この帯域幅は、サイト間の音声や映像のトラフィックを含めて、ネットワークを共有する他のアプリケーション用のその他の帯域幅とは別に必要です。提供される帯域幅では、さまざまなクラスのトラフィックに優先順位付けとスケジューリングを行うために、QoS が使用可能になっていなければなりません。帯域幅は、一般的に多めに設定し、少なめにサブスクライブします。

- QoS

  ネットワーク インフラストラクチャは、QoS 技術を使用して、一貫した予測可能なエンドツーエンド レベルのサービスをトラフィックに提供します。QoS も帯域幅も、それだけでは解決法になりません。QoS が使用可能になった帯域幅を、ネットワーク インフラストラクチャに設計する必要があります。

クラスタ内通信

一般に、クラスタ内通信とは、サーバ間のすべてのトラフィックを意味します。Intra-Cluster Communication Signaling（ICCS）と呼ばれるリアルタイム プロトコルもあります。このプロトコルは、クラスタ内の各サーバまたはノードにおけるコール処理の中心である、Cisco CallManager Service プロセスとの通信を提供します。

サーバ間のクラスタ内トラフィックは、次のものから構成されます。

- 主な設定情報を提供する IBM Informix Dynamic Server（IDS）データベースからのデータベース トラフィック。IDS トラフィックは、Cisco QoS の推奨事項に沿って再優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。この一例は、IDS データベース設定を使用する、エクステンション モビリティの拡張使用です。
- サブスクライバをパブリッシャに認証し、パブリッシャのデータベースにアクセスするために使用されるファイアウォール管理トラフィック。管理トラフィックは、クラスタ内のすべてのサーバ間を通過します。管理トラフィックは、Cisco QoS の推奨事項に沿って優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。
- ICCS リアルタイム トラフィック。このトラフィックは、シグナリング、コール アドミッション制御、および開始と終了時のコールについてのその他の情報から構成されます。ICCS は、Cisco CallManager Service が使用可能になっているすべてのサーバ間で、伝送制御プロトコル（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。クラスタには、Cisco CallManager Service が使用可能になっているサーバが 8 つしかないので、各サーバには最大 7 つの接続が可能です。このトラフィックは、優先 ICCS トラフィックであり、Cisco CallManager リリースおよびサービス パラメータ設定に応じてマークされます。
- CTI Manager リアルタイム トラフィック。このトラフィックは、コールに関係する CTI デバイスに使用されるか、Unified CM サーバ上のその他のサードパーティ製デバイスの制御またはモニタに使用されます。このトラフィックは、優先 ICCS トラフィックとしてマークされ、CTI Manager を備えた Unified CM サーバと、CTI デバイスを備えた Unified CM サーバとの間に存在します。

（注）　Unified CM サーバ間のトラフィックの種類について詳しくは、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html の TCP および UDP のポートの使用に関するドキュメントを参照してください。

Unified CM パブリッシャ

パブリッシャ サーバは、部分的なマスター データベースの読み取り専用コピーをクラスタ内の他のすべてのサーバに複製します。データベースのほとんどの変更は、パブリッシャで行われます。クラスタ内の別のサーバが通信不能である期間に、パブリッシャのマスター データベースに管理目的の更新などの変更が加えられた場合、パブリッシャは、通信が再確立されたときに、更新されたデータベースを複製します。ユーザ方向のコール処理機能に対するデータベースの変更は、IP Phone が登録されるサブスクライバ サーバで行われます。これらの機能には、次のものがあります。

- Call Forward All（CFA）
- Message Waiting Indication（MWI; メッセージ待機インジケータ）
- プライバシーの有効 / 無効
- Do Not Disturb（DND）の有効 / 無効
- Extension Mobility（EM; エクステンション モビリティ）のログイン
- モニタ（将来的に使用、現在ユーザ レベルの更新はありません）
- ハント グループのログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの CTI Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

各サブスクライバ サーバは、これらの変更をクラスタ内の他のすべてのサーバに複製します。パブリッシャが到達不能またはオフラインの間は、他のいかなる設定変更もデータベースに加えることはできません。パブリッシャに障害が発生している場合でも、次のものをはじめとするクラスタの通常の操作の大部分は、影響を*受けません*。

- コール処理
- フェールオーバー
- 設定済みデバイスの登録

これ以外のサービスやアプリケーションも影響を受ける場合があります。したがって、パブリッシャなしで機能するかどうかを配置時に確認する必要があります。

コール詳細レコード（CDR）およびコール管理レコード（CMR）

コール詳細レコードとコール管理レコードが使用可能である場合、各サブスクライバによって収集され、定期的にパブリッシャにアップロードされます。パブリッシャが通信不能である間、CDR および CMR は、サブスクライバのローカル ハードディスクに保存されます。パブリッシャとの接続が再確立されると、未処理の CDR はすべて、パブリッシャにアップロードされます。パブリッシャは、レコードを CDR Analysis and Reporting（CAR; CDR 分析とレポート）データベースに格納します。

遅延のテスト

任意の 2 台のサーバ間の最大ラウンドトリップ時間（RTT）は、80 msec 以下でなければなりません。この制限には、この 2 台のサーバ間の伝送パスの遅延がすべて含まれる必要があります。Unified CM サーバで **ping** ユーティリティを使用してラウンドトリップの遅延を確認しても、正確な結果は得られません。ping は、ベストエフォート型のパケットとして送信されます。ICCS トラフィックと同じ QoS 対応パスを使用して転送されません。したがって、遅延を確認するには、Unified CM サーバに最も近いネットワーク デバイスを使用することを推奨します。理想的には、サーバが接続されているアクセス スイッチです。Cisco IOS は、ICCS トラフィックが通過するのと同じ QoS 対応パス上で ping パケットが送信されるように、レイヤ 3 タイプ オブ サービス（ToS）ビットを設定できる拡張 ping を備えています。拡張 ping によって記録される時間は、ラウンドトリップ時間（RTT）、つまり通信パスを通過して戻るのに要する時間です。

次の例は、ToS ビット（IP Precedence）が 3 に設定された、Cisco IOS 拡張 ping です。

```
Access_SW#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 3
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

エラー率

予想されるエラー率はゼロでなければなりません。エラー、パケットのドロップ、または IP ネットワークに対するその他の障害は、クラスタのコール処理パフォーマンスに影響を与える可能性があります。これは、ダイヤル トーンの遅延、IP Phone 上のキーやディスプレイの反応の遅れ、またはオフフックしてから音声パスの接続までの遅れによって気付く場合があります。Unified CM はランダム エラーに対する許容性がありますが、クラスタのパフォーマンス低下を避けるために、エラーを回避する必要があります。

トラブルシューティング

クラスタ内の Unified CM サブスクライバが、予想より高い遅延、エラー、またはパケットのドロップにより、ICCS 通信の障害を検出する場合、次の症状のいくつかが発生する場合があります。

- クラスタ内のリモート Unified CM サーバ上にある IP Phone、ゲートウェイ、またはその他のデバイスが、一時的に通信不能になることがあります。
- コールの接続が切断されたり、コールのセットアップ中に失敗する場合があります。
- ユーザにダイヤル トーンが聞こえるまでに、予想以上に長い遅延が起こる場合があります。
- Busy Hour Call Completions（BHCC）が低い場合があります。

- ICCS（SDL セッション）がリセットされたり、接続が切断されることがあります。

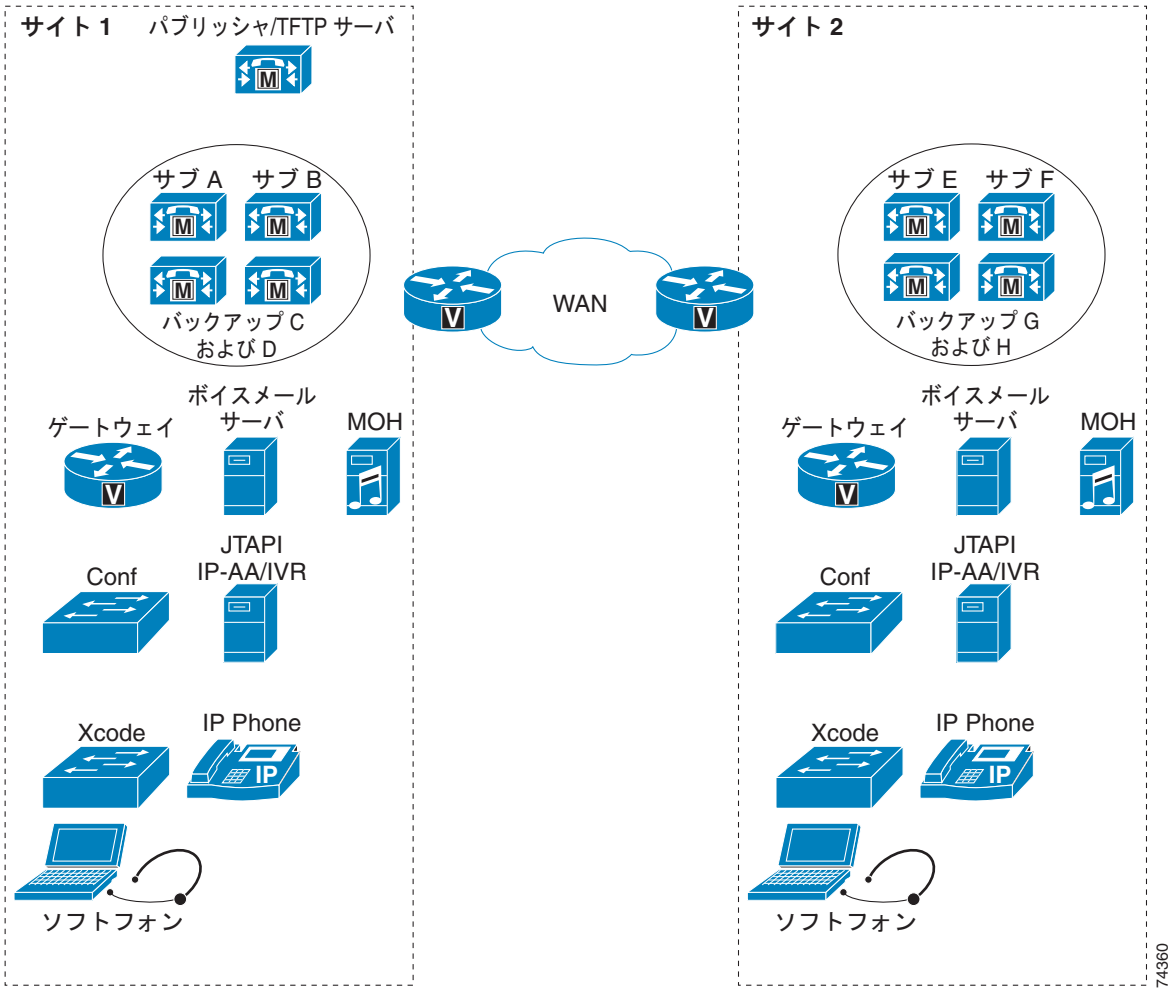
要約すると、ICCS 通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

- サーバ間の遅延を検証する
- エラーやパケットのドロップがないかどうか、すべてのリンクを調べる
- QoS が正常に設定されていることを確認する
- すべてのトラフィックをサポートするために、キューに対して、WAN を介した十分な帯域幅が提供されることを確認する

ローカル フェールオーバー配置モデル

ローカル フェールオーバー配置モデルは、WAN を介したクラスタリングに対する最大の復元性があります。このモデルの各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバがあります。この設定では、最大 4 つのサイトをサポートできます。電話機および他のデバイスの最大数は、配置されているサーバの数とタイプによって異なります。全サイトの IP Phone の最大総数は 30,000 です（図 5-13 を参照）。

図 5-13　ローカル フェールオーバー モデルの例



リモート フェールオーバー モデルを実装する場合は、次のガイドラインに従ってください。

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Unified CM の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（カンファレンス ブリッジと保留音）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強く推奨します。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、いくつかの機能を使用できないことがあります。たとえば、リモート サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。ただし、ユーザは、「Unified CM パブリッシャ」（P.5-49）の項にリストされているユーザ方向の機能に、引き続きアクセスできます。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファーストビジー トーンが聞こえるか、またはコール転送されます（ボイスメールまたは Call Forward Unregistered で設定された宛先に転送される可能性があります）。

- Unified CM クラスタ内の任意の 2 台のサーバ間に可能な最大ラウンドトリップ時間（RTT）は、80 msec です。

（注）　ラウンドトリップ遅延時間が長く、Busy Hour Call Attempts（BHCA; 最繁時呼数）が多い状況では、音声のカットスルー遅延が大きくなる場合があり、音声コール確立時の初期音声クリッピングの原因となる場合があります。

- WAN を介してクラスタリングされているサイト間での Busy Hour Call Attempts（BHCA; 最繁時呼数）が 10,000 の Intra-Cluster Communications Signaling（ICCS）トラフィックに対して、最低でも 1.544 Mbps（T1）の帯域幅が必要です。これは、呼制御トラフィックに必要な最低限の帯域幅で、WAN を介してクラスタリングされているサイト間でディレクトリ番号が共有されていない配置に適用されます。特定の遅延が発生している共有されていないディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

  合計帯域幅（Mbps）=（合計 BHCA/10,000）*（1 + 0.006 * 遅延）、遅延 = RTT 遅延（ms 単位）

  この呼制御トラフィックは、優先トラフィックに分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。

- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅に加え、リモートからパブリッシャとなるあらゆるサブスクライバ サーバに対するデータベースおよびその他のサーバ間トラフィック用に、最低でも 1.544 Mbps（T1）の帯域幅が必要になります。
- WAN を介した CTI Manager も配置する場合は、次の公式を使用して CTI 帯域幅（Mbps）を計算できます。

  （合計 BHCA/10,000）* 1.25

例 5-1　　2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタリングされており、ラウンドトリップ時間は 80 ms です。サイト 1 にはパブリッシャが 1 つと、TFTP および Music On Hold（MoH; 保留音）を組み合せたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機があり、それぞれ 1 つの DN を持っています。煩雑時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。同じ煩雑時に、サイト 2 の 2500 台の電話機もサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。この場合、次のように計算します。

煩雑時の合計 BHCA = 2500 * 3 + 2500 * 3 = 15,000

サイト間で必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 =（15,000/10,000）*（1 + 0.006 * 80）= 2.22 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）* 1.544 = 3 * 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 2.22 Mbps + 4.632 Mbps = 6.852 Mbps（およそ 7 Mbps）

- WAN を介してクラスタリングされているサイト間でディレクトリ番号が共有されている場合は、さらに帯域幅を確保する必要があります。最低限必要な 1.544 Mbps の帯域幅に加え、このようなオーバーヘッドと追加帯域幅が必要になります。共有 DN 間での 10,000 BHCA のトラフィックの場合、次の計算式を使用して計算できます。

  オーバーヘッド =（0.012 * 遅延 * シェアド ライン）+（0.65 * シェアド ライン）、各値の意味は次のとおりです。

  遅延 = IP WAN を介した RTT 遅延（ms 単位）

  シェアドライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

  特定の遅延が発生している共有されているディレクトリ番号間での、10,000 BHCA を超えるトラフィックの帯域幅を計算する場合は、次の計算式をガイドラインとして使用できます。

  合計帯域幅（Mbps）=（合計 BHCA/10,000）*（1 + 0.006 * 遅延 + 0.012 * 遅延 * シェアドライン + 0.65 * シェアドライン）、各値の意味は次のとおりです。

  遅延 = RTT 遅延（ms 単位）

  シェアドライン = WAN 経由でディレクトリ番号が共有されている追加の電話機の平均数

例 5-2　　ディレクトリ番号を共有する 2 つのサイトの帯域幅の計算

Unified CM を配置した 2 つのサイト（サイト 1、サイト 2）があると仮定します。2 つのサイトは WAN を介してクラスタリングされており、ラウンドトリップ時間は 80 ms です。サイト 1 にはパブリッシャが 1 つと、TFTP および Music On Hold（MoH; 保留音）を組み合せたサーバが 1 つ、そして 2 つの Unified CM サブスクライバ サーバが配置されています。サイト 2 には TFTP/MoH サーバが 1 つと、Unified CM サブスクライバ サーバが 2 つ配置されています。サイト 1 には 5000 台の電話機があり、それぞれ 1 つの DN を持っています。サイト 2 にも 5000 台の電話機がありますが、それぞれがサイト 1 の 5000 台の電話機と DN を共有しています。そのため、各 DN は WAN 経由で共有され、平均して 1 台の追加の電話機を持つことになります。煩雑時は、サイト 1 の 2500 台の電話機がサイト 2 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 1 の電話機も呼び出すことになります。同じ煩雑時に、サイト 2 の 2500 台の電話機がサイト 1 の 2500 台の電話機を呼び出します。それぞれのコールは、3 BHCA です。これにより、サイト 2 の電話機も呼び出すことになります。この場合、次のように計算します。

煩雑時の合計 BHCA = 2500 * 3 + 2500 * 3 = 15,000

サイト間で必要な合計帯域幅 = 合計 ICCS 帯域幅 + 合計データベース帯域幅

合計 BHCA が 15,000 であり、10,000 を超えているため、合計 ICCS 帯域幅 = (15,000/10,000) * (1 + 0.006 * 80 + 0.012 * 80 * 1 + 0.65 * 1) = 4.635 Mbps という計算式を使用できます。

合計データベース帯域幅 =（パブリッシャからリモートとなるサーバの数）* 1.544 = 3 * 1.544 = 4.632 Mbps

サイト間で必要な帯域幅 = 4.635 Mbps + 4.632 Mbps = 9.267 Mbps（およそ 10 Mbps）

（注） 上記の帯域幅は、ICCS、データベース、およびその他のサーバ間トラフィックに限定したものです。コールが IP WAN を経由する場合は、コールに使用する音声コーデックに応じて、音声またはメディア トラフィック用に追加の帯域幅をプロビジョニングする必要があります。

- クラスタ内のサブスクライバ サーバは、ローカル データベースを読み取ります。データベースの変更は、変更のタイプに応じて、ローカル データベースとパブリッシャのデータベースの両方で発生する可能性があります。クラスタ内のさまざまなサーバの同期には、Informix Dynamic Server（IDS）のデータベース複製が使用されます。そのため、長期間にわたる WAN 接続の喪失など、障害状態から回復する場合は、障害時に行われた可能性があるあらゆる変更と Unified CM

データベースを同期する必要があります。このプロセスは、パブリッシャとクラスタ内のその他のサーバへのデータベース接続が復元されると、自動的に実行されます。低帯域幅のリンクや遅延が大きいリンクでは、このプロセスに時間がかかる場合があります。また、まれなケースですが、手動によるリセットやサーバ間でのデータベース複製の修復が必要になる場合もあります。この操作は、Command Line Interface（CLI; コマンドライン インターフェイス）で **utils dbreplication repair all** や **utils dbreplication reset all** などのコマンドを使用して実行します。WAN を経由して、リモートのサブスクライバでデータベース複製の修復またはリセットを実行すると、クラスタ内のすべての Unified CM データベースが再同期されます。この場合、1.544 Mbps を超える帯域幅が必要になる場合があります。低帯域幅の場合、データベース複製の修復またはリセットが完了するまでに、時間がかかる場合があります。

（注） 同一のリモート ロケーションにある複数のサブスクライバに対して、データベース複製の修復またはリセットを実行すると、データベース複製の完了に時間がかかる場合があります。このようなリモートのサブスクライバのデータベース複製を修復またはリセットする場合は、1 つずつ実行することを推奨します。異なるリモート ロケーションにあるサブスクライバのデータベース複製を修復またはリセットする場合は、同時に実行できます。

- 集中型コール処理を使用するリモート支店を、WAN を介したクラスタリングを使用してメイン サイトに接続する場合は、WAN を介したクラスタリングに使用されるリンクがオーバーサブスクリプションにならないよう、慎重にコール アドミッション制御を設定します。
  - WAN を介したクラスタリングに使用されるリンク上で帯域幅が制限されていない場合（つまり、リンクへのインターフェイスが OC-3s または STM-1s で、コール アドミッション制御に関する要件がない場合）は、リモート サイトがメイン サイトのいずれかに接続される場合があります。これは、すべてのメイン サイトでロケーションを Hub_None として設定する必要があるためです。この設定が行われても、コール アドミッション制御に使用するハブアンドスポーク トポロジは保持されます。
  - Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）機能を使用している場合は、Unified CM ロケーションとリモート サイトにあるすべてのサイトが、メイン サイトのいずれかに登録される場合があります。
  - メイン サイト間の帯域幅が制限されている場合は、サイト間でコール アドミッション制御を使用し、ロケーションが Hub_None として設定されているメイン サイトにすべてのリモート サイトを登録する必要があります。このメイン サイトはハブ サイトと見なされ、それ以外のリモート サイトと、クラスタオーバー WAN サイトはすべて、スポーク サイトとなります。
- ソフトウェア アップグレード時は、ソフトウェア リリース ノートで説明されている標準のアップグレード手順を使用して、クラスタ内のすべてのサーバを同じ保守期間内にアップグレードする必要があります。IP WAN 経由のラウンドトリップ遅延時間が大きい場合は、ソフトウェア アップグレードにかかる時間が長くなる場合があります。また、1.544 Mbps（T1 リンク）などの低帯域幅では、ソフトウェア アップグレード プロセスの完了に時間がかかる場合があります。このような状況でアップグレード プロセスの速度を向上させるには、1.544 Mbps を超える帯域幅が必要になる場合があります。

ローカル フェールオーバーに対する Unified CM のプロビジョニング

ローカル フェールオーバー モデルに対する Unified CM クラスタのプロビジョニングは、「コール処理」（P.8-1）の章で説明されているキャパシティについての設計上のガイドラインに従う必要があります。WAN を介してサイト間の音声コールまたはビデオ コールが可能である場合、サイト間のコール アドミッション制御を提供するために、他のサイトのデフォルト ロケーションに加えて、Unified CM の *ロケーション*も設定する必要があります。デバイス数に対して帯域幅が余分にプロビジョニングされ

る場合でも、ロケーションに基づくコール アドミッション制御を設定するのが最良の方法です。ロケーションベースのコール アドミッション制御によってコールが拒否された場合は、自動代替ルーティング（AAR）機能によって公衆網への自動フェールオーバーを行うことができます。

冗長性とアップグレード時間を改善するために、2 台の Unified CM サーバで Cisco Trivial File Transfer Protocol（TFTP）サービスを使用可能にすることを推奨します。クラスタ内には 3 台以上の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。

サイトやサーバの利用可能なキャパシティに応じて、パブリッシャ サーバまたはサブスクライバ サーバのどちらかで、TFTP サービスを実行できます。TFTP サーバ オプションは、サイトごとに DHCP サーバ上で正しく設定する必要があります。DHCP を使用していないか、TFTP サーバが手動で設定される場合、ユーザが、サイトの正しいアドレスを設定する必要があります。

WAN の障害時に Unified CM の正常な動作に影響を与える可能性がある他のサービスも、連続したサービスを確保するために、すべてのサイトで複製されなければなりません。これらのサービスには、DHCP サーバ、DNS サーバ、社内電話帳、および IP Phone サービスがあります。各 DHCP サーバで、ロケーションごとに DNS サーバ アドレスを正しく設定してください。

IP Phone は、サイト間のシェアドライン アピアランスを備えている場合があります。WAN の障害時に、各ライン アピアランスの呼制御は分割されますが、WAN が回復された後、呼制御は 1 つの Unified CM サーバに戻ります。WAN の回復中に、2 つのサイト間には追加のトラフィックがあります。コール量が多い時期にこの状態が起きると、その期間中、共有ラインが予想どおりに動作しない場合があります。この状態が数分以上続くことはありませんが、これが問題になる場合は、影響を最小限に抑えるために、追加の優先順位付き帯域幅を設定できます。

ローカル フェールオーバー用のゲートウェイ

ゲートウェイは、通常、どのサイトにも配置されていて、公衆網へのアクセスに対応しています。ゲートウェイを同一サイトの Unified CM サーバに登録するために、デバイス プールを設定する必要があります。サイトのローカル ゲートウェイを公衆網アクセス用の第一選択肢として選択し、他のサイトのゲートウェイをオーバーフロー用の第二選択肢として選択するために、コール ルーティング（ルート パターン、ルート リスト、およびルート グループ）も設定する必要があります。各サイトで緊急用サービスへのアクセスを確保するように特に注意してください。

WAN 障害時にアクセスが必要のない場合、および WAN を介したコール数に対して十分な追加帯域幅が設定される場合、公衆網ゲートウェイへのアクセスを集中させることができます。E911 要件に対応するために、各サイトで追加のゲートウェイが必要な場合があります。

ローカル フェールオーバー用のボイスメール

Cisco Unity や他のボイスメール システムは、すべてのサイトに配置が可能で、Unified CM クラスタに組み込むことができます。この設定では、WAN 障害時に公衆網を使用しなくても、ボイスメールにアクセスできます。ボイスメール プロファイルを使用すると、同じロケーションにある IP Phone に、サイトに適したボイスメール システムを割り当てることができます。SMDI プロトコルを使用するボイスメール システム、サブスクライバ上の COM ポートに直接接続されたボイスメール システム、および Cisco Messaging Interface（CMI）を使用するボイスメール システムを、クラスタごとに最大 4 つ設定できます。

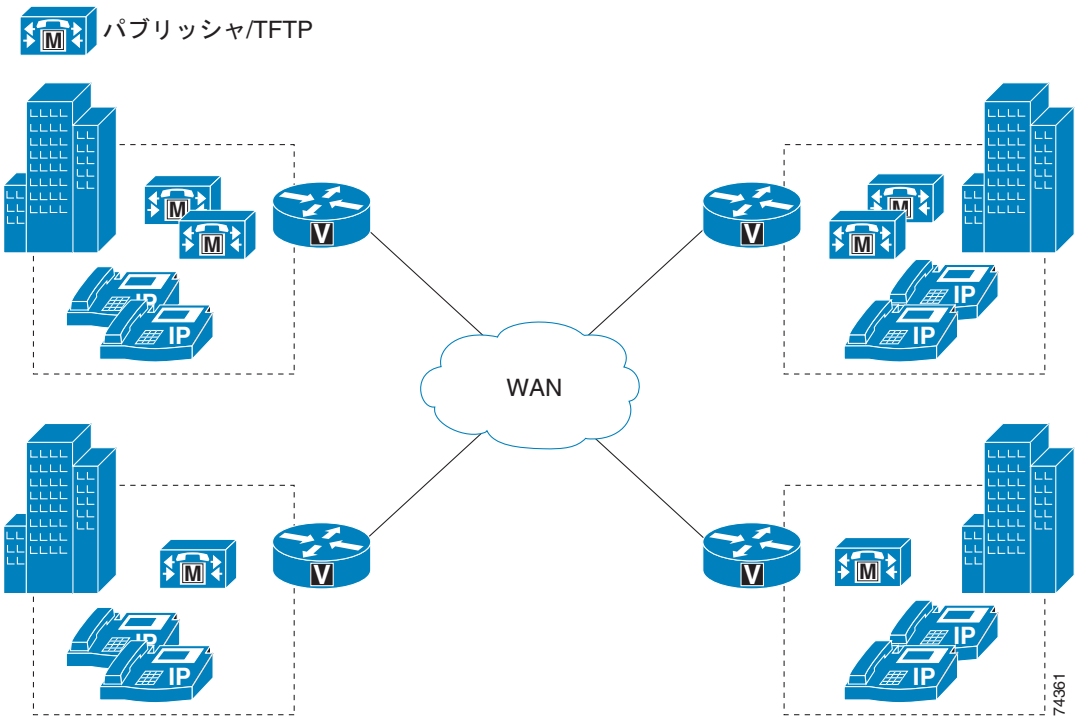
ローカル フェールオーバーに対する保留音とメディア リソース

各サイトでは、Music On Hold（MoH; 保留音）サーバや、他のカンファレンス ブリッジなどのメディア リソースに、ユーザのタイプおよび数に十分なキャパシティをプロビジョニングする必要があります。Media Resource Group（MRG; メディア リソース グループ）と Media Resource Group List（MRGL; メディア リソース グループ リスト）の使用により、メディア リソースは、オンサイト リソースによって提供され、WAN 障害時に使用できます。

リモート フェールオーバー配置モデル

リモート フェールオーバー配置モデルでは、バックアップ サーバを柔軟に配置できます。各サイトには、少なくとも 1 つのプライマリ Unified CM サブスクライバを含め、バックアップ サブスクライバを必要に応じて配置します。このモデルでは、最大 8 つのサイトを配置できます。また、「コール処理」（P.8-1）の章で説明されている 1:1 冗長性と 50/50 ロード バランシング オプションを使用すると、IP Phone やその他のデバイスは、通常、ローカル サブスクライバに登録されます。バックアップ サブスクライバは、他の 1 つ以上のサイトで、WAN を介して配置されます（図 5-14 を参照）。

図 5-14　　4 サイト構成のリモート フェールオーバー モデル



リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（「ローカル フェールオーバー配置モデル」（P.5-51）を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Unified CM サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。IP WAN を経由したバックアップ サブスクライバを設定しない場合は、Survivable Remote Site Telephony（SRST）ルータをバックアップのコール処理エージェントとして使用できます。
- Unified CM の *グループ*と *デバイス プール*を設定して、デバイスが第 2 または第 3 の選択肢として WAN を越えたサーバに登録できるようにします。

- デバイスが、WAN を介して同じクラスタ内のリモート Unified CM サーバに登録される場合、シグナリング トラフィックまたは呼制御トラフィックのために帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（「帯域幅のプロビジョニング」（P.3-47）を参照）。

（注）　ディザスタ リカバリを目的として、これら 2 つのタイプの配置の機能を組み合せることもできます。たとえば、Unified CM のグループでは、最大 3 台のサーバ（1 次、2 次、3 次）を設定できます。そのため、同一のサイトに 1 次および 2 次のサーバを配置し、3 次サーバを WAN 経由でリモート サイトに配置するように Unified CM のグループを設定できます。

WAN を介した Unified CMBE 6000 クラスタリング

Cisco Unified CMBE 6000 は、WAN を介したクラスタリングのコール処理ローカル フェールオーバー モデルを使用して配置できます。このタイプの展開では、Unified CM コール処理アプリケーションの地理的冗長性を提供するために、2 つの各サイトで 2 つの Unified CMBE 6000 サーバ ノードが配置されます。2 つの Unified CMBE 6000 サーバ ノードを両方とも UCS C200 ラックマウント サーバにすることができます。また、いずれかのサーバを通常の Cisco Media Convergence Server（MCS）にすることもできます。

WAN を介してクラスタリングできるのは Unified CM コール処理アプリケーションだけです。残りの Unified CMBE 共存アプリケーション（Cisco Unity Connection、Cisco Unified Presence、および Cisco Unified Contact Center Express）は WAN を介してクラスタリングできません。ただし、これらの残りの共存アプリケーションに対して冗長性を提供するために、2 つめの UCS C200 サーバはプライマリ UCS C200 サーバと共存させる必要があります。

WAN 配置を介した Unified CMBE 6000 コール処理クラスタリングは、これまでに説明した WAN を介した通常の Unified CM クラスタリングと同じガイドラインおよび要件に従う必要があります。ローカル フェールオーバー モデルを使用して WAN を介して Unified CMBE 6000 をクラスタリングする場合は、次のガイドラインに従ってください。

- Unified CM のグループとデバイス プールを設定して、各サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（カンファレンス ブリッジと保留音）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強く推奨します。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、いくつかの機能を使用できないことがあります。たとえば、セカンダリ サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。ただし、ユーザは、「Unified CM パブリッシャ」（P.5-49）の項にリストされているユーザ方向の機能に、引き続きアクセスできます。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファーストビジー トーンが聞こえるか、またはコール転送されます（ボイスメールまたは Call Forward Unregistered で設定された宛先に転送される可能性があります）。
- 2 つのサイトの 2 つの Unified CMBE 6000 サーバ ノード間で許可される最大 Round-Trip Time（RTT; ラウンドトリップ時間）は 80 msec です。
- WAN を介してクラスタリングされている 2 つのサイト間の Intra-Cluster Communication Signaling（ICCS）Busy Hour Call Attempts（BHCA; 最繁時呼数）には、1.544 Mbps（T1）の帯域幅が必要です。これは、呼制御トラフィックに必要な帯域幅であり、WAN を介してクラスタリ

ングされているサイト間でディレクトリ番号が共有されていない配置に適用されます。この呼制御トラフィックは、優先トラフィックに分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。

- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅以外に、2 つの Unified CMBE 6000 サーバ ノード間のデータベースおよび他のトラフィックに追加の 1.544 Mbps（T1）の帯域幅が必要です。

WAN を介したクラスタリングにリモート フェールオーバー モデルを使用した 2 つのサイトよりも高い地理的冗長性を提供するために、Unified CMBE 6000 配置で 2 つを超える UCS C200 ラックマウント サーバをクラスタリングできます（「リモート フェールオーバー配置モデル」（P.5-57）を参照）。ただし、Unified CMBE 6000 クラスタ全体でユーザの合計数が 1,000 を超えることはできず、クラスタ全体で設定されたデバイスの合計数が 1,200 を超えることはできません。ユーザ数が 1,000、設定済みデバイス数が 1,200 を超えるクラスタでの UCS C200 ラックマウント サーバの配置は、通常の Unified CM クラスタと見なされ、通常の Unified CM クラスタのすべての要件と設計ガイダンスに従います。

WAN を介したクラスタリングのリモート フェールオーバー モデルで 2 つを超える UCS C200 ラックマウント サーバを使用する Unified CMBE 6000 の配置では、次の追加ガイドラインに従う必要があります。

- WAN を介してクラスタリングされている各サイト間の Intra-Cluster Communication Signaling（ICCS）Busy Hour Call Attempts（BHCA; 最繁時呼数）には、1.544 Mbps（T1）の帯域幅が必要です。これは、呼制御トラフィックに必要な帯域幅です。
- Intra-Cluster Communication Signaling（ICCS）トラフィックに必要な帯域幅以外に、Unified CMBE 6000 パブリッシャ ノードからリモートの任意のサーバ ノード間のデータベースおよび他のサーバ間トラフィックに追加の 1.544 Mbps（T1）の帯域幅が必要です。

仮想サーバでの Unified Communications の配置

Cisco Unified Communications のアプリケーションは、VMware ESXi ハイパーバイザを使用して、仮想環境で仮想マシンとして実行できます。Unified Communications のアプリケーションは、Cisco Unified Computing System（UCS）に基づいており、Tested Reference Configuration（TRC）と呼ばれる選択されたハードウェア設定でテストされています。

ここでは、Cisco Unified Computing System（UCS）アーキテクチャ、アプリケーション仮想化のためのハイパーバイザ テクノロジー、および Storage Area Networking（SAN; ストレージ エリア ネットワーキング）の概念について説明し、あわせて各製品が企業向け Cisco Virtualized Unified Communications ソリューションのどの位置に納まるかを示します。また、仮想サーバで Unified Communications アプリケーションを配置するための設計考慮事項も示します。

ここでの説明は、次の場所で入手できる製品固有の詳細な設計ガイドラインに置き換わるものではありません。

- http://www.cisco.com/en/US/products/ps10265/index.html
- http://www.cisco.com/go/uc-virtualized

仮想サーバでの Unified Communications システムのサイジングについては、Cisco Unified Communications Sizing Tool を使用してください。このツールは、（有効なログイン認証を持つ）シスコ代理店および従業員が次の URL から入手できます。

http://tools.cisco.com/cucst

Cisco Unified Computing System

Unified Computing は、コンピューティング リソース（CPU、メモリ、および I/O）、IP ネットワーキング、ネットワークベースのストレージ、および仮想化を単一のハイ アベイラビリティ システムに統合するアーキテクチャです。このレベルの統合により、電力および冷却の費用を節約し、ネットワークへのサーバ接続を簡易化し、物理ホスト間でアプリケーション インスタンスを動的に再配置し、ディスク ストレージ容量をプールできます。

Cisco Unified Computing System は、多くのコンポーネントで構築されています が、サーバの観点からすると、UCS アーキテクチャは次の 2 つのカテゴリに分割されます。

- 「Cisco UCS B シリーズ ブレード サーバ」（P.5-60）
- 「Cisco UCS C シリーズ ラックマウント」（P.5-62）

Cisco Unified Computing System アーキテクチャの詳細については、次の URL から入手可能な資料を参照してください。

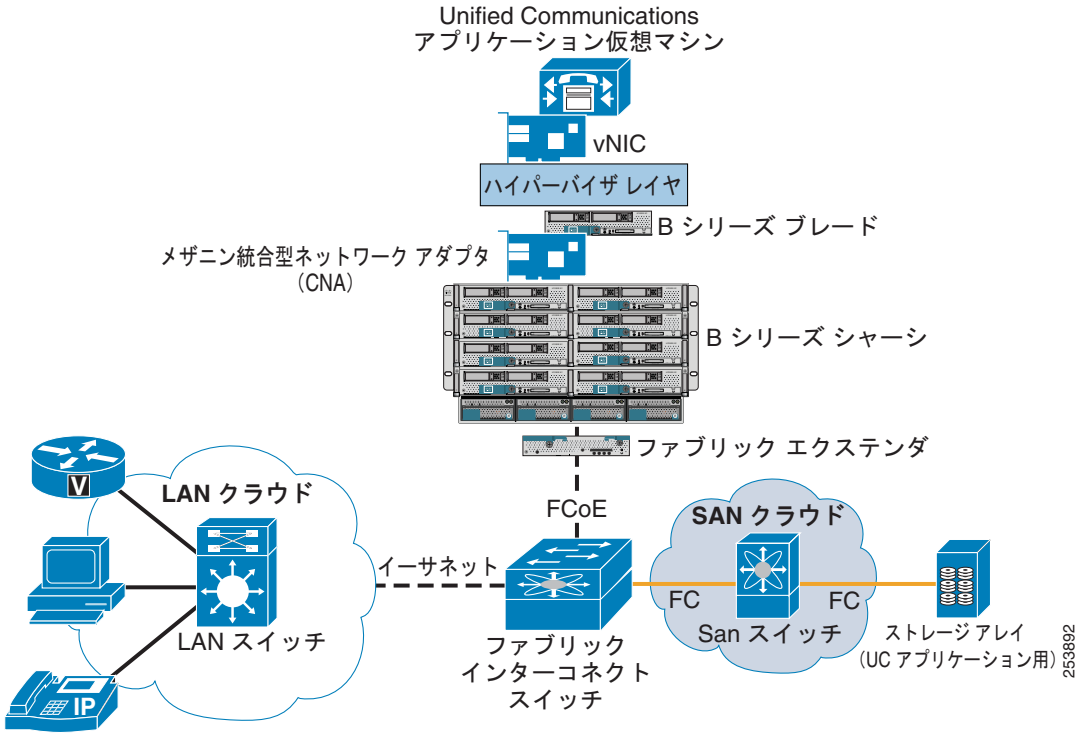
http://www.cisco.com/en/US/netsol/ns944/index.html

Cisco UCS B シリーズ ブレード サーバ

Cisco Unified Computing System（UCS）機能ブレード サーバは、x86 アーキテクチャに基づいています。ブレード サーバは、コンピューティング リソース（メモリ、CPU、および I/O）をオペレーティング システムおよびアプリケーションに提供します。ブレード サーバは、メザニン フォーム ファクタの Converged Network Adapter（CNA; 統合型ネットワーク アダプタ）を介して統合ファブリックにアクセスできます。

このアーキテクチャでは、Fibre Channel over Ethernet（FCoE）などの技術を利用して、単一のインフラストラクチャで LAN、ストレージ、および高性能コンピューティング トラフィックを転送する統合ファブリックを採用しています（図 5-15 を参照）。シスコの統合ファブリック技術は 10 Gbps イーサネットを基盤とするため、LAN、SAN、および高性能コンピューティング ネットワークのためにアダプタ、ケーブル、およびスイッチをいくつも用意する必要がありません。

図 5-15　Cisco UCS B シリーズ ブレード サーバでのユニファイド コミュニケーションの基本的なアーキテクチャ



ここでは、プライマリ UCS コンポーネントと、そのコンポーネントが Unified Communications ソリューションで機能する方法について簡単に説明します。Cisco UCS B シリーズ ブレード サーバの詳細については、次の URL で入手可能なモデル比較を参照してください。

http://www.cisco.com/en/US/products/ps10280/prod_models_comparison.html

Cisco UCS 5100 シリーズ ブレード サーバ シャーシ

Cisco UCS 5100 シリーズ ブレード サーバ シャーシは、B シリーズ ブレード サーバをホストするだけでなく、Cisco UCS 2100 シリーズ ファブリック エクステンダによってアップリンクのファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズ スイッチ）への接続も提供します。

Cisco UCS 2100 シリーズ ファブリック エクステンダ

Cisco UCS 2100 シリーズ ファブリック エクステンダは、B シリーズ シャーシに挿入され、Cisco UCS 5100 シリーズ ブレード サーバ シャーシを Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチに接続します。ファブリック エクステンダは、Fibre Channel over Ethernet（FCoE）プロトコルを使用して、ブレード サーバの FCoE 対応 CNA 間のトラフィックをファブリック インターコネクト スイッチ（Cisco UCS 6100 シリーズ）に渡すことができます。

Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチ

Cisco UCS 6100 シリーズ ファブリック インターコネクト スイッチは、10 ギガビット FCoE 対応スイッチです。B シリーズ シャーシ（およびブレード サーバ）はファブリック インターコネクトに接続し、ファブリック インターコネクトはデータセンター内の LAN または SAN スイッチング要素に接続します。

Cisco UCS Manager

管理がシステムのすべてのコンポーネントに統合されるため、Cisco UCS Manager を使用して UCS システム全体を単一のエンティティとして管理できます。Cisco UCS Manager では、直観的なユーザ インターフェイスを使用して、すべてのシステム設定操作を管理できます。

ハイパーバイザ

ハイパーバイザはサーバ ハードウェアで直接動作してハードウェアを制御するシン ソフトウェア システムであり、複数のオペレーティング システム（ゲスト）がサーバ（ホスト コンピュータ）で同時に動作できます。このため、ゲスト オペレーティング システム（Cisco Unified CM のオペレーティング システムなど）はハイパーバイザとは別の上のレベルで動作します。ハイパーバイザはクラウド コンピューティングおよび仮想化テクノロジーの基盤要素のいずれかであり、アプリケーションを統合するサーバの数が少なくて済みます。

ストレージ エリア ネットワーキング

Storage Area Networking（SAN; ストレージ エリア ネットワーキング）を使用すると、リモート ストレージ デバイスまたはストレージ アレイをサーバに接続して、ストレージがサーバにローカルに接続されているようにオペレーティング システムに認識させるようにできます。SAN ストレージは、複数のサーバ間で共有できます。

Cisco UCS C シリーズ ラックマウント

B シリーズ ブレード サーバだけでなく、Cisco Unified Computing System（UCS）も、x86 アーキテクチャに基づいた汎用ラックマウント サーバを特徴としています。C シリーズ ラックマウント サーバは、コンピューティング リソース（メモリ、CPU、および I/O）およびオプションのローカル ストレージをオペレーティング システムおよびアプリケーションに提供します。C シリーズ サーバの詳細については、次の Web サイトにある資料を参照してください。

http://www.cisco.com/en/US/products/ps10493/index.html

B シリーズ ブレード サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

ここでは、仮想サーバで Unified Communications サービスを実行する場合に従う必要がある設計規則および考慮事項を示します。次のような多くの Cisco Unified Communications アプリケーションが B シリーズ ブレード サーバで仮想化をサポートします。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified CM Session Manager Edition
- Cisco Unity Connection

- Cisco Unified Presence
- Cisco Unified Contact Center Express
- Cisco Unified Contact Center Enterprise

サポートされている Cisco Unified Communications アプリケーションの完全な一覧については、次の URL で入手可能な資料を参照してください。

http://www.cisco.com/go/uc-virtualized

ブレード サーバ

UCS B シリーズ プラットフォーム用の Tested Reference Configuration（TRC）は、統合型ネットワーク アダプタを搭載した Cisco B シリーズ ハーフ幅ブレード サーバ（UCS B200 シリーズ）に基づいています。1 つの B200 ブレードには、最大 2 つのマルチコア プロセッサをホストできる CPU ソケットが 2 つあります。また、シングル ハーフ幅のブレード サーバで複数の Unified Communications アプリケーションを実行する機能もあります。

Cisco Unified Communications アプリケーションは、Unified Communications 以外のアプリケーションは実行しない専用のブレードで実行する必要があります。各 Unified Communications アプリケーションは、専用の CUP およびメモリ リソースに割り当てて、リソースがオーバーサブスクリプションにならないようにする必要があります。

ハイパーバイザ

仮想 Unified Communications アプリケーションを実行するには、VMware ESXi ハイパーバイザが必要です。ブレード サーバに接続されているローカル ハード ドライブは、仮想マシンの格納には使用できません。これらは、ESXi ハイパーバイザ ソフトウェアのインストールにだけ使用できます。Unified Communications アプリケーションは、仮想マシンのテンプレートおよび設定についてそれぞれのガイドラインに従う必要があります。

Tested Reference Configuration を使用する場合、VMware vCenter は必須ではありませんが、大規模な配置では複数の ESXi ホストを管理することを強くお勧めします。

仮想マシンの特定の設定とサイジング要件については、次の URL で入手可能な各製品マニュアルを参照してください。

http://www.cisco.com/go/uc-virtualized

SAN およびストレージ アレイ

Cisco UCS B シリーズ プラットフォームに基づいた Tested Reference Configuration では、ファイバ チャネル SAN ストレージ アレイから実行するために仮想マシンが必要になります。SAN ストレージ アレイは、VMware ハードウェア互換リストの要件を満たす必要があります。iSCSI、FCoE SAN、および NFS NAS などのその他のストレージ オプションは、仕様ベースのハードウェア サポートによりサポートされています。詳細については、次の URL で入手可能なマニュアルを参照してください。

http://www.cisco.com/go/uc-virtualized

C シリーズ ラックマウント サーバ上で仮想 Unified Communications アプリケーションを実行する場合の設計上の考慮事項

Cisco UCS C シリーズ ラック マウント サーバに基づいた Tested Reference Configuration は、Cisco Unified Communications アプリケーションでは次の 2 つのハードウェア設定で利用できます。

- UCS C210
- UCS C200

次のような多くの Cisco Unified Communications アプリケーションが C シリーズ ラックマウント サーバで仮想化をサポートします。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified CM Session Manager Edition
- Cisco Unity Connection
- Cisco Unified Presence
- Cisco Unified Contact Center Express
- Cisco Unified Contact Center Enterprise

サポートされている Cisco Unified Communications アプリケーションの完全な一覧については、次の URL で入手可能な資料を参照してください。

http://www.cisco.com/go/uc-virtualized

UCS B シリーズとは異なり、UCS C210 ラック マウント サーバに基づいた Tested Reference Configuration では、直接接続されたストレージ ドライブ ローカルでの仮想マシンの保存、または FC SAN ストレージ アレイでの仮想マシンの保存がサポートされています。複数の Unified Communications アプリケーションを同じ C シリーズ サーバに配置できます。UCS C200 ラック マウント サーバでは、Cisco Unified Communications 仮想マシンのローカル格納のみが可能です。

UCS C210 サーバは、UCS C200 サーバよりも多くのユーザ領域をサポートします。

UCS C シリーズ ラックマウント サーバ上で Cisco Unified Communications アプリケーションを仮想サーバとして実行するには、満たしておかなければならない特定の要件があります。これらの要件については、次の資料を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/ps5748/ps378/solution_overview_c22-597556.html

仮想サーバが配置モデルに及ぼす影響

仮想サーバでの Cisco Unified Communications アプリケーションの配置では、物理サーバを使用するときと同じ配置モデルがサポートされます。「ネットワーク インフラストラクチャ」（P.3-1）の章では、Cisco UCS B ブレード仮想サーバの QoS 機能をネットワークに統合する方法に関する設計ガイドラインを示します。また、多くの場合、物理サーバ（Cisco MCS サーバなど）と Cisco UCS 仮想サーバの統合もサポートされます。たとえば、Music On Hold（MoH; 保留音）サーバは、Cisco MCS サーバ プラットフォームで実行できるほか、他のメンバー サーバが Cisco UCS 仮想サーバで実行されるクラスタのメンバーになることもできます。

この章で説明するすべてのコール処理配置モデルが、Cisco UCS 仮想サーバ プラットフォームでサポートされます。

U. S. Section 508 準拠についての設計上の考慮事項

どの配置モデルを選択するかにかかわらず、Cisco Unified Communications ネットワークを設計する場合は、障害者の方が利用しやすいテレフォニー機能になるように、Telecommunications Act Section 255 電気通信法および U.S. Section 508 に定める基準に準拠する必要があります。

Cisco Unified Communications ネットワークを構成する際は、次に説明する基本設計ガイドラインに従い、Section 508 を遵守してください。

- ネットワーク上の Quality of Service（QoS）を使用可能にします。
- ターミナル テレタイプ（TTY）デバイスまたは Telephone Device for the Deaf（TDD）に接続する電話には、G.711 コーデックのみを設定します。G.729 のような低ビット レートのコーデックを音声通信に適用している場合でも、Total Character Error Rate（TCER）が 1% を超えている場合は、TTY/TDD デバイスが適切に作動しないことがあります。
- 必要に応じて、TTY/TDD デバイスに G.711 を設定し、WAN に対応します。
- Echo Cancellation を使用可能（ON）にし、パフォーマンスを最適化します。
- Voice Activity Detection（VAD; 音声アクティビティ検出）は、TTY/TDD 接続に影響を与えるため、使用されることはありません。したがって、設定は使用可能、使用不可のどちらであっても関係ありません。
- Unified CM 内の *リージョン*および*デバイス プール*を適切に設定して、TTY/TDD デバイスが常時 G.711 コードを使用するようにします。
- TTY/TDD の Cisco Unified Communications ネットワークへの接続は、次のいずれかの方法で行います。
  - 直接接続（推奨方式）

    RJ-11 アナログ回線用 TTY/TDD を直接 Cisco FXS ポートに接続します。FXS ポートを備える Cisco 音声ゲートウェイであれば動作します。シスコは、この接続方式を推奨します。
  - アコースティック カップル

    IP Phone のハンドセットを TTY/TDD に接続しているカップリング機器に置きます。アコースティック カップルは、RJ-11 接続に比較すると信頼性が劣ります。カップリング方式は部屋の周囲の雑音やその他の要素で、一般的に通信エラーを起こしやすい方式です。
- 断続ダイヤル トーンをサポートする必要がある場合は、アナログ電話を Cisco VG224 または ATA 187 上に備えている FXS ポートに接続します。また、ほとんどの Cisco IP Phone では、断続ダイヤル トーンをサポートしています。この機能は、Audible Message Waiting Indication（AMWI; 音声メッセージ待機インジケータ）と呼ばれることもあります。この機能をサポートする具体的な Cisco IP Phone のモデルについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信

複数のコール処理エージェントが同じシステムに存在する場合、相互に認識するようにそれぞれを手動で設定できます。この設定には時間がかかることがあり、エラーも発生しやすくなっています。さまざまなコール処理エージェント間でコール ルーティングを実現するには、コール エージェントでスタティック ルートを設定し、変更のたびに更新する必要があります。

代わりに、Cisco Service Advertisement Framework（SAF）を使用すると、コール エージェント間でコール ルーティングおよびダイヤル プラン情報を自動的に共有できます。SAF を使用すると、シスコ以外のコール エージェント（TDM PBX など）も Cisco IOS ゲートウェイを介して相互接続して Service Advertisement Framework に参加させることができます。

Service Advertisement Framework（SAF）を使用すると、ネットワーク アプリケーションで IP ネットワーク内のネットワーク サービスに関する情報をアドバタイズしたり検出したりできます。SAF は、次の機能コンポーネントおよびプロトコルで構成されています。

- SAF クライアント：サービスに関する情報をアドバタイズしたり消費したりします。
- SAF フォワーダ：SAF サービスの可用性情報を配布したり維持したりします。
- SAF クライアント プロトコル：SAF クライアントと SAF フォワーダ間で使用されます。
- SAF フォワーダ プロトコル：SAF フォワーダ間で使用されます。

アドバタイズされたサービスの特性は、SAF フォワーダのネットワークにとって重要ではありません。SAF フォワーダ プロトコルは、サービスの可用性に関する情報を、SAF ネットワークに登録されている SAF クライアント アプリケーションに動的に配布するように設計されています。

SAF でアドバタイズできるサービス

理論上は、どのサービスでも SAF を介してアドバタイズできます。SAF を使用する最も重要なサービスは、Cisco Unified Communications の Call Control Discovery（CCD; コール制御ディスカバリ）です。CCD は SAF を使用して、Cisco Unified CM、Unified CME などの呼制御エージェントによってホストされる内部 Directory Number（DN; ディレクトリ番号）の可用性に関する情報を配布および維持します。また、CCD は、これらの内部ディレクトリ番号に公衆網から到達できるようにする対応した番号プレフィックスも配布します（「To PSTN」プレフィックス）。

SAF の動的な特性、およびコール エージェントがホストする DN 範囲と To PSTN プレフィックスの可用性を SAF ネットワーク内の他のコール エージェントにアドバタイズできることにより、静的でより労働集約的な他のダイヤル プラン配布方式を大幅に上回るメリットを提供します。

この章では、SAF 対応 Unified Communications ネットワークでの Call Control Discovery（CCD; コール制御ディスカバリ）の配置について説明します。SAF 自体の詳細については、「Service Advertisement Framework（SAF）」（P.3-64）を参照してください。

次のシスコ製品が、SAF に対応した Call Control Discovery（CCD; コール制御ディスカバリ）サービスをサポートしています。

- Cisco Unified Communications Manager（Unified CM）Release 8.0(1) 以降
- Cisco Integrated Services Router（ISR; サービス統合型ルータ）上の Cisco Unified Communications Manager Express（Unified CME）
- Cisco ISR プラットフォーム上の Survivable Remote Site Telephony（SRST）

- Cisco ISR プラットフォーム上の Cisco Unified Border Element
- Cisco ISR プラットフォーム上の Cisco IOS ゲートウェイ

CCD は、Cisco IOS Release 15.0(1)M 以降で動作する Cisco ISR プラットフォームでサポートされます。Cisco IOS Release 15.0(1)M の詳細については、次の Web サイトを参照してください。

- http://www.cisco.com/ios/release/15mt
- http://www.cisco.com/en/US/products/ps10621/index.html

Unified CM での CCD の使用の詳細については、次の URL で入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

SAF サービス ID

CCD が最初の SAF サービスです。SAF サービスは、SAF フォワーダと SAF クライアントからなるネットワークでそれぞれの SAF サービス ID によって識別されます。Unified Communications の CCD は、101:2:*x.x.x.x* という SAF サービス ID を使用します。その意味は次のとおりです。

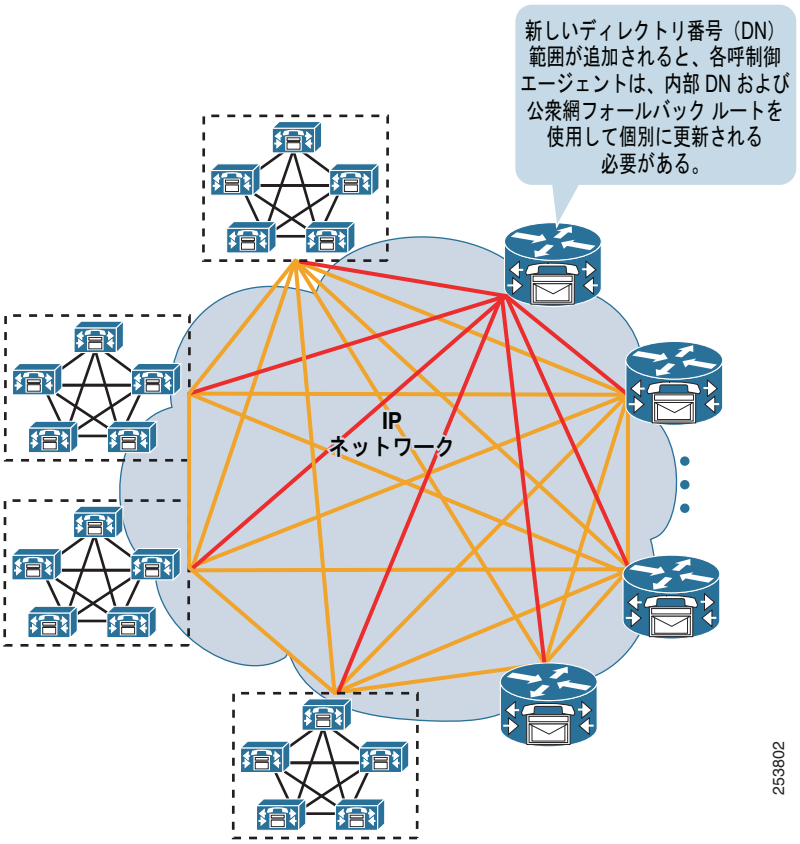
- サービス ID 101 = Unified Communications
- サブサービス ID 2 = CCD
- インスタンス ID *x.x.x.x* = Unified CM クラスタ（PKID）または Cisco IOS デバイスの ID

ネットワーク内での SAF CCD の配置

SAF CCD サービスを使用すると、Unified CM や Unified CME などの呼制御エージェントがホストするディレクトリ番号範囲の場所および可用性に関する情報を SAF 対応 Unified Communications ネットワーク内で動的に伝達できます。

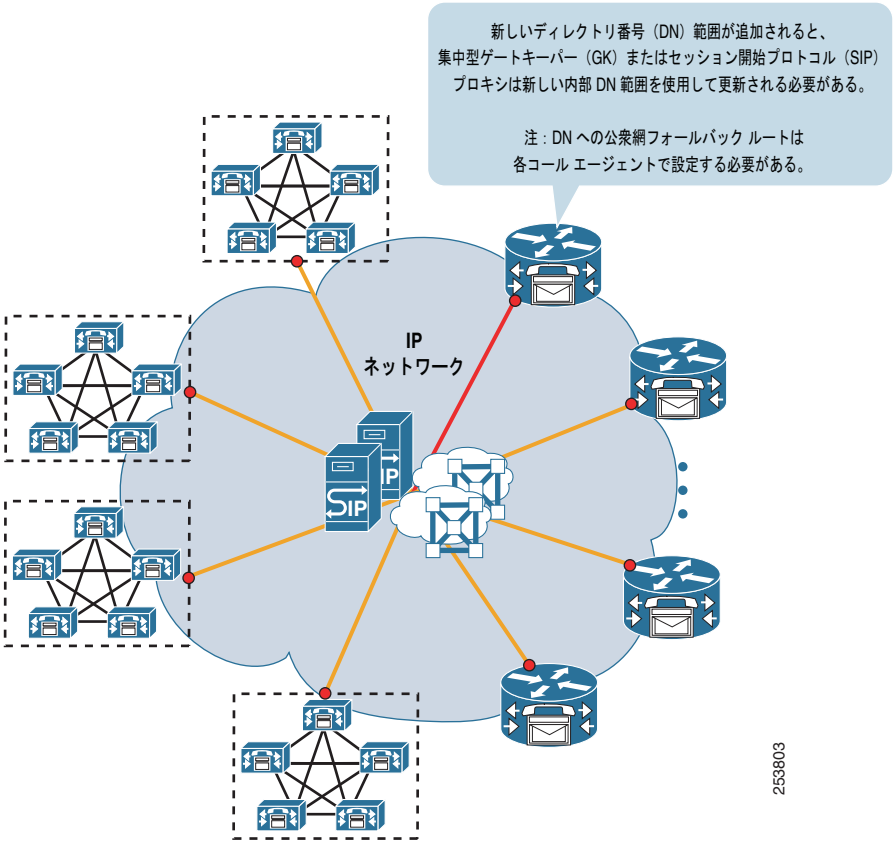
SAF を配置して DN 情報を配布および保守する利点は、4 個の Unified CM クラスタと 40 個の Unified CME で構成される Unified Communications ネットワークでダイヤル プランを管理する場合を考えてみると理解できます。静的に設定したネットワークでは、Unified Communications システム内に新しいディレクトリ番号範囲が導入された場合、その新しい番号範囲に到達する方法の詳細を、Unified Communications ネットワーク内の他のすべての呼制御アプリケーションが入手できるようにする必要があります。最悪の場合、すべての呼制御アプリケーション間に接続のフル メッシュを構築し、新しい番号範囲とその到達方法に関する情報で各呼制御アプリケーションを更新する必要があります（図 5-16 を参照）。この設定変更の連鎖は時間がかかってエラーが発生しやすいため、多大な管理作業が必要になります。

図 5-16　呼制御アプリケーション間の接続のフル メッシュ



ダイヤル プランは、ゲートキーパーまたは SIP プロキシに集中化できます（図 5-17 を参照）。これにより、設定オーバーヘッドは削減されますが、集中化できるのが内部ダイヤル プランに限られます。集中型ダイヤル プランへのアクセスが使用できなくなった場合、公衆網ルートなどの代替ルートを使用できるのは、そのルートが各呼制御アプリケーションでバックアップ ルートとして設定されている場合に限られます。

図 5-17　　集中型内部ダイヤル プラン



SAF CCD を使用すると、各呼制御アプリケーションがディレクトリ番号範囲とその対応する「To PSTN」プレフィックスを SAF ネットワーク内の他のすべての呼制御アプリケーションにアドバタイズできます（図 5-18 および図 5-19 を参照）。そのために、SAF CCD は次の制限を解除します。

- 内部システム全体のダイヤル プランをホストする集中型アプリケーションの必要性。
- 新しい DN 範囲およびその対応する「To PSTN」プレフィックスが Unified Communications ネットワークに追加された場合、各呼制御アプリケーションを個別に設定するという要件。

また、SAF CCD には静的な性質ではなく動的な性質があります。DN 範囲を削除するか、または呼制御アプリケーションへの IP 接続を失うと、SAF ネットワークは、使用できない DN へのルートを取り消して他のすべての呼制御アプリケーションを自動的に更新します。同様に、接続を再確立すると（または DN 範囲を再設定すると）、SAF ネットワークは他のすべての呼制御アプリケーションを更新して、DN 範囲を復元します。

図 5-18　Unified CM 内部 DN 範囲および対応する「To PSTN」プレフィックスの SAF ネットワークへのアドバタイズ

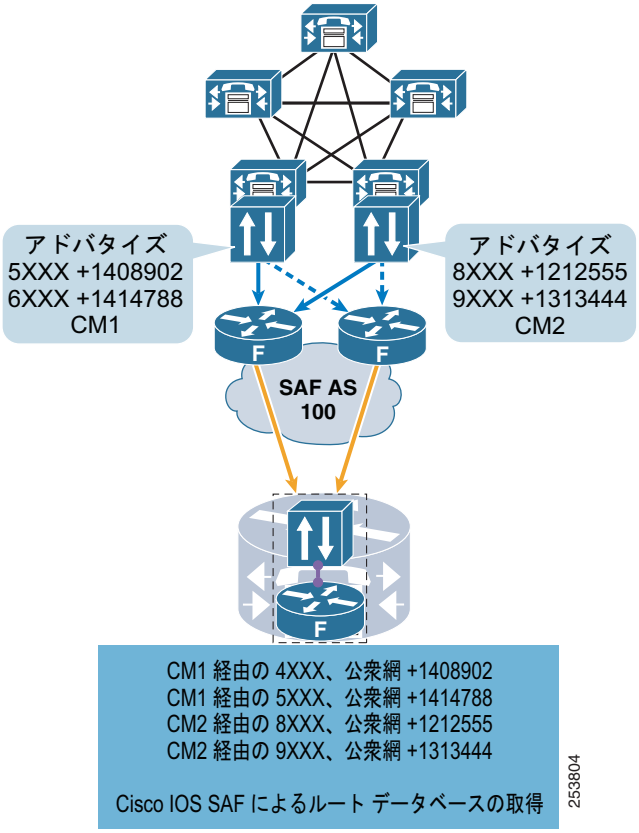
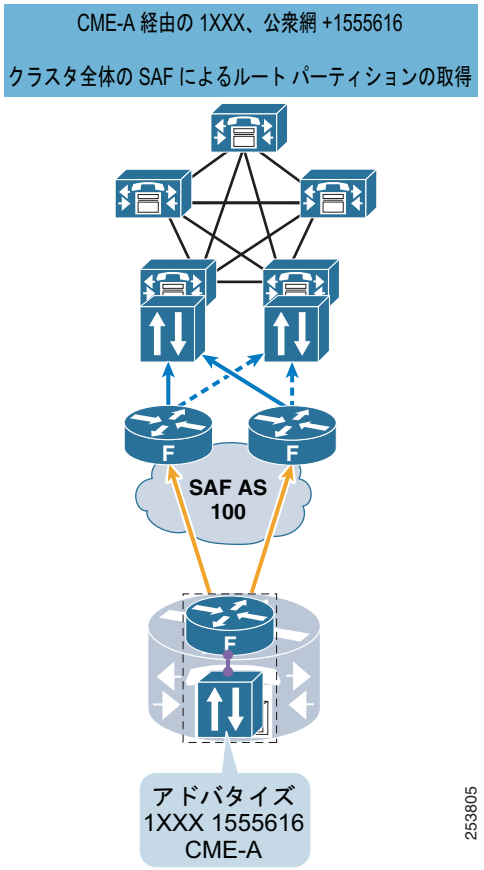


図 5-19　Unified CME 内部 DN 範囲および対応する「To PSTN」プレフィックスの SAF ネットワークへのアドバタイズ



SAF CCD 操作と標準の Unified CM コール ルーティングの比較

SAF CCD を使用したコール ルーティングは、標準の Unified CM コール ルーティングとは根本的に異なります。標準の Unified CM コール ルーティングではルート パターン、ルート リスト、およびルート グループを使用しますが、これらは SAF CCD では使用しません。代わりに、ディレクトリ番号、ディレクトリ番号範囲、およびリモート エンドポイントへの「To PSTN」プレフィックスが、静的に設定されるのではなく、SAF CCD 対応クラスタによって動的に学習されます（図 5-20 を参照）。SAF CCD では、各 Unified CM クラスタ（または他の SAF 対応呼制御アプリケーション）が、SAF ネットワークにアドバタイズするディレクトリ番号や DN 範囲などを設定します。SAF CCD は、クラスタ内の SAF 対応 SIP トランクまたは H.323 トランクの IP アドレスおよびポート番号をアドバタイズして、これらの番号に到達する方法もアドバタイズします。

また、各 SAF 対応クラスタは、DN、DN 範囲、関連付けられた「To PSTN」プレフィックス、およびトランク情報に関する他のクラスタからのアドバタイズメントを監視します。このような SAF 学習ルートは、単一のパーティションに配置されます。このパーティションへのアクセス権があるデバイスであれば、SAF 内でアドバタイズされるデバイスに到達できます。SAF CCD では、内部 DN 範囲とその To PSTN ルートだけを配布することを推奨します。

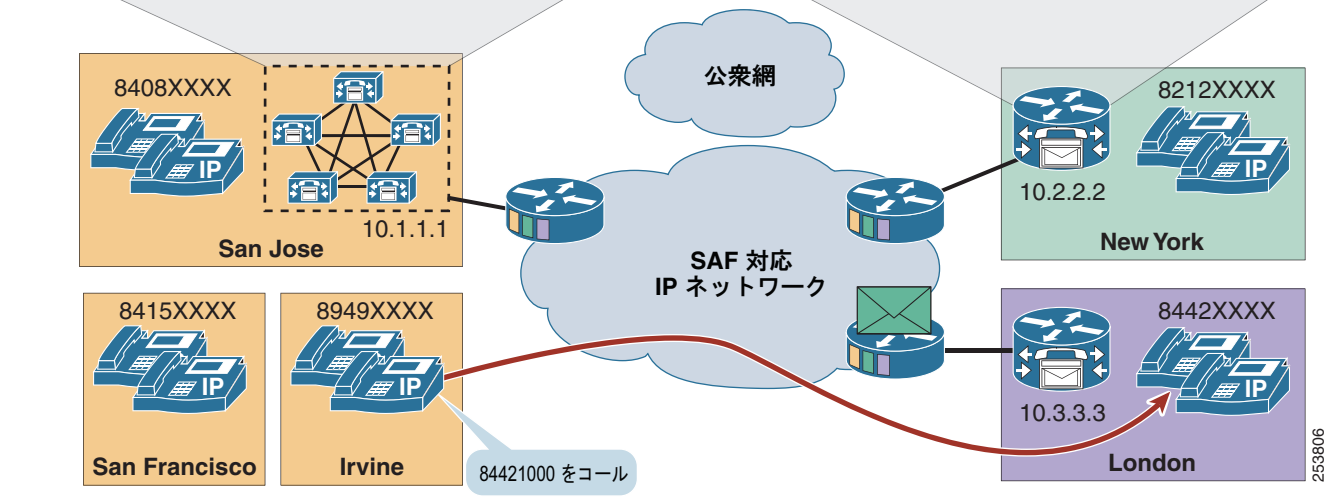
図 5-20　SAF CCD での動的コール ルーティング

San Jose Unified CM ルーティング テーブル

DN パターン	「対ダイヤルイン方式（DID）」規則	IP アドレス	プロトコル
8212XXXX	4:+1212444	10.2.2.2	SIP
8442XXXX	**4:+442077111**	**10.3.3.3**	**H.323**

New York Unified CME ルーティング テーブル

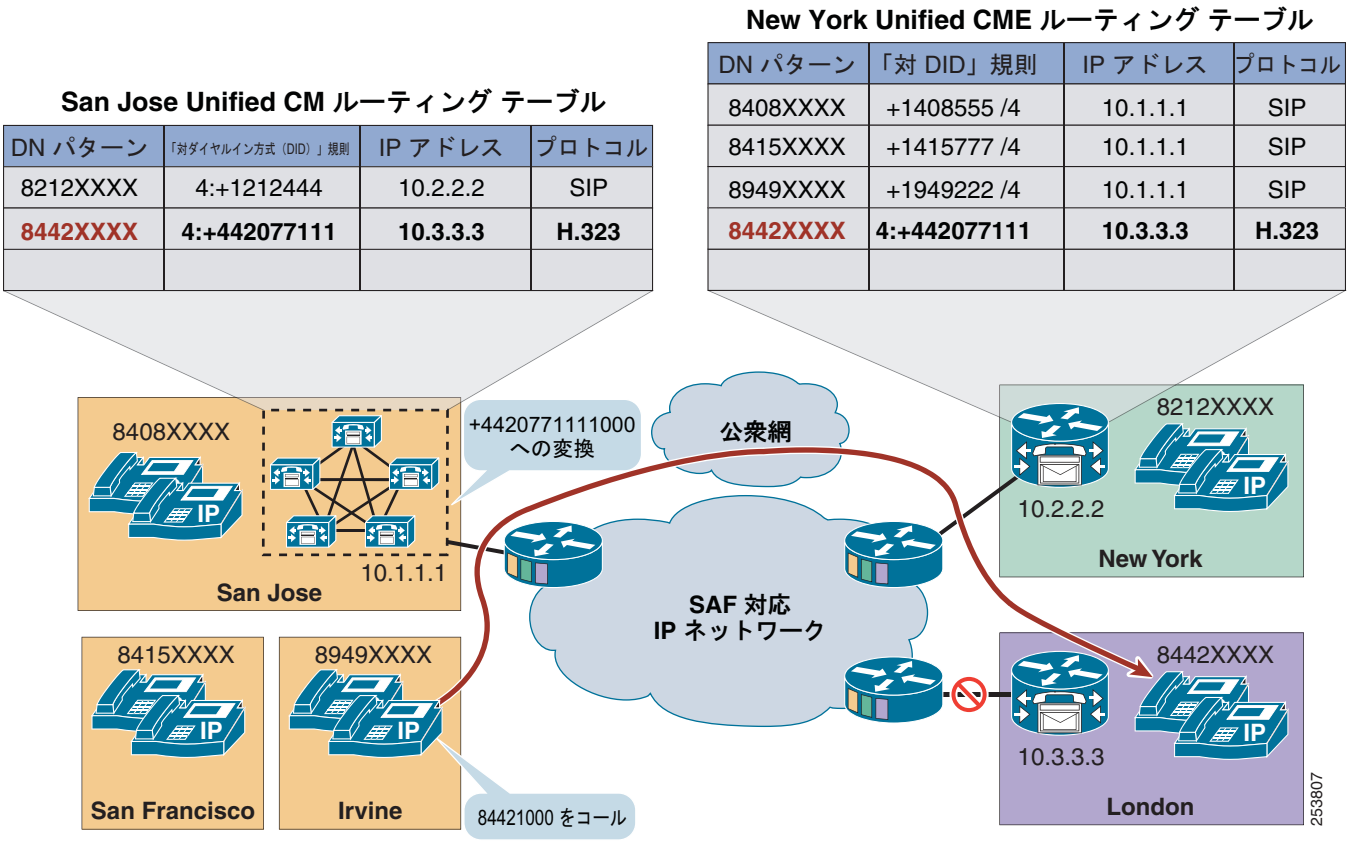
DN パターン	「対 DID」規則	IP アドレス	プロトコル
8408XXXX	+1408555 /4	10.1.1.1	SIP
8415XXXX	+1415777 /4	10.1.1.1	SIP
8949XXXX	+1949222 /4	10.1.1.1	SIP
8442XXXX	**4:+442077111**	**10.3.3.3**	**H.323**



SAF 学習ルートを使用して発信されたコールは、着信側番号への IP パスが使用できない場合、自動的に公衆網にフェールオーバーされます（図 5-21 を参照）。コールは、次の順序に従ってルーティングされます。

- 選択した IP パスを取得して、着信番号に到達します。
- IP パスが使用できない場合は、公衆網プレフィックスを使用して、着信番号を変更し、コールを公衆網経由でルーティングします。

図 5-21　SAF CCD での自動公衆網フェールオーバー



SAF CCD は、特定の SIP コールまたは H.323 コールに対して IP ルートを 1 つだけ選択できるという点で、標準のコール ルーティングとは異なります。一方、標準のコール ルーティングでは、ルート リストおよびルート グループを使用して、単一のコールに複数の IP パスを定義し、連続して試行できます。

CCD および Unified CM

CCD を使用すると、Unified CM は複数のディレクトリ番号、ディレクトリ番号範囲、および対応する「To PSTN」プレフィックスを SAF 対応ネットワークにアドバタイズできます。CCD は、Unified CM に新たに複数の設定可能なコンポーネントを導入します。

- SAF フォワーダ設定（Unified CM 上の外部 SAF クライアント）
- SAF 対応トランク
- ホスト DN パターン
- ホスト DN グループ
- CCD アドバタイズ サービス
- CCD 要求サービス

SAF フォワーダ設定（Unified CM 上の外部 SAF クライアント）

Unified CM 上の SAF フォワーダ設定は、Unified Communications ネットワークで SAF フォワーダに対する外部 SAF クライアントの設定を表します。Unified CM SAF フォワーダ設定では、次の項目を定義します。

- リモート SAF フォワーダの宛先 IP アドレスおよびポート番号
- SAF フォワーダでの認証に使用するセキュリティ プロファイル（ユーザ名およびパスワード）
- クライアント ラベル

  これは、SAF フォワーダが Unified CM 外部クライアントを特定の SAF 自律システムにマッピングするときに使用する文字列です。Cisco IOS はクライアント ラベルのバルク プロビジョニングをサポートしており、@ で終わるクライアント ラベル文字列は基本名または基本ラベルであると見なされます。ルータに設定された基本ラベルは、基本名で @ に続く文字を有効なクライアント ラベルとして受け付け、外部クライアントが送信した REGISTER メッセージに含まれるクライアントを識別します。

たとえば、Unified CM クラスタ A は、CUCM-A をクラスタの基本名として使用でき、設定された各 SAF フォワーダ（Unified CM 上の外部 SAF クライアント）の基本名に続く @ の後に番号を付加できます。Cisco IOS で外部クライアント CUCM-A を基本名として定義すると、Cisco IOS フォワーダは、次のような CUCM-A@ で始まるクライアント ラベルを受け付けます。

- CUCM-A@Client-1
- CUCM-A@Client-2
- CUCM-A@Client-3
- CUCM-A@Client-4

これで、SAF クライアント 1 ～ 4 は、同じ SAF フォワーダおよび SAF Autonomous System（AS; 自律システム）に登録できます。

Unified CM クラスタ内での外部 SAF クライアント インスタンスの作成とアクティブ化

デフォルトでは、Unified CM の [SAF Forwarder Configuration] ページで設定した外部 SAF クライアントのインスタンスが、クラスタ内のどのコール処理ノードにも作成されます（図 5-22 を参照）。外部 SAF クライアントがアクティブになるのは、コール処理ノードで CCD アドバタイズ サービスまたは CCD 要求サービスのインスタンスもアクティブになっている場合だけです。コール処理ノードでのアドバタイズ サービスおよび要求サービスのアクティブ化は、各サービスに関連付けられた SAF トランクによって決まります（詳細については、「CCD アドバタイズ サービスおよび要求サービス」（P.5-78）を参照してください）。

図 5-22　Unified CM での単一の SAF フォワーダの定義

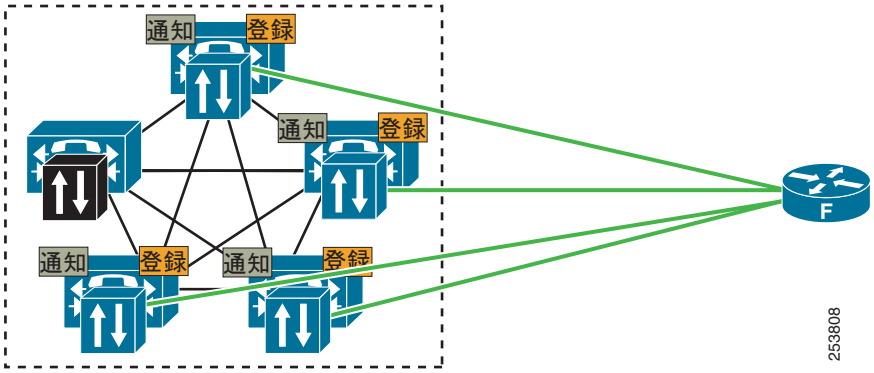
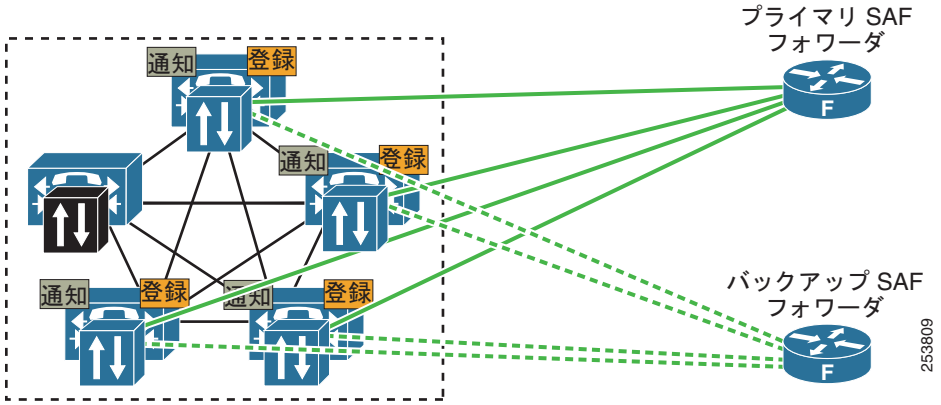


図 5-22 に、単一の SAF フォワーダにアクティブな 4 つの外部 SAF クライアントが接続されている様子を示します（灰色表示の SAF クライアントはアクティブではありません。アクティブなアドバタイズ サービスまたは要求サービスが Unified CM ノードに関連付けられていないためです）。アクティブな各外部 SAF クライアントが、SAF フォワーダへの接続を確立し、SAF ネットワークに登録し、関連付けられているサービスを公開し、SAF AS でアクティブな SAF CCD サービスをサブスクライブします。このような重複は復元力および冗長性の確保に役立ちますが、その一方でクラスタと SAF フォワーダ内にオーバーヘッドが発生します。クラスタ内でのアドバタイズ サービスおよび要求サービスの実行場所を慎重に選択することによって、このような重複および冗長性を微調整できます。詳細については、「CCD アドバタイズ サービスおよび要求サービス」（P.5-78）を参照してください。

複数の SAF フォワーダ

冗長性を確保するために、クラスタ内に複数の SAF フォワーダを設定できます。SAF クライアントは、プライマリとバックアップの SAF フォワーダへのセキュアな接続を確立し、SAF フォワーダに登録し、HostedDN サービスの公開要求をプライマリ SAF フォワーダに送信します。SAF クライアントは、クライアントからの登録要求に最初に応答した SAF フォワーダを選び、システム起動時に 1 つの SAF フォワーダをプライマリとして選択し、別の SAF フォワーダをバックアップとして選択します。SAF クライアントは、プライマリ SAF フォワーダだけを対象とするサービスを公開し、サブスクライブします。SAF クライアントは、通常の間隔でキープアライブを SAF フォワーダに送信して、SAF フォワーダへの接続を保持します。プライマリ SAF フォワーダへの接続が失敗した場合、SAF クライアントはバックアップ SAF フォワーダに切り替えて、それまでプライマリ SAF フォワーダに送信されたすべての公開要求およびサブスクライブ要求をバックアップ SAF フォワーダに送信します。

図 5-23　Unified CM での 2 つの SAF フォワーダの定義



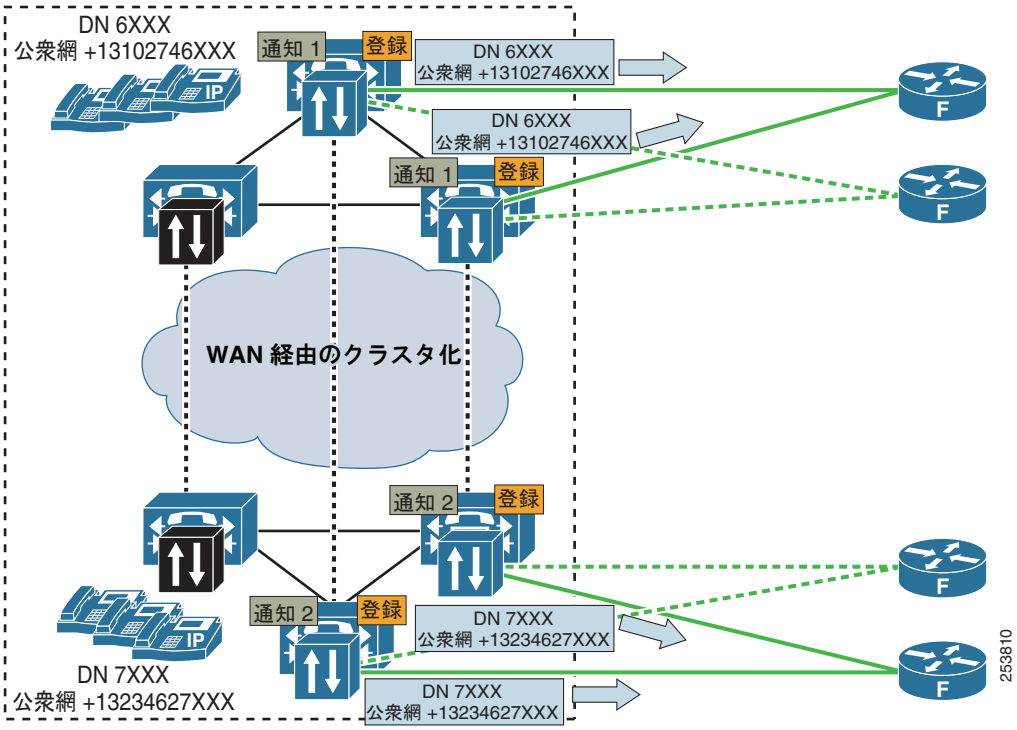
高度な SAF クライアント設定

デフォルトでは、SAF クライアントのインスタンスが、Unified CM クラスタ内のすべてのコール処理ノードに作成されます。高度な SAF フォワーダ設定オプションを使用すると、管理者はクラスタ内の特定のコール処理ノードのみに SAF クライアントを作成できます。この設定オプションでは、管理者はクラスタ内の特定のノードに SAF クライアントを作成できるほか、WAN を介したクラスタリングを採用するシステム向けに CCD サービスを広域に分散するように SAF CCD を設定できます。

SAF CCD および WAN を介したクラスタリング

WAN を介したクラスタリングを採用するクラスタ内では、複数の SAF クライアント インスタンスおよび複数のアドバタイズ サービスを作成して、特定の Unified CM ノードに関連付けることによって、クラスタ内のローカルな Unified CM トランクおよびノードの地理的な関連付けとともに、CCD ホスト ディレクトリ番号範囲を SAF ネットワークにアドバタイズできます。

図 5-24　WAN を介したクラスタリングにおいて、SAF CCD により SAF クライアントを選択する設定



SAF 対応トランク

SAF 対応トランクは、SAF 対応呼制御アプリケーション間でコールをルーティングするためにだけ使用されます。標準のルート パターン、ルート リスト、およびルート グループとは併用できません。SAF 対応トランクの宛先アドレスは、SAF を介して学習されるため設定できません。それ以外のトランク パラメータは設定できます。

次のトランク タイプで SAF を有効にできます。

- SIP トランク：SIP トランクの新規作成時に [Trunk Service Type] として [Call Control Discovery] を選択すると、有効になります。
- H.323 非ゲートキーパー制御クラスタ間トランク：[Trunk] 設定ページで [Enable SAF] チェックボックスをオンにすると、有効になります。

このどちらのトランク タイプも、Unified CM クラスタ間および Unified CM と Cisco IOS ゲートウェイ間で使用できます。

CCD は、SAF 対応トランクを次の 2 つの目的で使用します。

- コールの発信：このような SAF 対応トランクは、CCD 要求サービスに関連付けられます。
- 着信コールの受け付け：このような SAF 対応トランクは、CCD アドバタイズ サービスに関連付けられます。このような SAF 対応トランクの IP アドレスおよびポート番号は、アドバタイズ サービスに関連付けられた DN 範囲とともに公開されます。

アドバタイズ サービスと要求サービスのどちらも、SAF 対応トランクを使用できます。

CCD アドバタイズ サービスは、ホスト DN 範囲のトランクの詳細を公開するとき、SAF トランクの Cisco Unified Communications Manager グループに属する各 Unified CM ノードの IP アドレスおよびポート番号を個別の SAF アドバタイズメントで送信します。たとえば、Cisco Unified

Communications Manager グループに CUCM1 および CUCM2 がある SIP トランク A からホスト DN 範囲 5*XXX* をアドバタイズする場合、CCD アドバタイズ サービスは次の 2 つのアドバタイズメントを公開します。

- SIP トランク IP アドレス（CUCM1）ポート番号 5060 を経由する 5XXX
- SIP トランク IP アドレス（CUCM2）ポート番号 5060 を経由する 5XXX

このアドバタイズメントを受信するクラスタの要求サービスは、5XXX への 2 つのルートを SAF 学習ルート パーティションに配置します。

- SIP トランク IP アドレス（CUCM1）ポート番号 5060 を経由する 5XXX
- SIP トランク IP アドレス（CUCM2）ポート番号 5060 を経由する 5XXX

このクラスタから 5XXX へのコールが、2 つの使用可能な SIP トランク宛先をラウンドロビン順に選択します。

SAF トランクは、TCP または UDP 転送プロトコルをサポートします。SAF トランクが複数の呼制御アプリケーションから着信コールを受け付けることができるため、SAF 対応トランクでは TLS ベースのシグナリング認証と暗号化がサポートされません。

ホスト DN パターンおよびホスト DN グループ

ホスト DN グループとは、ホスト DN パターンのグループのことです。ホスト DN グループのホスト DN パターンは、一般に物理的なサイトに関連付けられたディレクトリ番号の範囲のことです。ホスト DN グループごとに「To PSTN」フェールオーバー ルーティング用の番号削除および先頭付加情報を設定できます。同じ DN パターンを複数のホスト DN グループに関連付けることはできません。

ホスト DN パターンには、1 つのディレクトリ番号（たとえば、5000）も、広範囲のディレクトリ番号（たとえば、5*XXX*）も定義できます。どの DN パターンも一意である必要があります。各ホスト DN パターンは、公衆網フェールオーバー ルーティングに対応するための番号削除および先頭付加情報とともに設定できます。ホスト DN パターンでの公衆網フェールオーバー設定は、ホスト DN グループ レベルの公衆網フェールオーバー設定よりも優先されます。

CCD アドバタイズ サービスおよび要求サービス

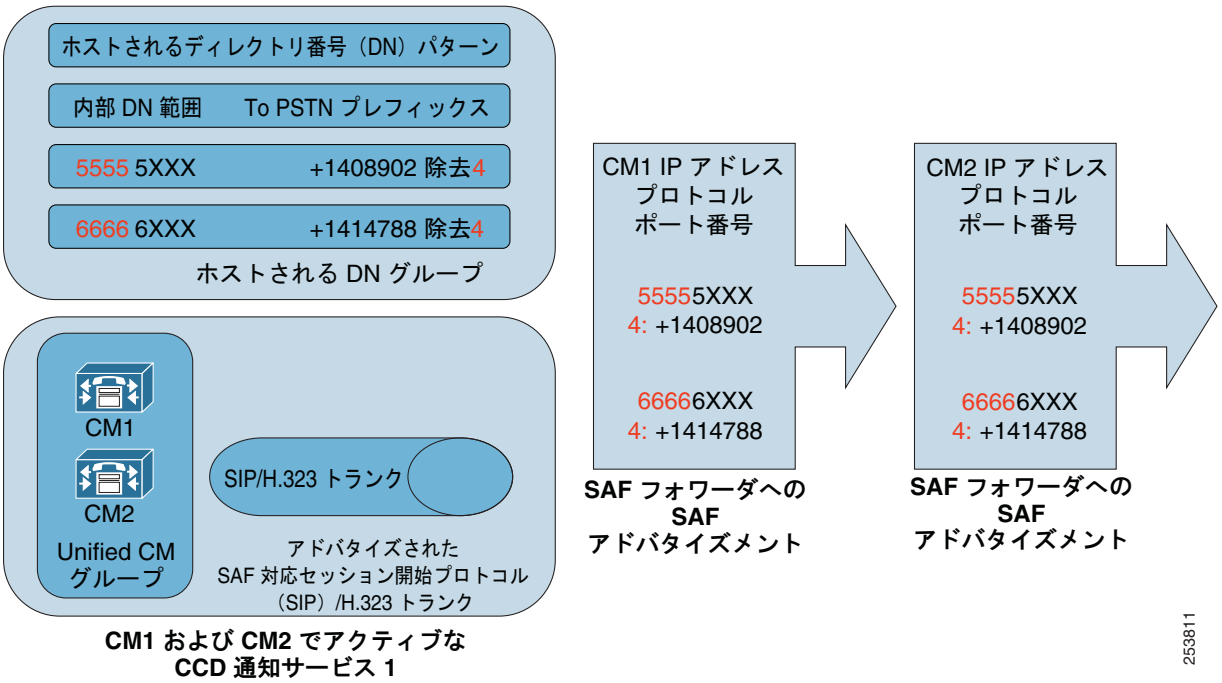
CCD は、2 つの Unified CM サービスを使用して、SAF ネットワークと通信します。アドバタイズ サービスは DN 範囲およびその関連するトランクを SAF ネットワークに公開するために使用し、要求サービスは SAF ネットワーク内の他のコール エージェントから DN 範囲への到達可能性を学習するために使用します。以降の項では、この 2 つのサービスについて説明します。

CCD アドバタイズ サービス

CCD アドバタイズ サービスは、1 つのホスト DN グループを SAF 対応 SIP トランクや H.323 トランクに関連付けます。アドバタイズ サービスは、関連付けられた SAF 対応トランクの属する Cisco Unified Communications Manager グループ（Unified CM Group）内のそれぞれのサーバで作成されてアクティブ化されます。アドバタイズ サービスは、各トランクのある Unified CM Group 内のそれぞれのサーバ上にある SAF クライアントを使用して、ホスト DN グループおよび関連付けられたトランク ノードに関する情報をクライアントの SAF フォワーダに公開します（図 5-25 を参照）。

SIP トランクおよび H.323 トランクがそれぞれ異なる機能セットをサポートするため（たとえば、H.323 トランクは Annex M1 を介した QSIG をサポートします）、アドバタイズ サービスごとにトランク タイプを 1 つだけ選択するのが一般的です。H.323 トランクと SIP トランクの両方を選択すると、このアドバタイズ サービスに関連付けられたホスト DN 範囲へのコールがラウンドロビン方式で SIP トランクと H.323 トランクの両方に分散されます。

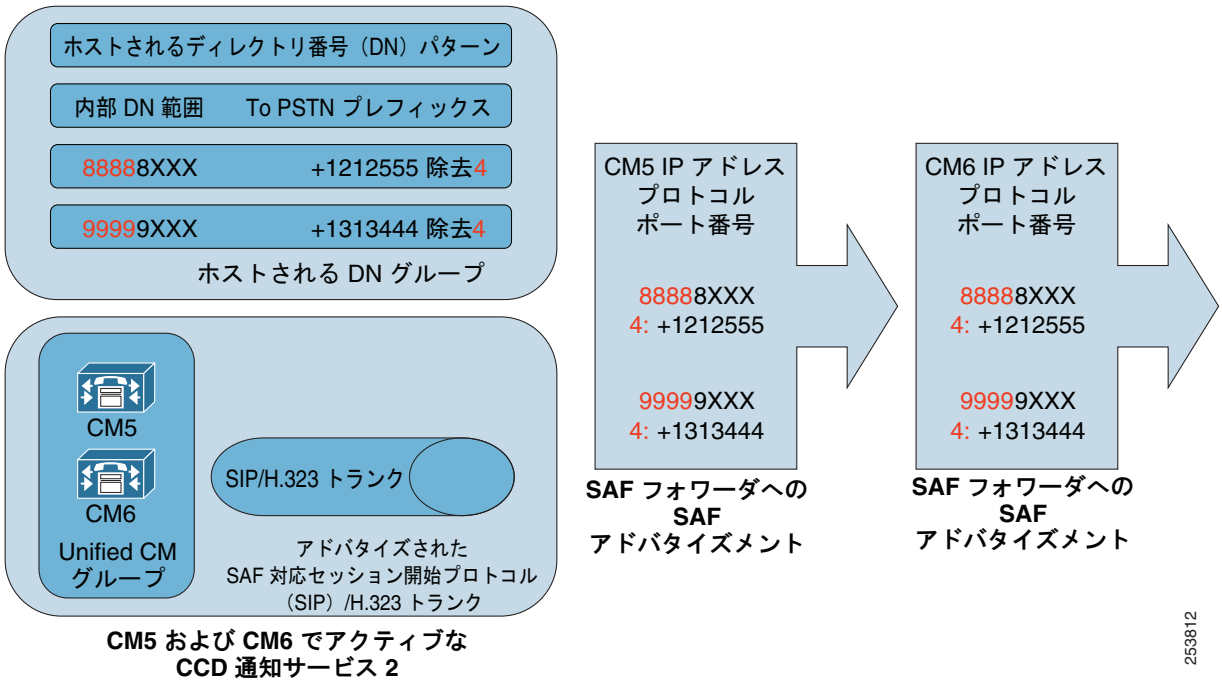
図 5-25　CM1 と CM2 でアクティブな CCD アドバタイズ サービス 1



CM1 および CM2 でアクティブな CCD 通知サービス 1

Unified CM クラスタ内に複数のアドバタイズ サービスを作成できます。アドバタイズ サービスは、他のアドバタイズ サービスと同じ（または異なる）SAF 対応トランクを使用できます。ただし、各アドバタイズ サービスを一意のホスト DN グループに関連付ける必要があり、クラスタ内の複数のアドバタイズ サービスで同じホスト DN パターンをアドバタイズすることはできません。複数のアドバタイズ サービスを作成すると、着信コールを DN 範囲に従ってクラスタ内の複数のトランク サーバに分散させることができます（図 5-26 を参照）。

図 5-26　CM5 と CM6 でアクティブな CCD アドバタイズ サービス 2

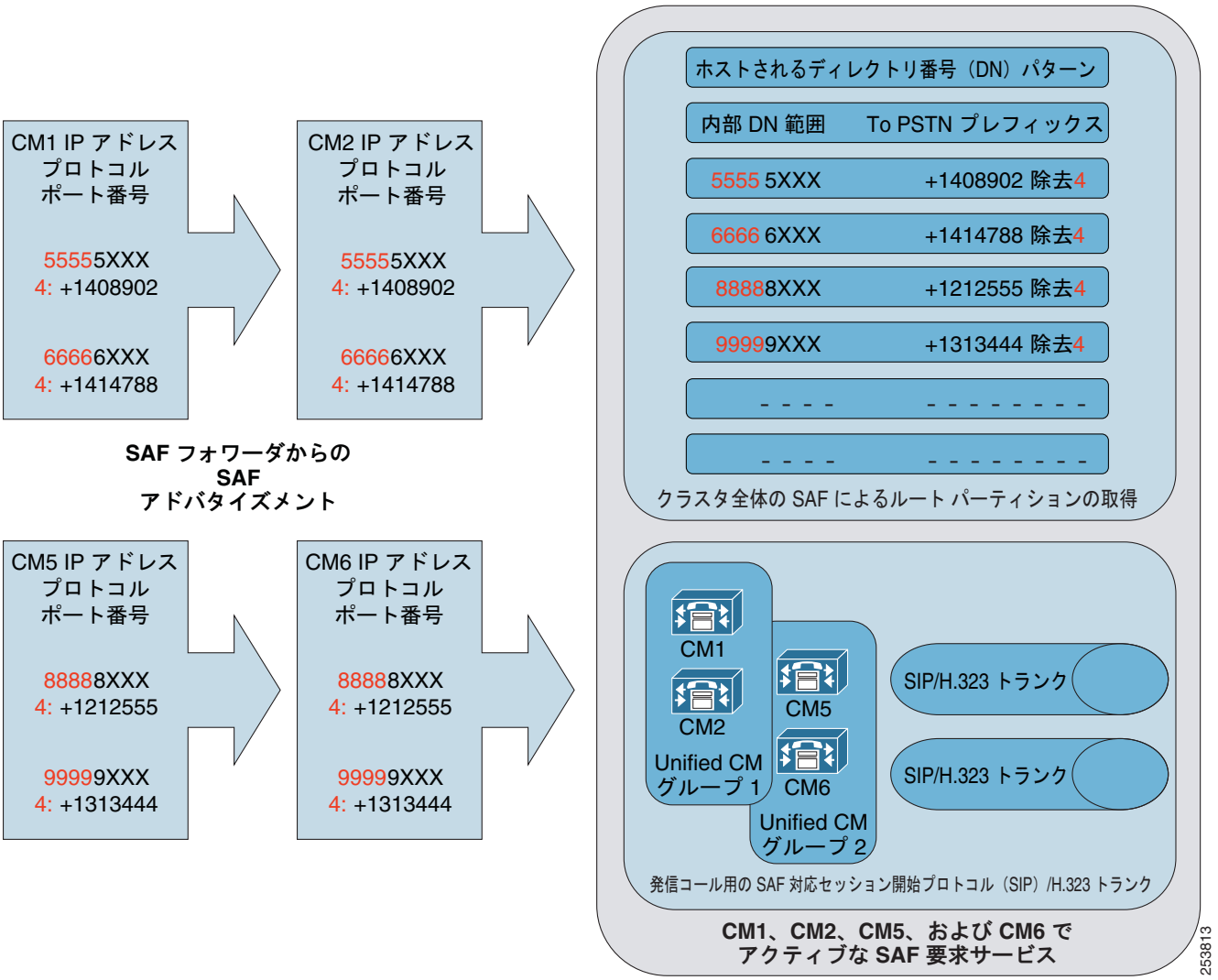


CCD 要求サービス

CCD 要求サービスは、SAF AS でアドバタイズされるホスト DN ルートに関する情報を収集して、SAF 学習ルート用のパーティションに配置します（図 5-27 を参照）。要求サービスは、発信 SAF コールを開始するのに使用する SAF トランクを選択するときにも使用されます。複数の SAF 対応トランクを選択できます。複数のトランクを選択した場合、発信コールに使用する SAF トランクとその対応する Unified CM Group サーバ ノードがラウンドロビン方式で選択されます。アドバタイズ サービスと同様に、要求サービスには通常同じプロトコル タイプのトランクを関連付けます。また、要求サービスは、学習した DN パターンや学習した「To PSTN」パターンに数字をプレフィックスとして付加できます。

Unified CM クラスタに要求サービスを 1 つだけ設定でき、その要求サービスは関連付けられた SAF トランクの Unified CM Group のすべてのノードでアクティブになります。

図 5-27　Unified CM CCD 要求サービス



CCD 学習パターンのブロック

Unified CM を使用すると、SAF CCD 管理者は SAF CCD 学習ルート パーティションから学習ルート情報を消去およびブロックできます。次のエントリの 1 つ以上に一致するかどうかに基づいて、ルートをブロックできます。

- Learned Pattern（たとえば、500*X*）
- Learned Pattern Prefix（たとえば、+1408）
- Remote Call Control Entity Name（エンタープライズ パラメータでは、これは Unified CM クラスタ ID です）
- Remote Call Control IP Address（これは、Cisco IOS SAF CCD ルータまたは Unified CM クラスタ内の 1 つ以上の Unified CM サーバのアドレスです）

ここに挙げたエントリは、必要に応じて次のように論理 AND を組み合せて使用できます。

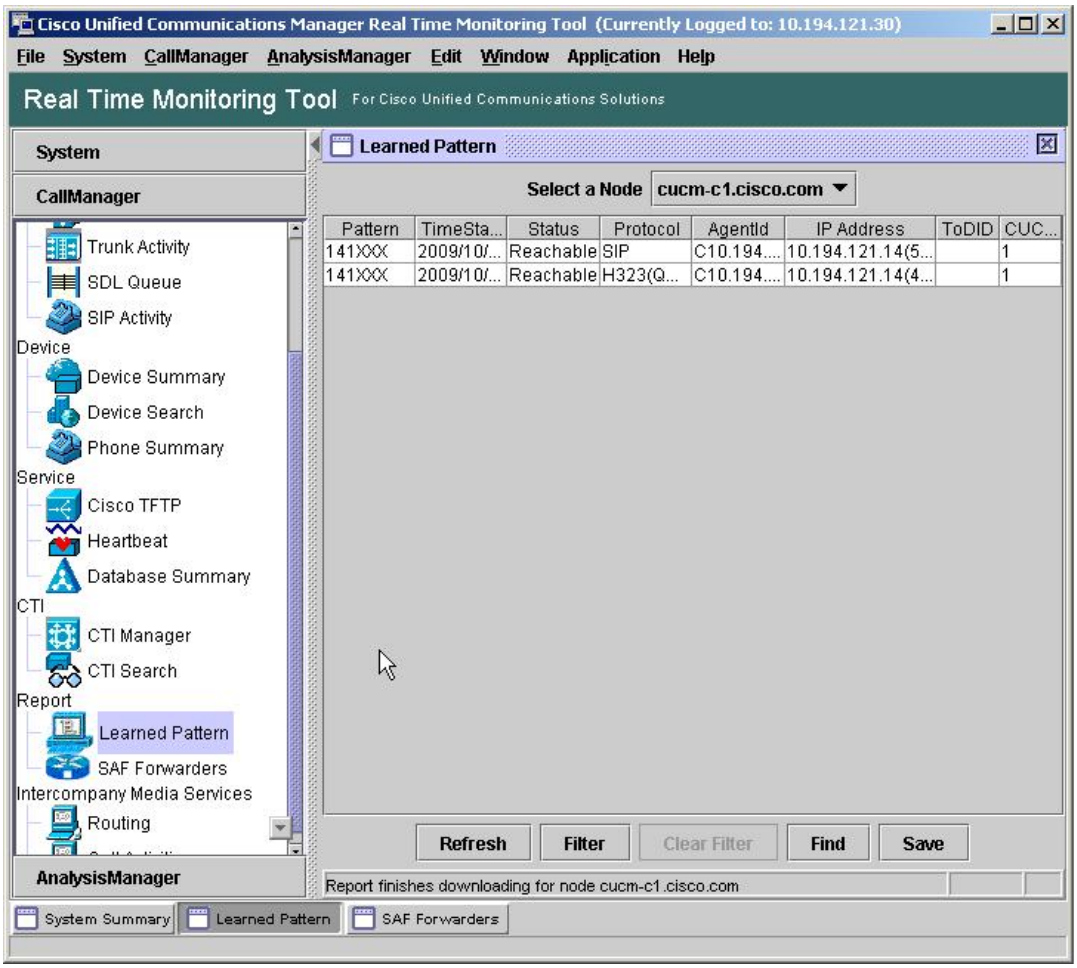
Pattern = "5XXX" AND Prefix = "+1408" AND Remote Call Control Address = "10.10.1.1"

CCD 学習パターンのブロックが特に有益なのは、SAF CCD 配置のうち、Unified CM クラスタが複数の SAF AS に接続していて、DN ルート情報を AS にアドバタイズしながら、その AS から送信される DN ルート情報の一部または全部を受信しないようにしたい場合です。

Unified CM での SAF 学習ルートの表示

SAF 学習ルートは動的な性質があるため、Unified CM データベースには保持されませんが、メモリに格納されます。SAF 学習ルートを表示し、SAF フォワーダをモニタするには、Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）を使用します（図 5-28 を参照）。

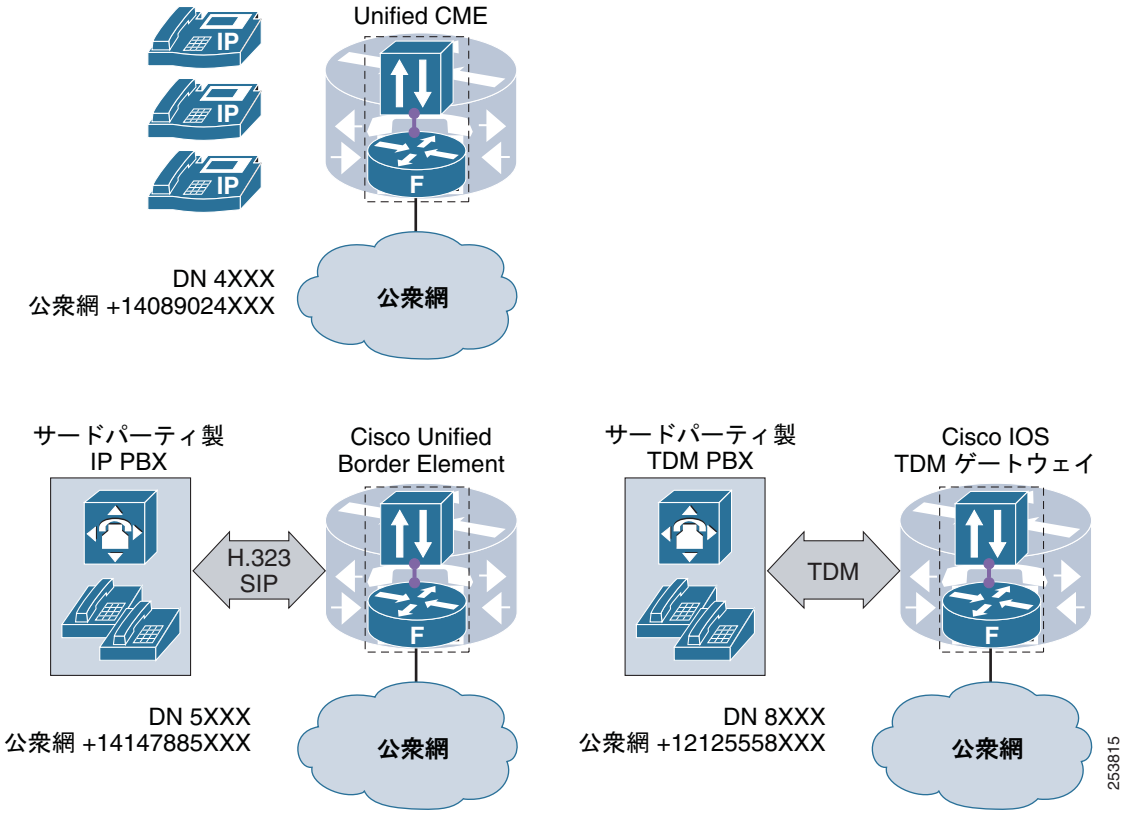
図 5-28　SAF CCD 用 Real-Time Monitoring Tool（RTMT）



Cisco IOS-Based SAF CCD

Cisco IOS ベースの SAF CCD は、Cisco IOS Release 15.0(1)M を搭載した Integrated Services Router（ISR; サービス統合型ルータ）プラットフォーム上の Unified CME、SRST、Cisco Unified Border Element、および Cisco IOS ゲートウェイでサポートされます（図 5-29 を参照）。Cisco IOS SAF CCD の設定は、ここに挙げたどの製品でも同じです。ただし、SRST は CCD の特殊な事例であり、「SAF CCD と SRST」（P.5-86）の項で説明します。

図 5-29　Cisco IOS ベースの SAF CCD コール エージェント



Unified CME、Cisco IOS TDM ゲートウェイ、および Cisco Unified Border Element の場合、SAF CCD を使用すると、この各製品に関連付けられたエンドポイントの内部ディレクトリ番号範囲および「To PSTN」プレフィックスをアドバタイズできます。また、他の SAF CCD 対応呼制御アプリケーションから SAF アドバタイズメントをサブスクライブできます。

Cisco IOS と Unified CM のどちらの場合でも、SAF CCD を使用して外部公衆網の番号範囲（テールエンド ホップオフなど）をアドバタイズすることは推奨*しません*。その主な理由は次のとおりです。

- SAF CCD は、IP、公衆網、または TDM トランクのキャパシティに関する情報を提供しません（たとえば、SAF CCD では、2 DS0 の ISDN BRI と 24 DS0 の T1 TDM インターフェイスが等しく重み付けされます）。
- すべての SAF CCD ルートが、単一のパーティションに配置されます。つまり、どの SAF CCD ユーザもすべての SAF CCD 学習ルートにアクセスでき、SAF CCD サービス クラスを作成することはできません。

Cisco IOS SAF CCD 設定の原則は Unified CM のものと同じですが、命名規則およびコマンドは異なります。

内部 SAF クライアント

Cisco IOS ベースの SAF CCD アプリケーションの場合、SAF クライアントおよびフォワーダは Cisco IOS 内に共存します。内部 SAF クライアントと内部 SAF フォワーダとの間で、設定および認証は必要ありません。

外部 SAF クライアント

Cisco IOS SAF フォワーダに対して外部 SAF クライアントの認証を有効にするには、**external-client** Cisco IOS コマンドを使用して、外部クライアントのラベルまたは基本名、ユーザ名、パスワード、およびキープアライブ タイマーを定義します。

SAF 対応トランク

SAF トランクを定義するには、**profile trunk-route** Cisco IOS コマンドを使用します。トランクルート プロファイルでは、SAF トランクの IP アドレス、ポート番号、プロトコル（SIP または H.323）、および転送プロトコル（UDP または TCP）を定義します。

DN パターン、DN ブロック、および DN サービス

Cisco IOS では、ディレクトリ番号、DN 範囲、および「To PSTN」プレフィックスの定義および設定が、Unified CM 設定と比較すると若干異なります。Cisco IOS は、DN ブロックという概念を採用して、DN 番号および DN 範囲をグループ化します。DN ブロックには、複数の DN パターンを含めることができます。番号の削除および先頭付加に関する「To PSTN」フェールオーバー規則も、DN ブロック コマンドラインで定義します。公衆網フェールオーバー規則は、Cisco IOS では **alias** と呼ばれます（公衆網フェールオーバー規則は、サイト コードおよび拡張 DN パターンを連結したものに適用されます）。DN ブロックの Cisco IOS 設定の例を次に示します。

```
profile dn-block 1 alias 1408902 strip 3
    pattern 1 extension 5xxx
    pattern 2 extension 6xxx
```

呼制御プロファイル、DN サービス、およびサイト コード

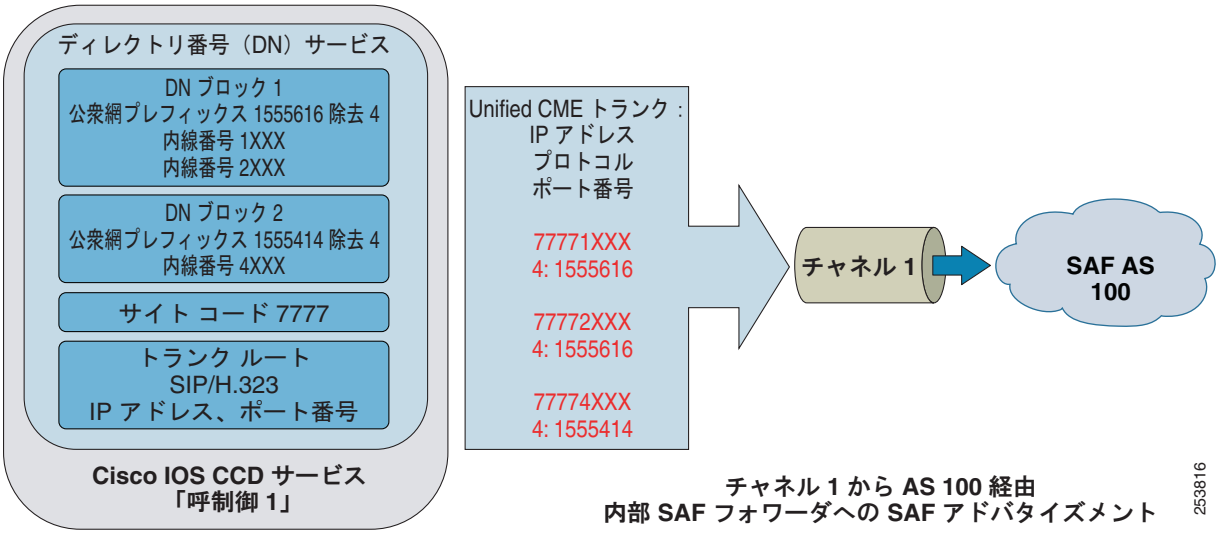
CCD 呼制御プロファイルは、DN サービスに関連付けられます。Cisco IOS の DN サービスは、Unified CM のアドバタイズ サービスと同等であると考えることができます。DN サービスは、1 つ以上の DN ブロック、1 つのトランク ルート、および 1 つのサイト コードをグループ化するために使用します。サイト コードが存在する場合、アドバタイズする拡張 DN パターンの先頭に付加される 1 つ以上の数字で構成されます。

複数の呼制御プロファイルを作成できます。同じ DN ブロック、トランク ルート、およびサイト コードを複数の呼制御プロファイルで再利用できますが、SAF AS に関連付けることができるプロファイルは 1 つだけです。

SAF AS 内の SAF サービスの公開とサブスクライブ

呼制御プロファイルは、設定された SAF「チャネル」を利用して、自身に関連付けられた DN 範囲、「To PSTN」フェールオーバー規則、およびトランク ルートを 1 つの SAF AS にアドバタイズします。SAF チャネルは、1 つの呼制御プロファイルだけに含まれる CCD サービス情報を 1 つの SAF AS に公開できます（図 5-30 を参照）。

図 5-30　チャネル 1 を介して SAF AS 100 にアドバタイズする Cisco IOS CCD サービス呼制御 1



SAF チャネルは、ワイルドカード サービス ID を使用して、SAF AS 内のすべての CCD サービスをサブスクライブできます。また、SAF サービス ID のインスタンス値で特定した SAF CCD サービスを最大 2 つまでサブスクライブできます（Unified CM のインスタンス値はクラスタ PKID です）。次に例を示します。

ワイルドカード SAF サービス ID =

サービス：	**サブサービス：**	**インスタンス．**	**インスタンス．**	**インスタンス．**	**インスタンス．**
101:	2:	FFFFFFFF.	FFFFFFFF.	FFFFFFFF.	FFFFFFFF.

ヒント　ルータ上の Cisco IOS SAF CCD サービスのサービス ID を表示するには、Cisco IOS コマンド **show eigrp service-family ipv4** [*AS number*] **events** を使用します。サービス ID が「connected」（たとえば、101:2:59F8412.0.0.6F0100）と表示されます。

Cisco IOS での発信 SAF CCD コール

Cisco IOS は、SAF を設定可能なセッション ターゲットとして標準の Cisco IOS 音声ダイヤル ピアに追加します。ダイヤル ピアには、標準と SAF のダイヤル ピアを選択する順序を制御するために、プリファレンス設定を割り当てることもできます。

SAF CCD と SRST

SRST CCD は、SAF 配置の特殊なタイプです。SRST CCD は、番号範囲を SAF にアドバタイズしません。Unified CM や Unified CME など他の SAF CCD サービスからのアドバタイズメントを監視するだけです。SRST CCD は、SAF 学習 IP ルートを使用しません。公衆網ルートだけを使用し、ルータおよび関連付けられた電話機が SRST モードのときにだけ機能します。

SAF for SRST CCD を使用すると、新たに SRST ルータを Unified Communications ネットワークに追加するたびに、すべての SRST ルータを新しい番号拡張規則で更新するという非常に手間のかかるタスクを回避できます。

（SAF ではなく）標準の SRST の動作では、Unified CM が使用できなくなると、電話機が内線番号を SRST リファレンス ルータに登録します（図 5-31 を参照）。SRST モードでは、通常どおり内線番号をダイヤルして、SRST ルータに登録されている他の電話機にコールを発信できます。SRST モードの電話機を使用して別のサイトの電話機をコールするときは、着信側電話機の公衆網番号をダイヤルする必要があります（図 5-32 を参照）。Cisco IOS の番号拡張コマンドは SAF CCD の公衆網フェールオーバー規則とよく似ており、このコマンドを使用すると、ダイヤルした内線番号を SRST モードの完全な公衆網番号に拡張できます。

SRST ルータの数が多い Unified Communications 配置では、新たに SRST ルータを Unified Communications ネットワークに追加すると、すべての SRST ルータがこの新規 SRST サイトの公衆網アクセス プレフィックスに対応する番号拡張規則を追加する必要があります。

SAF for SRST CCD を使用すると、すべての SRST サイトの公衆網フェールオーバー規則を SAF AS 内のすべての SRST ルータに分散させることができます。

図 5-31　SAF SRST CCD のある Unified CM 配置の通常の（Unified CM）動作

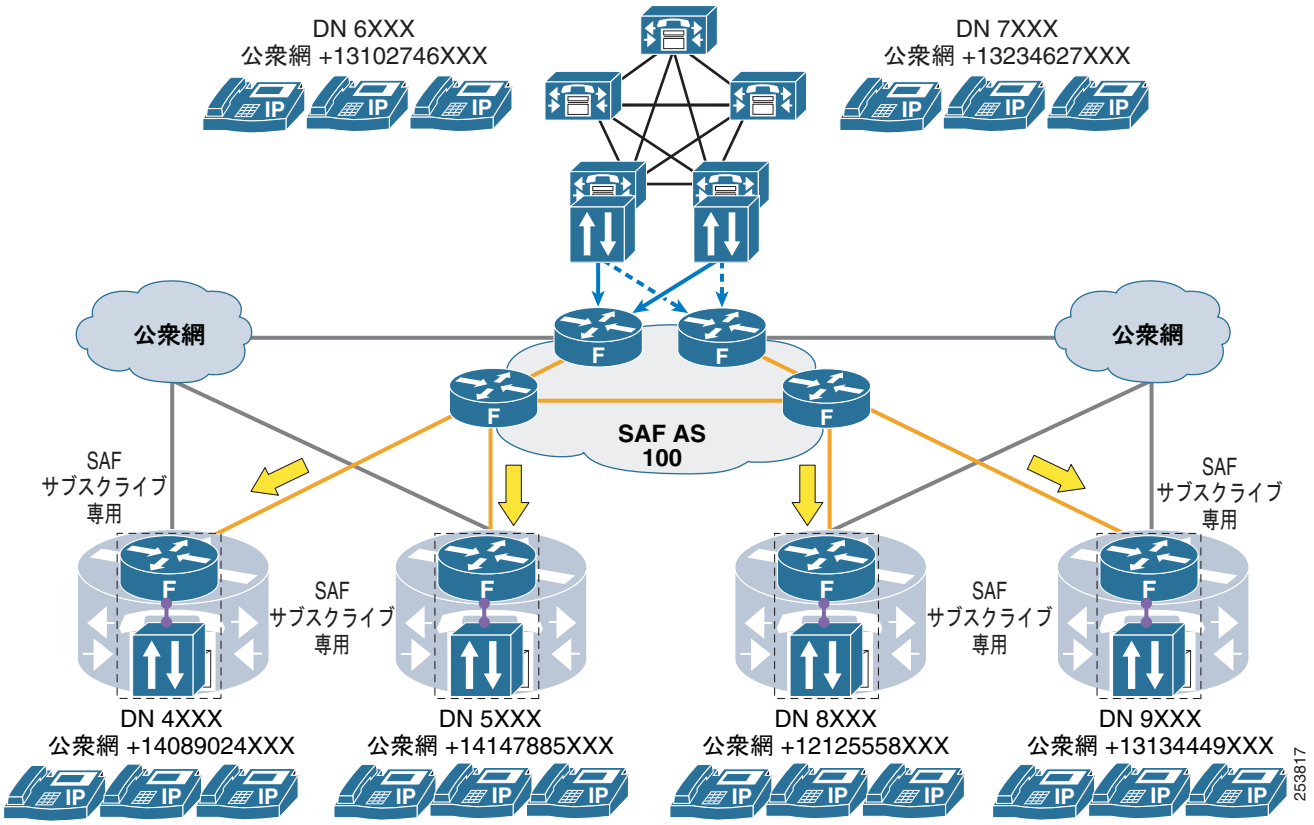
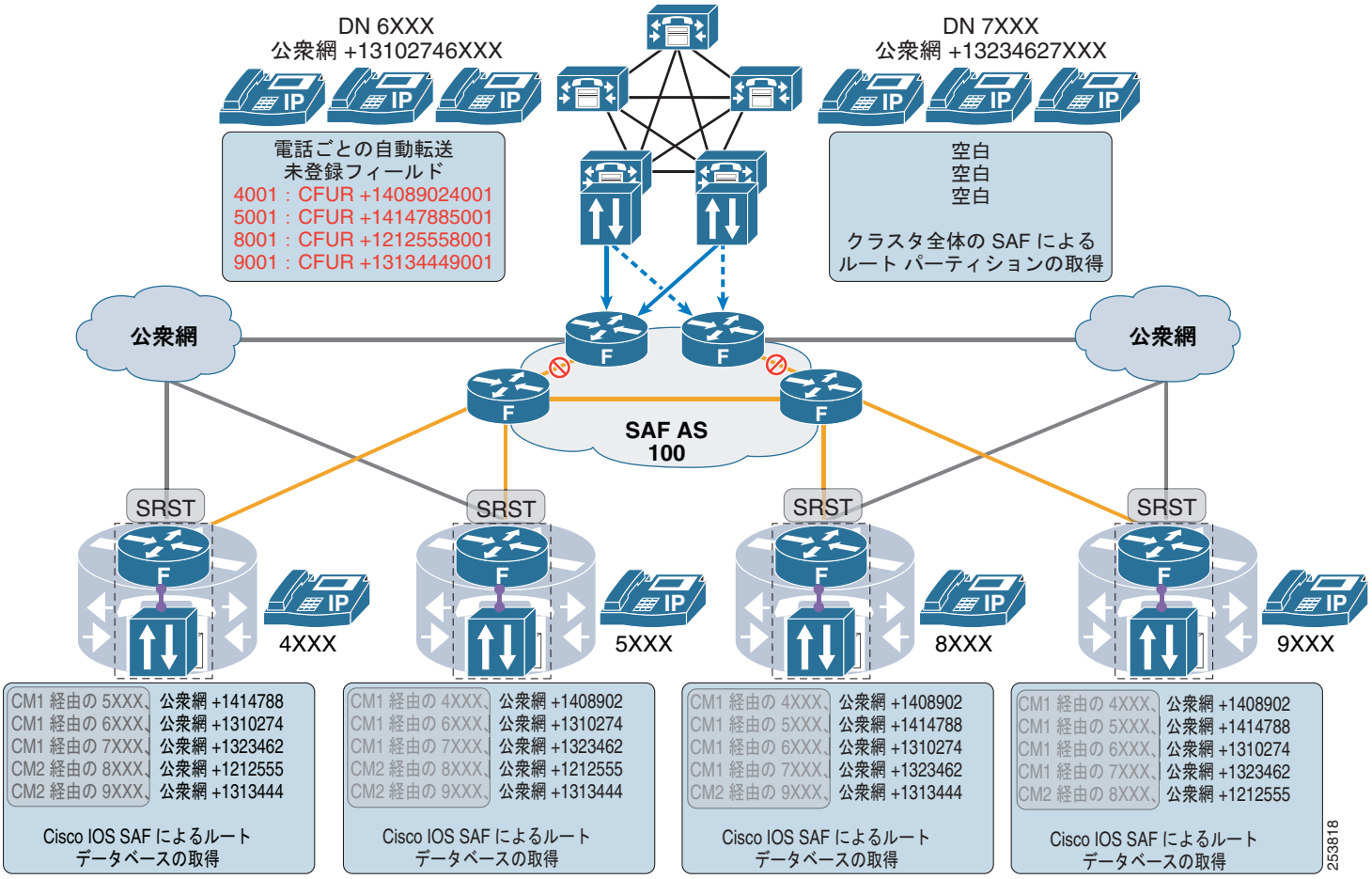


図 5-32　SAF SRST CCD のある Unified CM 配置の SRST 動作



代表的な SAF CCD ベースの Unified Communications 配置

図 5-33 に、代表的な SAF CCD ネットワーク配置を示します。

図 5-33　リージョン コール エージェント、SAF クライアント、および SAF フォワーダのあるグローバル SAF ネットワーク

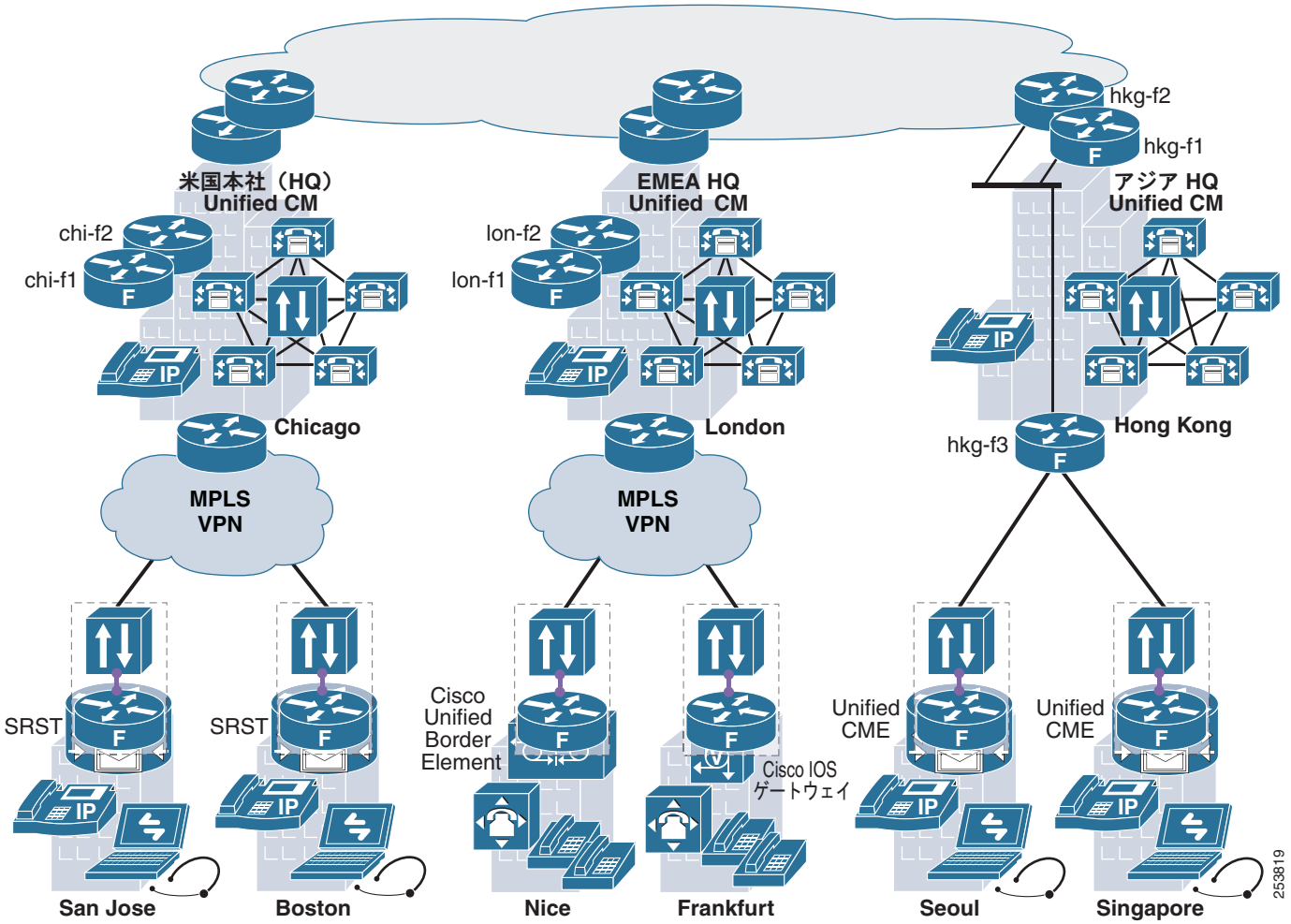
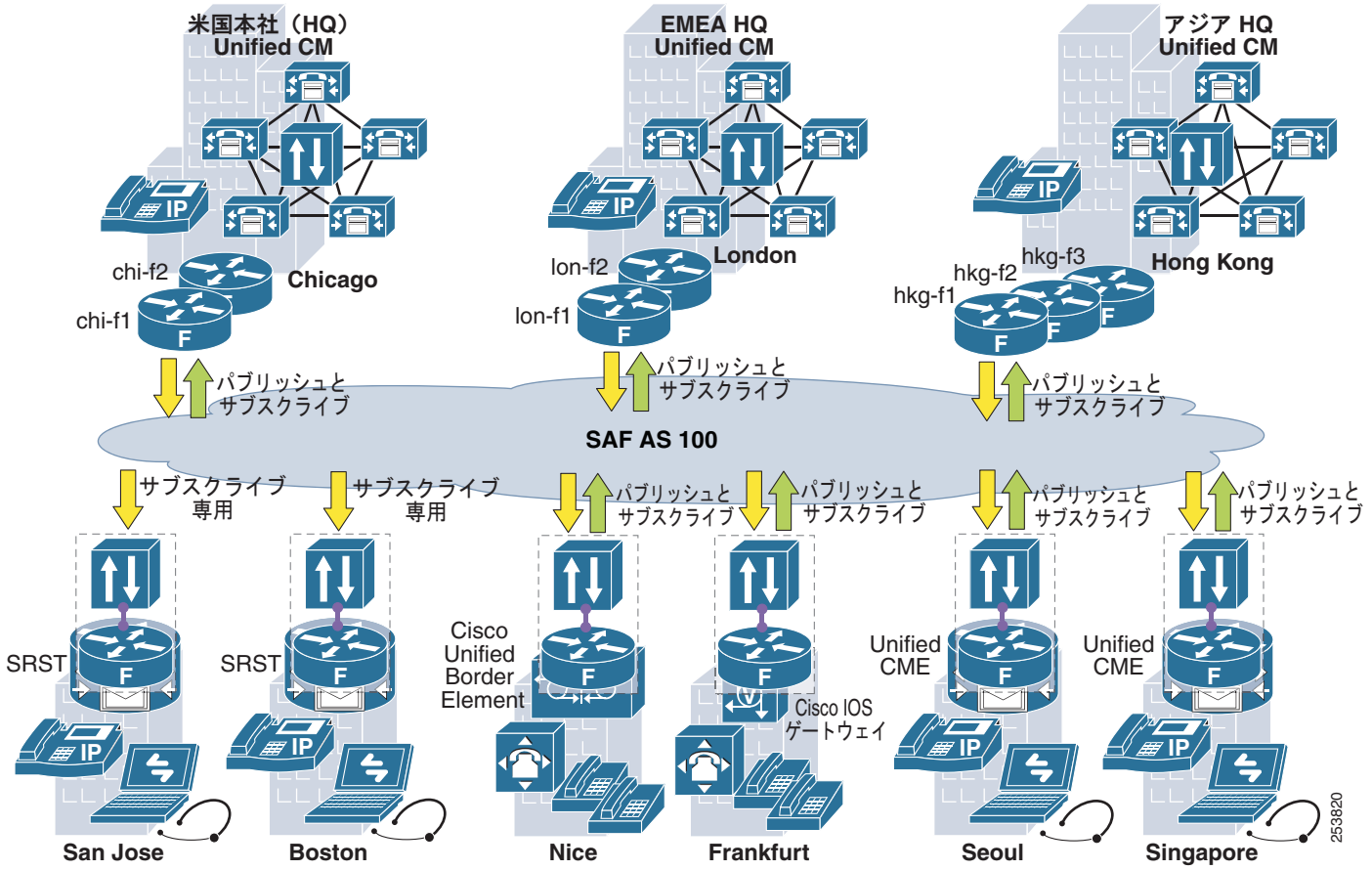


図 5-34 に、リージョン コール エージェント、SAF クライアント、および SAF フォワーダのある同じグローバル SAF ネットワークの論理図を示します。

図 5-34　リージョン コール エージェント、SAF クライアント、および SAF フォワーダのあるグローバル SAF ネットワークの論理図



SAF CCD 配置の考慮事項

SAF CCD への移行は比較的リスクがありません。SAF を使用するデバイスをネットワークで有効にする前に、SAF CCD ネットワークを構築して基本的な動作およびスケーラビリティをテストできます。Unified CM ユーザは、SAF 学習ルート パーティションを自身のデバイスまたはプロファイルに追加することによって、SAF CCD ネットワークを使用できます。Cisco IOS では、標準のダイヤル ピアよりも SAF ダイヤル ピアのプリファレンスを優先させることができます。これにより、SAF をネットワーク全体で段階的に有効にできます。

次のスケーラビリティ制限が、Unified CM および Cisco IOS SAF CCD 製品に適用されます。

- アドバタイズする DN パターンは Unified CM クラスタあたり最大 2,000
- 学習する DN パターンは Unified CM クラスタあたり最大 20,000
- アドバタイズする DN パターンは Unified CME、Cisco Unified Border Element、または Cisco IOS ゲートウェイあたり最大 125
- 学習する DN パターンは Unified CME、Cisco Unified Border Element、Cisco IOS ゲートウェイ、または SRST あたり最大 6,000（プラットフォーム依存）

極めて大規模な SAF CCD ネットワークでは、複数の SAF AS を使用して、SAF がアドバタイズする DN パターンの配布を制限できます。Unified CM や Cisco Unified Border Element では、1 つの SAF AS からの SAF アドバタイズメントを手動で集約して、別の SAF AS に静的にアドバタイズすることもできます。

SAF CCD ポート番号

SAF CCD は、次のポート番号を使用します。

- SAF EIGRP：IP プロトコル 88
- Unified CM SAF クライアントから Cisco IOS SAF フォワーダへの間 ：TCP ポート 5050（設定可能）
- アドバタイズする SIP トランク：ポート 5060
- アドバタイズする H.323：エフェメラル ポート番号

（注） Cisco Adaptive Security Appliance（ASA）ファイアウォールは、標準の SIP 検査およびフィックスアップを使用して、SAF 対応 SIP トランク コールの RTP メディア ストリームのためにファイアウォールのピンホールを開きます。SAF 対応 H.323 トランク コールの H.323 検査およびフィックスアップはサポートされません。

CHAPTER 6

IP テレフォニーの移行オプション

この章では、個々のスタンドアロン通信コンポーネントを統合 Cisco Unified Communications システムに移行するための複数の方法について説明します。この章のトピックは、使用するプロトコルや必要な機能に基づく決定などの技術的視点ではなく、カスタマーまたはビジネスの視点から説明しています。

共存か、または移行か

これは、回答する必要がある重要な質問です。

共存とは、通常、2 つ以上のシステムが長期間（6 か月を超える任意の期間）にわたって共存することを意味します。このシナリオでは、PBX、ボイスメール、またはその他のいずれの機能であっても、機能の透過性が重要な考慮事項になります。必要な機能の透過性レベルを実現するために、既存のシステムへの投資やアップグレードが必要となる場合があります。

移行は、通常、短期間（6 か月未満の任意の期間）で実施します。このシナリオでは、ユーザは、移行が「短い」期間で完了することを認識しているため、既存の機能のサブセットをより許容しやすくなります。この「短い」期間については、多くの場合、既存のシステム機能で十分であるため、一般的に、移行では共存よりもコストが少なくなります。

移行の前提条件

カスタマーは、任意の Unified Communications サービスを実装する前に、基盤となる IP インフラストラクチャが「UC 対応」（冗長性、ハイ アベイラビリティ、Quality of Service（QoS）、インライン パワー イーサネット ポートなど）となっていることを確認する必要があります。詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。

通常、すべての要件（FAX/ モデム、環境制御システムなど）が適切に特定および考慮されるように、何らかのサイト調査またはユーザ調査を実行する必要があります。

Unified Communications の移行

Unified Communications システム（または該当する個々の Unified Communications サービス）への移行には、次の 2 つの方法があります。

段階的な移行

この方法は、通常、配置する Unified Communications サービスを中心とした、小規模な試用から開始します。カスタマーが Unified Communications サービスの試用に慣れたあと、移行を開始します。この場合は、ユーザのグループを一度に 1 つずつ Unified Communications サービスの実稼動バージョンに移動します。

並行カットオーバー

この方法は、段階的アプローチと同様に開始しますが、試用が進行し、カスタマーが納得した時点で、すべてのユーザを一度に新しい Unified Communications サービスにカットオーバーする日時を選択します。

並行カットオーバーには、段階的な移行に比べて次の利点があります。

- 並行カットオーバーを採用した場合、予期しない事態が発生したとき、最小限の労力で、基本的に以前の状態のままのシステムに戻すことができる、バックアウト計画を使用できます。たとえば、PBX からの段階的な移行の場合、IP テレフォニー ゲートウェイからの着信 PSTN トランクを PBX に転送して戻すだけで、ユーザに対してサービスを復元できます。
- 並行カットオーバーを採用すると、ライブ トラフィックを伝送する前に、Unified Communications サービスの設定を確認できます。このシナリオでは、Unified Communications サービスのカットオーバー前に任意の期間実行できるため、すべてのユーザ情報（電話機、ゲートウェイ、ダイヤル プラン、メールボックスなど）を適切に設定できます。
- 加入者がカットオーバー前の都合のよいときに Unified Communications サービスを調べたり使用したりできるようにすることによって、ゆとりを持ってトレーニングを実行できます。
- システム管理者は、「利害共同体」のために特別なプロビジョニングを行う必要はありません。段階的な移行では、コール ピックアップ グループ、ハント グループ、シェアド ラインなどの機能の完全性の維持を考慮する必要があります。これらのアソシエーションは、並行カットオーバーで完全な Unified Communications サービスに移行するときに、簡単に決定できます。

並行カットオーバーには、サポートするインフラストラクチャを含み、Unified Communications サービスのために最初の時点で十分な資金が必要になるという短所があります。これは、サービスを提供する前に、サービス全体を配置する必要があるためです。一方、段階的な移行では、必要となったときにシステムの個々のコンポーネントを購入できます。このアプローチでは、完全に配置する前に、小規模な試用システムから開始できます。

いずれかの方法が正しいというわけではなく、それぞれのカスタマーの環境と優先事項に応じて、最適なオプションが決まります。

例 6-1　　IP テレフォニーの段階的な移行

このアプローチは、通常、主要な企業 PBX に接続された IP テレフォニーの小規模な試用を伴います。使用するシグナリング プロトコルの選択は、必要な機能および実装コストによって決まります。Cisco Unified Communications Manager（Unified CM）では、通常の PSTN タイプ PRI や QSIG PRI、および H.323 と SIP をサポートしています。これらのオプションのうち、QSIG PRI は、通常、任意の 2 つのシステム間に最高レベルの機能透過性を提供します。

PSTN タイプ PRI は、基本的なコール接続および Automatic Number Identification（ANI; 自動番号識別）を提供します。このプロトコルで発信者名情報がサポートされる場合もあります。このレベルの接続は、すべての PBX で使用できるため、最もコストがかからないオプションと見なされます。つまり、PBX は、PRI を介してパブリック ネットワークに接続できる場合、Unified CM に接続できます。これは、Unified CM が接続の「ネットワーク」側として設定できるためです。

PSTN タイプ PRI または QSIG では、段階的な移行のプロセスが似ています。ユーザをグループ単位で PBX から Unified CM に移動しますが、一度にグループを 1 つずつ移動して、移行を完了します。

約 60 のビルに分散された 23,000 人ものユーザで構成されている Cisco San Jose キャンパスでは、この方法で IP テレフォニーへの移行が行われました。週末ごとに 1 つのビルという割合で、開始から完了までちょうど 1 年かかりました。選択されたビル内のすべてのユーザが特定され、金曜日の夜に、それらのユーザの内線番号が PBX から削除されました。同時に、PBX ルーティング テーブルへの追加が行われ、これらの内線番号にダイヤルしたすべての人が正しい PRI トランクを通じてルーティングされ、Unified CM に配信されるようにしました。週末の間に、ユーザの新しい内線番号が Unified CM に作成され、新しい IP Phone が該当するオフィス ロケーションに届けられ、月曜日の朝には使用できる準備が整っていました。このプロセスは、すべてのユーザが移行されるまで、各ビルに対して繰り返されました。

例 6-2　　IP テレフォニーの並行カットオーバー

すべての IP Phone およびゲートウェイが完全に設定および配置され、ユーザのデスク上には IP Phone と PBX 電話機の両方が同時に置かれます。このアプローチでは、システムをテストする機会だけでなく、新しい IP Phone にユーザが慣れる機会を提供します。発信専用のトランクも IP テレフォニー システムに接続できるため、新しい IP Phone を使用して外部コールおよび内部コールを発信する機会がユーザに提供されます。

IP テレフォニー システムが完全に配置された時点で、着信 PSTN トランクを PBX から IP テレフォニー ゲートウェイに移動して新しいシステムを完全なサービスに移行する日時を選択できます。IP テレフォニー システムの運用に確信を持てるまで、PBX をそのまま残しておき、確信できた時点で PBX の使用を停止することもできます。

Cisco San Jose キャンパスのボイスメール サービスは、23,000 人ものユーザにサービスを提供する 4 つの Octel 350 システムによって行われていました。Cisco Unity サーバがインストールされ、ユーザのメールボックスが設定されました。ユーザは、新しいアクセス番号をダイヤルして自分の Unity メールボックスにアクセスできます。これにより、自分の名前とグリーティングを録音し、また同時に新しい Telephony User Interface（TUI; テレフォニー ユーザ インターフェイス）に慣れることができます。約 2 週間後、Unified CM Bulk Administration Tool（BAT）の更新が金曜日の夜に実行され、話中転送番号と無応答転送番号（CFB/CFNA）、および Unity システムへのすべてのユーザの Messages ボタンの宛先番号が変更されました。月曜日の朝に仕事に戻ったときには、Unity によるサービスがユーザに提供されていました。Octel 350 システムは 1 か月間そのまま残されたため、Octel 350 システムの使用停止までに、ユーザは Octel 350 システムに残っていたすべてのメッセージに応答できました。

マルチサイト企業における QSIG の必要性

1 つのロケーションだけで構成される企業もあれば、複数のサイトで構成される企業もあります。企業によっては、遠く離れた場所に分散している可能性もあります。マルチサイト企業用の PBX ネットワークは、通常、独自のプロトコル（Avaya DCS、Nortel MCDN、Siemens CorNet、NEC CCIS、Fujitsu FIPN、Alcatel ABC など）を実行する T1 トランクまたは E1 PRI トランクをロケーションに応じて使用して接続されています。これらの独自のネットワーキング プロトコルによって、PBX はエンド ユーザ間に高レベルの機能透過性を提供できます。

QSIG は、異なるベンダーが提供する PBX の相互接続を可能にするために開発されたため、同様のレベルの機能透過性を実現します。

QSIG をサポートすることで、Unified CM を大規模な企業ネットワークに導入できると同時に、ユーザ間の機能透過性も維持できます。PBX ロケーションは、IP テレフォニーに適宜変換できます。

ただし、短期間で PBX の使用を停止する場合、PBX 上で QSIG をすでに有効にしているか、または PBX の追加機能が特に必要である場合を除き、PBX のアップグレード コストは妥当ではありません。たとえば、PBX を 2 ～ 3 か月で使用中止にする予定である場合、PBX で QSIG を有効化するのに 30,000 ドルかけるのは有益ではありません。

IP テレフォニーの移行の概要

IP テレフォニーの移行の 2 つの方法はいずれも適切に機能し、いずれか一方が正しいということはありませんが、ほとんどの場合、並行カットオーバーの方法が、より適切に機能します。また、大規模な企業では、QSIG を使用して Unified CM を企業ネットワークの一部に組み込むことによって、いずれの移行方法にも改良を加えることができます。

シスコは、Unified CM システムと PBX システム間の相互運用性テスト専用の実験施設を持っています。このテストの結果は、次の Web サイトに公開されているアプリケーション ノートとして入手できます。

http://www.cisco.com/go/interoperability

このアプリケーション ノートは頻繁に更新され、この Web サイトには新しいドキュメントが絶えず追加されています。この Web サイトを頻繁に確認して、最新情報を入手してください。

集中型 Unified Communications 配置

企業が Unified Communications の集中型配置を選択した場合は、次の 2 つのオプションがあります。

- 外側から開始し、中央サイトに向かって内側に進める（つまり、最も小さいサイトから最も大きいサイトへ）。
- 中央サイトから開始し、エッジに向かって外側に進める。

ほとんどのカスタマーは、次の利点があるため、最初のオプションを選択します。

- すべての Unified Communications サービスを完全に配置したあと、Unified Communications をリモート ロケーションに配置する前に小規模な試用を実行できる。
- Unified Communications の配置は、一度に 1 つずつのロケーションで実行でき、以降のロケーションは適宜移行できる。
- このオプションは、Unified Communications のコア サービスが中央サイトに配置されたあとには、実装コストが最も低くなる。
- IT スタッフは、中央サイトに移行する前に、小規模サイトの移行時に貴重な経験を積むことができる。

リモート サイトは、並行アプローチで移行する必要がありますが、中央サイトは、並行または段階的のいずれかのアプローチを使用して移行できます。

どの Unified Communications サービスを最初に移行するか

この選択は、カスタマーの個別のビジネス ニーズに大きく依存します。また、Cisco Unified Communications ソリューションによって、個々のサービスのほとんどを他のサービスとは独立して配置できます。たとえば、IP テレフォニー、音声メッセージング、コンタクト センター、およびコラボレーションは、すべて互いに独立して配置できます。

この機能により、大幅な柔軟性がカスタマーにもたらされます。あるカスタマーが、ボイスメール システムのサポートが終了したことによって、顧客満足度の低下につながるさまざまな問題を抱えているとします。多くの場合、Cisco Unity は現在の PBX とともに配置および統合できるため、この問題を解決できます。新しいボイスメール システムが適切に運用されるようになったあと、次の Unified Communications サービス、つまり IP テレフォニーに取り組むことができます。

PART 2

Unified Communications コール ルーティング

CHAPTER 7

Cisco Unified Communications コール ルーティングの概要

ネットワーク インフラストラクチャが Cisco Unified Communications システムに配置されると、コール ルーティングのアプリケーション、コンポーネント、およびサービスをネットワーク インフラストラクチャの最上位で階層化できるようになります。ネットワーク インフラストラクチャ上に配置できる、また場合によっては配置する必要があるアプリケーションと機能は、数多く存在します。一般的に、次のコール ルーティング コンポーネント、機能、およびサービスを配置する必要があります。

- コール処理エージェント：テレフォニー サービスとコール ルーティングの機能を提供します。
- ダイヤル プラン：ユーザが行うことができるコールのタイプを制限するために、エンドポイントの番号、ダイヤルされる番号の分析、および制限クラスを提供します。
- コール アドミッション制御：コール処理コンポーネントおよびネットワーク帯域幅の全体的なコール キャパシティに基づいて、所定の時間にネットワーク上で許可するコール数を制限することにより、ネットワーク帯域幅のオーバーサブスクリプションを回避するメカニズムを提供します。
- ビデオ テレフォニー サービス：ビデオ エンドポイントをプロビジョニングおよび登録する機能以外に、ネットワーク上でビデオ コールを設定、ルーティング、および維持する機能を提供します。
- 公衆網ゲートウェイおよびプロバイダーの音声とデータ サービス：公衆網、インターネット、サービス プロバイダー IP ベースのトランクなど、企業外部の音声およびデータ ネットワークへのアクセスを提供します。
- リモート サイトのサバイバビリティ：ネットワーク接続の障害またはフラッピングが原因で中央サイトのテレフォニー サービスが使用できなくなった場合に、基本的なテレフォニー サービスをリモート サイトで継続して使用できるようにします。

本 SRND のこの章では、上記の機能、コンポーネント、およびサービスについて説明します。各章では、コンポーネントまたはサービスの概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。各章では、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこの部分に含まれる章は、次のとおりです。

- 「コール処理」（P.8-1）

  この章では、IP テレフォニー コール ルーティングを容易にする、さまざまなタイプのコール処理アプリケーションとプラットフォームについて説明します。この章では、コール処理アーキテクチャ（ハードウェア オプション、Unified CM クラスタリング機能、コール処理のハイ アベイラビリティに関する考慮事項、キャパシティ プランニングなど）について説明します。

- 「ダイヤル プラン」（P.9-1）

  この章では、コール処理アプリケーションがコールを適切な番号にルーティングできるようにする、ダイヤル プランの機能と機能性について説明します。この章では、ダイヤル プラン サービスのさまざまな側面（ダイヤル プラン構成要素、ダイヤル プラン番号オプションと設計上の考慮事項、制限クラス、着信コールと発信コールの機能、ダイヤル プランとコール ルーティング冗長メカニズムなど）について検討します。

- 「緊急サービス」（P.10-1）

  この章では、企業の IP テレフォニー環境から公衆網上の Public Safety Answering Point（PSAP）を介して緊急サービスにアクセスする方法について説明します。この内容は、医療、火災、およびその他の緊急応答サービスが重要なニーズとなる可能性があるため、ほとんどの配置において重要となります。この章では、企業の内外におけるさまざまな緊急サービス コンポーネントの概要について説明します。また、立案、911 ネットワーク サービス プロバイダー、ゲートウェイ インターフェイス、および番号とロケーションのマッピングについても説明します。

- 「コール アドミッション制御」（P.11-1）

  この章では、電話コールの音声品質が許容できなくなる原因となる、IP リンクの潜在的なオーバーサブスクリプションについて説明します。また、オーバーサブスクリプションを回避するために、所定の時間にネットワーク上で特定の数の同時コールだけを許可するためのコール アドミッション制御の使用についても説明します。この章では、コール アドミッション制御タイプ（ロケーションベースのコール アドミッション制御と RSVP など）、およびアドミッション制御サービスを適切に配置するための設計と配置のガイドラインについて説明します。

- 「IP ビデオ テレフォニー」（P.12-1）

  この章では、協力通信の重要で不可欠な要素であるビデオ テレフォニーについて説明します。この章では、ビデオ テレフォニー コンポーネント、プロトコルとコーデック、マルチポイント会議、およびビデオ コール ルーティングのゲートキーパーの側面について説明します。

- 「ゲートウェイ」（P.13-1）

  この章では、音声ゲートウェイと IP ゲートウェイについて説明します。これらのゲートウェイは、公衆電話網上の電話機に接続するためのパスを提供するため、Unified Communications 配置の不可欠なコンポーネントです。この章では、ゲートウェイ トラフィックのタイプとパターン、プロトコル、キャパシティ プランニング、プラットフォームの選択、および FAX とモデムのサポートについて説明します。

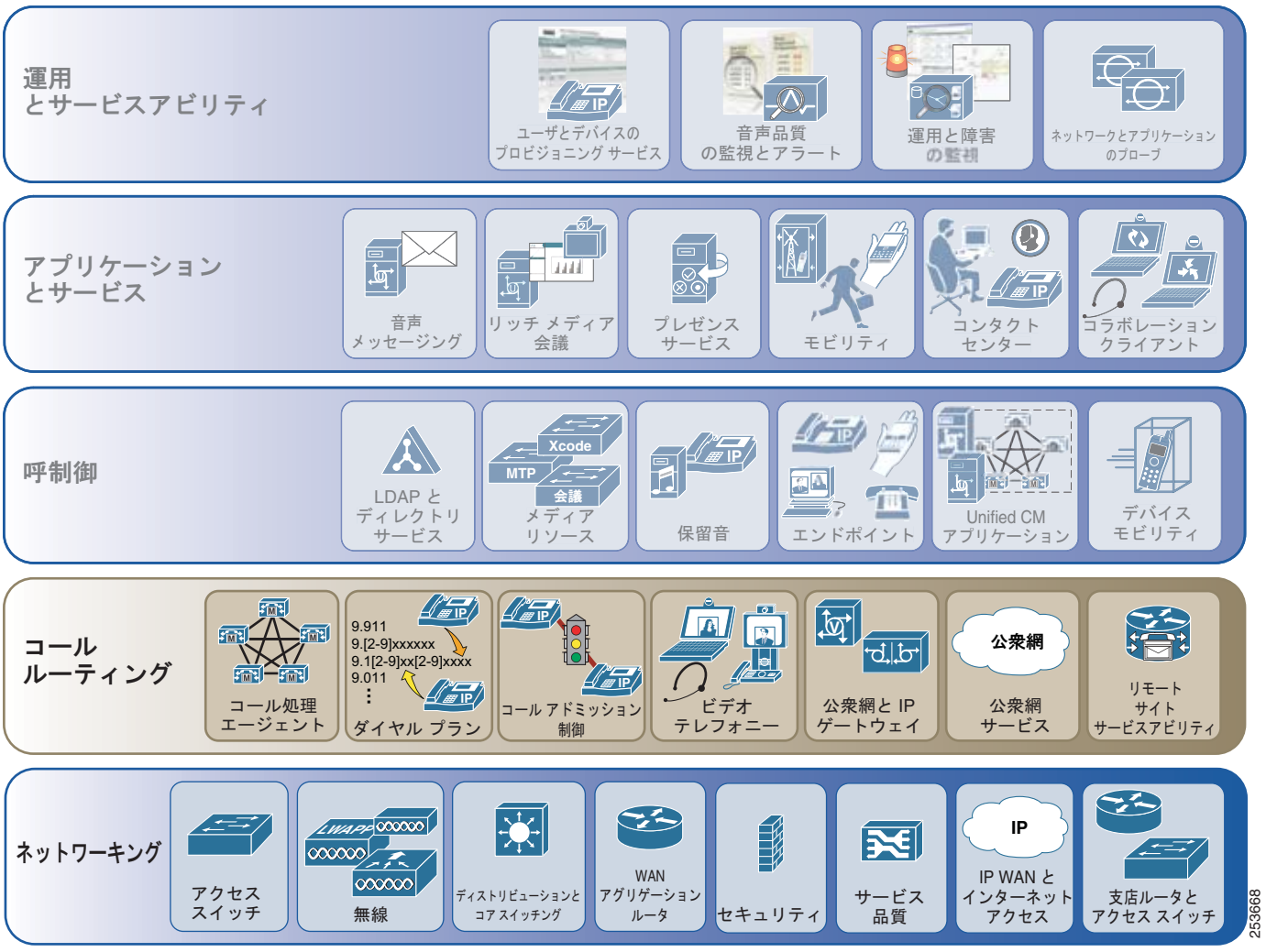
- 「Cisco Unified CM トランク」（P.14-1）

  この章では、クラスタ間トランクとプロバイダー トランクの両方について説明します。これらのトランクによって、IP を介して音声コールをルーティングしたり、さまざまな Unified Communications の機能と機能性を使用できます。この章では、H.323 トランクと SIP トランク、コーデック、およびこれらのトランクを介した付加サービスについて説明する以外に、ネットワーク コール負荷に対応するためのトランクのサイジングについて説明します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムの場合と同様、Unified Communications のコール ルーティング コンポーネントとサービスは、基盤となるネットワーク インフラストラクチャの最上位で階層化する必要があります。図 7-1 は、Cisco Unified Communications システム アーキテクチャ全体でのコール ルーティング アプリケーションとサービスの論理的ロケーションを示しています。

図 7-1　Cisco Unified Communications のコール ルーティング アーキテクチャ



Unified Communications のコール ルーティング コンポーネントとサービス（コール処理エージェント、IP ゲートウェイと公衆網ゲートウェイなど）は、基盤となるネットワーク インフラストラクチャを使用して、ネットワークに接続およびアクセスします。コール ルーティングのコンポーネントおよび機能は、基盤となるネットワーク インフラストラクチャに接続することで、エンドツーエンドのネットワーク接続および Quality of Service を利用して、企業ネットワークと公衆電話網の両方にアクセスできます。一方、コール ルーティングのアプリケーションとサービスは、基本的な Unified Communications 機能（呼制御、ダイヤル プラン、コール アドミッション制御、ゲートウェイ サービスなど）を配置内のその他のアプリケーションとサービスに提供します。たとえば、Unified CM クラ

スタは、スイッチを介して IP ネットワークに接続し、ネットワーク内のその他のデバイスおよびアプリケーションと通信する以外に、その他のロケーション内のその他のデバイスおよびサービスにアクセスします。同時に、Unified CM クラスタは、IP Phone などの呼制御コンポーネントとサービスに対して、電話登録、メディア リソースのプロビジョニングと割り当てなどのサービスを提供します。

また、コール ルーティング コンポーネントがネットワーク インフラストラクチャに依存してネットワーク接続を行っているのと同様、コール ルーティングのコンポーネントとサービスも、多くの場合、完全に機能するために相互依存しています。たとえば、Unified CM は、ネットワーク内のさまざまな IP エンドポイントに登録サービスおよびコール ルーティング サービスを提供する一方で、企業の外側にコールをルーティングするために、ゲートウェイおよびゲートウェイ サービスに完全に依存しています。

ハイ アベイラビリティ

ネットワーク インフラストラクチャの場合と同様に、重要な Unified Communications コール ルーティング サービスでは、ネットワークまたは個々のコール ルーティング コンポーネントで障害が発生した場合でも必要な機能を引き続き使用できるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。Unified CM クラスタリング メカニズムには冗長な性質が備えられているため、単一のサーバまたはコンポーネント（Unified CM クラスタのサブスクライバ ノードなど）に障害が発生しても、その影響がほとんどまたはまったくない場合があります。ただし、その他の場合には、単一の障害が複数のコンポーネントまたはサービスに影響を及ぼすことがあります。たとえば、公衆網ゲートウェイまたは IP ゲートウェイの障害によって、公衆電話網にアクセスできなくなる可能性があります。また、Unified CM などコール処理エージェントが引き続き使用可能で、ほとんどの機能とサービスを提供できる場合でも、ゲートウェイに障害が発生してパスを使用できなくなると、コールを公衆網にルーティングできません。このようなタイプの状況を回避するためには、複数の公衆網ゲートウェイを配置して、冗長なゲートウェイ サービスを提供し、コール ルーティングを必要に応じて両方のゲートウェイで処理できるように、コール処理エージェントを設定する必要があります。

ダイヤル プランやコール アドミッション制御などの機能とサービスの場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続またはコール処理エージェント アプリケーション サーバの障害によって機能が一時的に失われ、コール エージェントがコールをルーティングできなくなり、これにより、発信者がコールを発信できなくなることが含まれます。また、コール アドミッション制御サービスが、コールを初期化するエンドポイントで使用できない場合は、ネットワークのオーバーサブスクリプションも発生することがあります。たとえば、RSVP コール アドミッション制御が使用中の場合に、RSVP Agent に障害またはネットワークへの接続の切断が発生すると、コールは依然として通過できますが、コール アドミッション制御サービスではそのコールが認識されないため、品質が低下する可能性があります。このようなタイプのシナリオを回避するには、コール アドミッション制御の復元性を提供します。このことを行うには、複数の RSVP Agent を配置することにより、障害が発生した RSVP Agent によって別の RSVP Agent によるコール アドミッション制御サービスの提供が妨げられないようします。

また、ハイ アベイラビリティの考慮事項は、ビデオ エンドポイントやリモート サイトのサバイバビリティなどのコンポーネントとサービスに関する考慮事項でもあります。デバイスが中央サイトのエージェントからコール処理サービスを利用する、ネットワーク接続リモート サイトが含まれた配置の場合、たとえば、SRST を使用するリモート サイトのサバイバビリティによって、中央サイトへの接続が切断された場合でも、リモート サイト内のローカル電話機が引き続きコール処理サービスを受信するようにできます。同様に、ビデオ エンドポイントのハイ アベイラビリティを確保するために、複数の Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）を配置して、いずれかに障害が発生した場合に備えることができます。

キャパシティ プランニング

ネットワーク インフラストラクチャは、個々のコンポーネントおよびシステム全体のキャパシティとスケーラビリティを考慮して設計および配置する必要があります。同様に、コール ルーティング コンポーネントとサービスの配置についても、キャパシティとスケーラビリティを考慮して設計する必要があります。さまざまなコール ルーティング アプリケーションとサービスを配置する場合、それらのアプリケーションとサービス自体のスケーラビリティの考慮が重要となるだけでなく、基盤となるネットワーク インフラストラクチャのスケーラビリティを考慮する必要があります。ネットワーク インフラストラクチャは、使用可能な帯域幅を持ち、コール ルーティング コンポーネントによって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティング インフラストラクチャおよびそのコンポーネントは、必要なすべてのデバイス設定と登録以外に、コール負荷または Busy Hour Call Attempts（BHCA; 最繁時呼数）を処理できる必要があります。

たとえば、Unified CM などのコール処理エージェントの場合は、ユーザ数、エンドポイント数、および時間あたりのユーザごとのコール数という観点で配置のサイズを評価し、必要な負荷を処理するために十分なリソースを配置することが重要です。コール処理エージェントのサイズが小さく、十分なリソースがない場合は、負荷の増加に伴い、機能とサービスが失敗するようになります。コール処理の配置のサイズを設定する場合の 2 つの主な考慮事項は、コール処理タイプとコール処理ハードウェアです。これらは両方とも、ユーザ、ロケーション、デバイスなどの数を考慮して、システムのサイジングを適切に設定するために重要です。例として、Cisco Unified Communications Manager は、Cisco Unified Communications Manager Express よりもキャパシティが大幅に高いため、大規模な配置への使用に適しています。また、コール処理エージェントを実行するために選択されたサーバ プラットフォームによって、多くの場合、最大の負荷が決まります。

リモート サイトのサバイバビリティのためのキャパシティ プランニングは、バックアップ コール処理ハードウェアに依存するという点で、ほとんど同じです。バックアップまたは存続可能なコール処理サービスを提供するために、適切な Cisco IOS プラットフォームを選択する場合は、通常、中央サイトへの接続が切断されたときにそのサイトでサポートする必要があるデバイスまたはユーザの数を決定することから開始します。このサイジングで同等に重要となるのは、ローカル公衆網ゲートウェイ サービスです。中央サイトへの接続が切断された場合、ローカル公衆網ゲートウェイには、最も煩雑する時間に、すべてのコールをブロックされることなくルーティングできる十分な回線がありますか。これに対する回答がいいえである場合、コール処理をバックアップできるようにリモート サイトを適切にサイジングするには、ゲートウェイまたはトランクを追加する必要があります。

公衆網ゲートウェイと IP ゲートウェイについても、配置のサイズを適切に設定して、最も煩雑する時間におけるすべてのコールを処理するために、十分なキャパシティを使用できるようにする必要があります。場合によっては、十分なリソースを提供するために、複数の公衆網ゲートウェイまたは IP ゲートウェイを配置する必要がある場合があります。

コール アドミッション制御のサイジングを行う場合は、必要なコール数をサポートするために、ネットワーク接続上で十分な帯域幅を使用できるようにしてください。十分な帯域幅を使用できない場合、追加のネットワーク キャパシティ、ゲートウェイ、および IP トランクまたはテレフォニー トランクが必要となる場合があります。

ダイヤル プラン サービスのサイジングも重要となります。ただし、多くの場合、エンドポイントや電話番号の数、ルート パターン、またはその他のダイヤル プラン構成要素の観点からのダイヤル プラン キャパシティは、使用されるコール処理エージェントおよびプラットフォームに完全に依存します。

ビデオ テレフォニーなどのコンポーネントおよびサービスの場合、適切なサイジングが同様に重要となります。ビデオ テレフォニーのキャパシティ プランニングに関する考慮事項では、主に、ネットワークの帯域幅、使用可能なビデオ ポート、および MCU セッションが重要となります。基盤となるネットワーク インフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、アプリケーション サーバおよび MCU を増やしたり、サーバまたは MCU ハードウェアを大容量モデルにアップグレードしたりすることで、キャパシティを追加できます。

CHAPTER 8

コール処理

音声コールとビデオ コールの処理は、IP テレフォニー システムによって提供される重要な機能です。この機能は、特定のタイプのコール処理エンティティまたはコール処理エージェントによって処理されます。コール処理の操作は重要であるため、ユニファイド コミュニケーションの配置を設計して、コール処理システムが、必要なユーザ数およびデバイス数を処理するのに十分なスケーラビリティと、ネットワークおよびアプリケーションのさまざまな異常または障害を処理するのに十分な復元性を持つようにすることが重要です。

この章では、シスコのコール処理製品によってスケーラブルで復元性のあるコール処理システムを設計するためのガイドラインを示します。このような製品には、Cisco Unified Communications Manager（Unified CM）、Cisco Unified Communications Manager Business Edition（Unified CMBE）、および Cisco Unified Communications Manager Express（Unified CME）があります。また、この章ではゲートキーパー機能についても説明します。この機能は、複数のコール処理システムまたはコール処理エージェントが並行して配置されるシナリオにおいて、ユニファイド コミュニケーションの配置のもう 1 つの重要な機能です。すべての場合で、主に次の要素を中心に説明します。

- 規模：ユーザ、ロケーション、ゲートウェイ、アプリケーションなどの数
- パフォーマンス：コールのレート
- 復元性：冗長性の規模

この章では、特に次のトピックについて説明します。

- 「コール処理アーキテクチャ」（P.8-3）

  ここでは、一般的なコール処理アーキテクチャおよびさまざまなコール処理ハードウェア オプションについて説明します。また、Unified CM クラスタリングについても説明します。

- 「コール処理のハイ アベイラビリティ」（P.8-14）

  ここでは、ネットワークの冗長性、サーバおよびプラットフォームの冗長性、ロード バランシングなど、コール処理のハイ アベイラビリティの考慮事項について説明します。

- 「コール処理のキャパシティ プランニング」（P.8-25）

  ここでは、エンドポイントやユーザ、ロケーション、リージョン、トランク、ゲートウェイの数など、コール処理配置のサイジングのためのガイドラインを示します。また、この章では、Unified Communications Sizing Tool についても説明します。このツールは、Unified Communications の展開のさまざまなコンポーネントのサイジングおよび必要なリソースに関するガイダンスを提供します。IP テレフォニー展開を計画するときは、このツールを使用する必要があります。

- 「コール処理の設計上の考慮事項」（P.8-34）

  ここでは、基本設計のガイドラインとコール処理を配置するためのベスト プラクティスの要約リストを示します。

- 「コンピュータ テレフォニー インテグレーション（CTI）」（P.8-37）

  ここでは、Cisco Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）アーキテクチャについて説明し、CTI のコンポーネントとインターフェイス、CTI 機能、CTI のプロビジョニングとキャパシティ プランニングについて説明します。

- 「ゲートキーパーの設計上の考慮事項」（P.8-46）

  ここでは、Cisco Unified Communications の配置でゲートキーパーをどのように使用できるかについて説明します。シスコのゲートキーパーは、もう 1 台のスタンバイ ゲートキーパーとペアにすることも、クラスタ化してさらに高いパフォーマンスと復元性を実現することもできます。ゲートキーパーは、コール ルーティングとコール アドミッション制御に使用することもできます。

- 「Unified CM と Unified CM Express の相互運用性」（P.8-54）

  ここでは、分散型コール処理配置における Cisco Unified CM と Cisco Unified Communications Manager Express（Unified CME）間での H.323 と SIP での統合について説明します。

この章の新規情報

表 8-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 8-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco MCS 7890-C1（Unified CMBE 3000 専用アプライアンス）	「コール処理ハードウェア」（P.8-5）	2011 年 6 月 30 日
仮想 Unified CM 配置用の仕様ベースの VMware ハードウェア サポート、Open Virtualization Archive（OVA）テンプレート、およびエンドポイント登録と CTI キャパシティの増加	「仮想配置用の Cisco ハードウェア」（P.8-7） 「Unified CM のキャパシティ プランニング」（P.8-25） 「UCS プラットフォームでの Unified CM のキャパシティ プランニング」（P.8-26） 「CTI のキャパシティ プランニング」（P.8-40）	2011 年 6 月 30 日
Cisco Unified CM クラスタの最大エンドポイント キャパシティが 30,000 から 40,000 に増加（MCS 7845-I3 サーバと Unified CM 8.6 を使用）	「Unified CM のキャパシティ プランニング」（P.8-25）	2011 年 6 月 2 日
1 つの Unified CM クラスタあたりの CTI 接続および制御されるデバイスの最大制限が 40,000 に増加し（MCS 7845-I3 サーバと Unified CM 8.6 を使用）、CTI ラインおよびアプリケーション キャパシティ ファクタリングが改善	「CTI のキャパシティ プランニング」（P.8-40）	2011 年 6 月 2 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）3000	「コール処理アーキテクチャ」（P.8-3）	2011 年 2 月 28 日
Cisco Unified Computing System（UCS）C200 シリーズ ハードウェア（Unified CMBE 6000 の配置用）	「コール処理アーキテクチャ」（P.8-3）	2011 年 1 月 31 日
Computer Telephony Integration（CTI）のリソース要件	「Unified CM クラスタに必要な CTI リソースの決定」（P.8-42）	2010 年 7 月 23 日

表 8-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco UCS C シリーズ ハードウェア プラットフォームでの Unified CM の配置	「コール処理ハードウェア」（P.8-5）	2010 年 7 月 23 日
デバイスのキャパシティ プランニングと Cisco Unified Communications Manager Business Edition（Unified CMBE）の BHCA サイジング	「コール処理のキャパシティ プランニング」（P.8-25）	2010 年 4 月 2 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）のハードウェア	「コール処理アーキテクチャ」（P.8-3）	2010 年 4 月 2 日
Cisco Unified Computing System（UCS）B シリーズ ハードウェア プラットフォームでの Unified CM の配置	「コール処理ハードウェア」（P.8-5）	2010 年 4 月 2 日
UCS B シリーズ ハードウェア プラットフォーム上の Unified CM のハイ アベイラビリティに関する考慮事項（複数の UCS B200 ブレード サーバにサーバ ノード インスタンスを分散させる必要性など）	「Unified CM のハイ アベイラビリティ」（P.8-16）	2010 年 4 月 2 日

コール処理アーキテクチャ

ユニファイド コミュニケーション システムの設計と配置を成功させるには、コール ルーティング機能を提供する基盤のコール処理アーキテクチャを理解することが重要です。この機能は、次のシスコのコール処理エージェントによって提供されます。

- Cisco Unified Communications Manager Express（Unified CME）

  Cisco Unified CME は、小規模な単一サイト配置、大規模な分散マルチサイト配置、およびバックアップ機能を Cisco Unified CM の集中型コール処理配置に提供するためにリモート サイトのローカル コール処理エンティティを必要とする配置に、コール処理サービスを提供します。

- Cisco Unified Communications Manager Business Edition（Unified CMBE）

  Cisco Unified CMBE は、小規模な単一サイト配置または小規模な分散マルチサイト配置に、コール処理サービスを提供します。Cisco Unified CMBE には、CMBE 3000、CMBE 5000、および CMBE 6000 の 3 つのバージョンがあります。この 3 つのバージョン間の違いを次に示します。

  - Unified CMBE が配置されるハードウェア、および共存して実行できるアプリケーションとサービスの数。Unified CMBE 3000 および CMBE 5000 では、共存する Cisco Unified CM コール処理サービスおよび Cisco Unity Connection メッセージング サービスを提供します。Unified CMBE 6000 には、Unified CM および Unity Connection のほか、Cisco Unified Presence および Cisco Contact Center Express のサービスも含まれます。
  - システムのキャパシティ。Unified CMBE 3000 は、300 ユーザ、および最大で 400 のエンドポイントをサポートします。Unified CMBE 5000 は、500 ユーザ、および最大で 575 のエンドポイントをサポートします。Unified CMBE 6000 は、1,000 ユーザ、および最大で 1,200 のエンドポイントをサポートします。
  - インストールおよびアップグレードの手順。Unified CMBE 3000 および CMBE 5000 は、1 つのソフトウェア イメージを使用して、サポートされる Cisco MCS プラットフォーム上で Unified CM および Unity Connection のインストールやアップグレードをネイティブに実行します。Unified CMBE 6000 は、ディスクリート ソフトウェア イメージを使用して、Cisco

UCS C200 シリーズ プラットフォーム上の VMware に共存する各アプリケーション（Unified CM、Unity Connection、Unified Presences、および Unified Contact Center Express）のインストールまたはアップグレード（または両方）を実行します。

Unified CMBE 3000 および CMBE 6000 がサポートされるのは、Cisco Unified CM 8.5 からであることに注意してください。

- Cisco Unified Communications Manager（Unified CM）

  Cisco Unified CM は、小規模～非常に大規模な単一サイト配置、マルチサイト集中型コール処理配置、およびマルチサイト分散コール処理配置に、コール処理サービスを提供します。

ここでは、さまざまなコール処理ハードウェア オプションについて説明し、Unified CM クラスタリングの概要を示します。

コール処理ハードウェア

表 8-2 に、3 つのエンタープライズ コール処理タイプ、これらのコール処理アプリケーションが置かれるサーバまたはプラットフォームのタイプ、およびそれらのプラットフォームの全般的な特性を示します。

表 8-2　コール処理プラットフォームのタイプ

コール処理タイプ	プラットフォーム タイプ	シスコのプラットフォーム モデル	特性
Cisco Unified CME	Cisco IOS ルータ	2800、2900、3700、3800、および 3900 シリーズ[1]	• 単一プロセッサ • 単一または複数の電源装置（モデルによって異なる）
Cisco Unified CMBE	Cisco Unified Computing System（UCS）C シリーズ ラックマウント サーバ（Unified CMBE 6000）	UCS C200 シリーズ	• 複数のプロセッサ • 単一電源装置[2] • RAID 10 搭載の複数の SAS ディスク ドライブのサポート（ESXi を実行し、ローカル ディスク ドライブ上に Cisco Unified Communications 仮想マシンを格納） • ベア メタル サポートなし[7]
	標準 Cisco Media Convergence Server（MCS）（Unified CMBE 5000 用）	MCS 7828[3]	• 単一プロセッサ • 単一電源装置 • RAID 0/1 搭載の SATA コントローラをサポート • 2 つの IP インターフェイス
	Unified CMBE 3000 バージョン 8.5(1) 以降の標準 MCS	MCS 7816-I5	• 単一プロセッサ • 単一電源装置 • 非 RAID SATA ハード ディスク • 2 つの IP インターフェイス
	Unified CMBE 3000 バージョン 8.6(1) 以降用の専用アプライアンス	MCS 7890-C1	• 単一プロセッサ • 単一電源装置 • T1/E1 ポートを 2 個搭載した統合音声ゲートウェイ • メディア リソース用オンボード DSP • 単一の IP インターフェイス

表 8-2　コール処理プラットフォームのタイプ（続き）

コール処理タイプ	プラットフォーム タイプ	シスコのプラットフォーム モデル	特性
Cisco Unified CM	標準 MCS	MCS 7815、MCS 7816、または同等のサーバ	• 単一プロセッサ • 単一電源装置 • 非 RAID SATA ハード ディスク • 2 つの IP インターフェイス[4]
	RAID 搭載の標準 MCS	MCS 7825 または同等のサーバ	• 単一プロセッサ • 単一電源装置 • RAID 0/1 搭載の SATA コントローラをサポート • 2 つの IP インターフェイス
	ハイ アベイラビリティ MCS	MCS 7835、MCS 7845、または同等のサーバ	• 1 つまたは複数のプロセッサ • 複数の電源装置 • RAID 1 搭載の複数の Serial Attached SCSI（SAS）ドライブ • 2 つの IP インターフェイス
	Unified Computing System（UCS）B シリーズ ブレード サーバ	Cisco UCS B200 シリーズ[5]	• ハーフ幅ブレード • 複数のプロセッサ • 複数の電源装置 • 複数の SAS ディスク ドライブ（ESXi を実行）[6] またはディスクレス ブレード • FC SAN ストレージ上に格納される Cisco Unified Communications 仮想マシン • ベア メタル サポートなし[7]
	Unified Computing System（UCS）C シリーズ ラックマウント サーバ	Cisco UCS C200 シリーズ[5]	• 複数のプロセッサ • 1 つまたは複数の電源装置 • 複数の SAS ローカル ディスク ドライブ • ベア メタル サポートなし[7]
		Cisco UCS C210 シリーズ[5]	• 複数のプロセッサ • 1 つまたは複数の電源装置 • 複数の SAS ローカル ディスク ドライブ（ESXi のみを実行、ESXi および Unified Communications 仮想マシンを実行、またはディスクレス ブレード） • ベア メタル サポートなし[7]

1. これは、サポートされる Cisco IOS プラットフォームの詳細なリストではありません。
2. UCS C200 ラックマウント サーバは複数の電源装置をサポートしますが、Unified CMBE 6000 構成は、単一電源装置のみをサポートします。
3. Cisco MCS 7828 は Unified CMBE（BE 5000）のみをサポートします。
4. Cisco MCS 7815 プラットフォームの IP インターフェイスは 1 つだけです。

5. または仕様ベース ハードウェアと同等のサーバ。「仮想配置用の Cisco ハードウェア」（P.8-7）を参照してください。
6. UCS B シリーズ ブレード サーバのディスクは、仮想マシン ソフトウェア（ESXi）専用です。Unified CM などのアプリケーションはインストールされず、ブレード上のドライブで実行されません。
7. UCS B シリーズおよび C シリーズ サーバは、Cisco Unified Communications アプリケーションにベア メタル サポートを提供しません。UCS B シリーズおよび C シリーズ サーバは、ESXi ハイパーバイザ ソフトウェアを実行する必要があります。

サポートされている MCS サーバまたは同等品の全リストについては、次の Web サイトで入手可能な資料を参照してください。

http://www.cisco.com/go/swonly

必要な規模、パフォーマンス、および冗長性に応じて、特定の配置に適したコール処理タイプとプラットフォームを決定します。一般に、Unified CM およびハイエンドな MCS サーバや UCS サーバではキャパシティと可用性は向上し、Unified CME と Unified CMBE ではキャパシティと冗長性のレベルは低下します。冗長性とスケーラビリティの詳細については、「コール処理のハイ アベイラビリティ」（P.8-14）および「コール処理のキャパシティ プランニング」（P.8-25）を参照してください。

仮想配置用の Cisco ハードウェア

Unified CM は、Tested Reference Configuration（TRC）と呼ばれる選択されたハードウェア設定でテストされます。TRC では、「フル搭載」の Unified Communications 仮想マシンを実行して、特定の保証性能、キャパシティ、およびアプリケーション共存のシナリオについてテストが実行され、文書化されています。TRC は、特定の配置シナリオ用に事前に作成されたシスコのパッケージ ソリューションをご希望のお客様、またはハードウェア仮想化の十分な経験のないお客様（または両方）を対象としています。TRC は、上記の Cisco UCS B シリーズおよび C シリーズに基づいています。

あるいは、仕様ベースのハードウェア サポートでは、より柔軟なハードウェア設定（たとえばその他の UCS プラットフォームや iSCSI、FCoE、NAS（NFS）ストレージ システムのサポートを追加すること）が可能です。仕様ベースのハードウェア サポートは、仮想化およびサーバとストレージのサイジングに関する深い専門知識を持っており、独自のハードウェア標準の使用を希望するお客様を対象としています。

サポートされているハードウェア設定の詳細については、次の Web サイトで入手可能な資料を参照してください。

http://www.cisco.com/go/uc-virtualized

Unified CM クラスタのサービス

MCS-7815 または MCS-7816 で実行される Cisco Unified CME、Cisco Unified CMBE 3000 および 5000、および Unified CM は、スタンドアロンの呼処理アプリケーションまたはエンティティです。ただし、それ以外のすべてのサーバ プラットフォームで実行される Unified CM には、クラスタリングの概念があります。Unified CM アーキテクチャでは、複数の物理サーバを 1 つのコール処理エンティティまたは IP PBX システムとして連携させることができます。このサーバ グループを *クラスタ*と呼びます。Unified CM サーバのクラスタは、設計上の制限事項を遵守している限り、IP ネットワークを介して分散していてもかまいません。クラスタを使用することで、空間的な冗長性、およびそれに伴う復元性を Unified Communications システムの設計にもたらすことができます。

Unified CM クラスタの内部には、それぞれ固有のサービスを提供する複数のサーバが存在します。これらの各サービスは、同じ物理サーバ上で他のサービスと共存できます。たとえば、小規模なシステムでは、データベース サービス、コール処理サービス、およびメディア リソース サービスを単一のサーバで提供できます。クラスタの規模とパフォーマンスを強化する必要が高まった場合は、これらのサービスの多くを専用物理サーバに移行する必要があります。

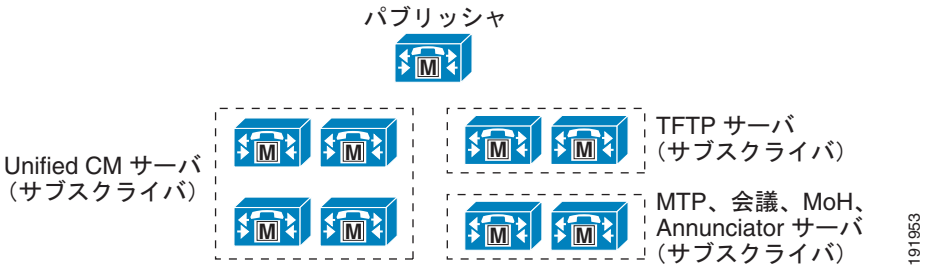
（注）　クラスタ内のすべてのサーバに対して同じサーバ モデルを使用することを推奨しますが、個別のハードウェア バージョンがすべてサポートされており、すべてのサーバで同じバージョンの Unified CM が実行されている場合、クラスタ内にサーバ モデルを混在させることもサポートされます。ただし、クラスタ内のさまざまなサーバ モデル間でのキャパシティの相違を考慮する必要があります。クラスタの全体的なキャパシティは、最終的にはクラスタ内の最小のサーバのキャパシティによって決まる場合があるためです。クラスタ内のすべてのサーバが同じモデル タイプの場合、異なるベンダーのサーバをクラスタ内に混在させることもサポートされ、キャパシティに悪影響はありません。コール処理キャパシティの詳細については、「コール処理のキャパシティ プランニング」（P.8-25）の項を参照してください。

次の項では、Unified CM クラスタを形成しているサーバが実行する各種の機能について説明し、必要な規模、パフォーマンス、および復元性を達成するようにサーバを配置する方法について、ガイドラインを示します。

クラスタ サーバ ノード

図 8-1 に、複数のサーバ ノードで構成された一般的な Unified CM クラスタを示します。

図 8-1　　一般的な Unified CM クラスタ



パブリッシャ

パブリッシャはすべてのクラスタに必要なサーバであり、図 8-1 に示すように、クラスタごとに 1 つのパブリッシャだけを配置できます。このサーバは、最初にインストールする必要があります。クラスタ内の他のすべてのサブスクライバに対して、データベース サービスを提供します。パブリッシャ サーバは、コンフィギュレーション データベースに完全な読み取りと書き込みのアクセスができる唯一のサーバです。

1,250 ユーザを超える大規模なシステムの場合には、管理操作によるテレフォニー サービスへの影響を防止するために、専用パブリッシャを推奨します。専用パブリッシャのサーバ上で、コール処理または TFTP サービスが提供されることはありません。代わりに、これらのサービスはクラスタ内の他のサブスクライバ サーバによって提供されます。

パブリッシャ用のハードウェア プラットフォームは、クラスタで必要な規模とパフォーマンスを基準として選択する必要があります。パブリッシャは、コール処理サブスクライバと同等のサーバ パフォーマンスを持つものにすることを推奨します。可能な場合には、パブリッシャをハイ アベイラビリティサーバにして、ハードウェアの障害による影響を最小限に抑えるようにします。

サブスクライバ

Unified CM ソフトウェアのインストール時に、パブリッシャとサブスクライバという 2 つのタイプのサーバを定義できます。これらの用語は、データベース間の関係をインストール時に定義するために使用されています。ソフトウェアを初期インストールしたときに使用可能になるのは、データベース サービスとネットワーク サービスだけです。すべてのサブスクライバ ノードは、パブリッシャにサブスクライブして、データベース情報のコピーを取得します。ただし、Unified CM クラスタの初期化時間を短縮するために、クラスタ内のすべてのサブスクライバ サーバは、初期化時にデータベースのローカル コピーを使用しようとします。これにより、Unified CM クラスタの全体的な初期化時間は短縮されます。すべてのサブスクライバ ノードは、パブリッシャまたは他のサブスクライバ ノードからの変更通知によって、データベースのローカル コピーを更新された状態に保ちます。

図 8-1 に示すように、複数のサブスクライバ ノードが同じクラスタのメンバーになることができます。サブスクライバ ノードには、Unified CM コール処理サブスクライバ ノード、TFTP サブスクライバ ノード、および会議や Music on Hold（MoH; 保留音）などの機能を提供するメディア リソース サブスクライバ ノードがあります。

コール処理サブスクライバ

コール処理サブスクライバは、Cisco CallManager サービスが使用可能になっているサーバです。このサービスが使用可能になった時点で、このサーバはコール処理機能を実行できるようになります。電話、ゲートウェイ、メディア リソースなどのデバイスが登録やコール発信を実行できるのは、このサービスが使用可能になっているサーバに対してのみです。図 8-1 に示すように、複数のコール処理サブスクライバが同じクラスタのメンバーになることができます。実際、Unified CM は、クラスタごとに最大 8 つのコール処理サブスクライバ ノードをサポートします。

クラスタ内の各コール処理サブスクライバ ノードには、そのサブスクライバ ノード上で Cisco CallManager サービスを使用可能にするために、固有のサーバ ライセンスが必要です。パブリッシャが使用不可になっていると、サーバ上で Cisco CallManager サービスを使用可能にできません。パブリッシャはライセンス サーバとして機能し、Cisco CallManager サービスをアクティブにするために必要なライセンスを配布するからです。

TFTP サブスクライバ

TFTP サブスクライバまたはサーバ ノードは、Unified CM クラスタの一部として、次の 2 つの主要な機能を実行します。

- サービスのためのファイルの提供。電話やゲートウェイなどのデバイスのコンフィギュレーション ファイル、電話および一部のゲートウェイのアップグレード用バイナリ ファイル、さまざまなセキュリティ ファイルなど。
- コンフィギュレーション ファイルおよびセキュリティ ファイルの生成。通常は署名済みであり、ダウンロード用として提供する前に暗号化されることもあります。

この機能を提供する Cisco TFTP サービスは、クラスタ内の任意のサーバで使用可能にできます。ただし、何らかの設定を変更すると、TFTP サービスがコンフィギュレーション ファイルを再生成するため、1,250 ユーザを超えるクラスタでは、他のサービスが影響を受ける場合があります。このため、1,250 ユーザを超えるクラスタまたは頻繁な設定変更を伴う機能を備えたクラスタでは、図 8-1 に示すように、特定のサブスクライバ ノードを TFTP サービス専用にすることを推奨します。

TFTP サブスクライバのハードウェア プラットフォームには、コール処理サブスクライバと同じものを使用することを推奨します。

メディア リソース サブスクライバ

メディア リソース サブスクライバまたはサーバ ノードは、会議や保留音などのメディア サービスをエンドポイントとゲートウェイに提供します。これらのタイプのメディア リソース サービスは、Cisco IP Voice Media Streaming Application サービスによって提供されます。このサービスは、クラスタ内の任意のサーバ ノードで使用可能にできます。

メディア リソースには、次のものがあります。

- Music On Hold（MoH; 保留音）：保留状態になっているデバイス、会議に転送または追加されるデバイスに対して、マルチキャストまたはユニキャストの保留音を提供できます（「保留音」（P.17-26）を参照）。
- Annunciator サービス：電話番号を間違えていることや、コール ルーティングが使用不可になっていることを伝える場合に、トーンの代わりに音声アナウンスを流します（「Annunciator」（P.17-24）を参照）。
- カンファレンス ブリッジ：Ad Hoc 会議と Meet-Me 会議のための、ソフトウェア ベースの会議を提供します（「会議」（P.17-7）を参照）。
- Media Termination Point（MTP; メディア ターミネーション ポイント）サービス：H.323 クライアント、H.323 トランク、および Session Initiation Protocol（SIP）エンドポイントおよびトランク用の機能を提供します（「メディア ターミネーション ポイント（MTP）」（P.17-16）を参照）。

クラスタ内でメディア リソースを実行する場合は、メディア リソース サービスの処理とネットワークに関する要件が追加される場合に備えて、すべてのガイドラインに準拠することが重要です。一般に、マルチキャスト MoH と Annunciator サービスには専用のメディア リソース サブスクライバを使用せず、ユニキャスト MoH およびソフトウェア ベースの大規模な会議と MTP に、図 8-1 に示すような専用のメディア リソース サブスクライバを使用することを推奨します（これらのサービスが、「メディア リソース」（P.17-1）、の章で説明している設計ガイドラインの範囲内にない場合は除きます）。

その他のクラスタ サービス

Unified CM クラスタ内の特定のタイプのサブスクライバ ノード以外に、Unified CM コール処理サブスクライバ ノードで実行できるその他のサービスもあり、追加機能を提供して使用可能にできます。

Computer Telephony Integration（CTI）Manager

CTI Manager サービスは、Cisco CallManager サービスと TAPI または JTAPI 統合アプリケーションの仲介者として機能します。このサービスは、CTI を利用するアプリケーションのクラスタで必要です。CTI Manager サービスは、CTI アプリケーションの認証を提供し、アプリケーションがエンドポイントの回線をモニタおよび制御できるようにします。CTI Manager は、コール処理サブスクライバ上だけで使用可能にできます。したがって、クラスタ内では最大で 8 つのノードで CTI Manager サービスを実行できます。

CTI Manager の詳細については、「コンピュータ テレフォニー インテグレーション（CTI）」（P.8-37）を参照してください。

Unified CM のアプリケーション

Unified CM 上では、Cisco Unified CM Assistant、エクステンション モビリティ、Web Dialer などのさまざまなタイプのアプリケーション サービスを使用可能にできます。これらのアプリケーションに関する設計ガイドラインの詳細については、「Cisco Unified CM アプリケーション」（P.19-1）の章を参照してください。

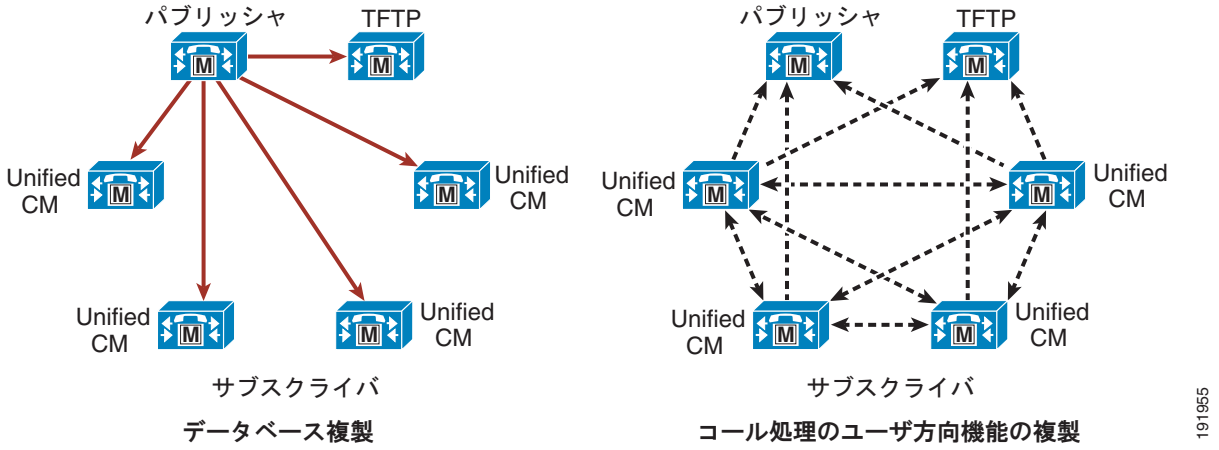
クラスタ内通信

クラスタ内通信（Unified CM クラスタ内の通信）には、2 種類あります（図 8-2 および図 8-3 を参照）。1 つは、すべてのデバイス設定情報を含んでいるデータベースを配布するためのメカニズムです（図 8-2 の「データベース複製」を参照）。コンフィギュレーション データベースは、パブリッシャ サーバに保存され、コピーがクラスタのサブスクライバ ノードに複製されます。データベースの変更のほとんどはパブリッシャで加えられ、サブスクライバ データベースに伝達されます。そのため、クラスタのメンバー全体で設定の一貫性が確保され、データベースの空間的な冗長性が容易になります。

ユーザ方向のコール処理機能に対するデータベースの変更は、エンド ユーザ デバイスが登録されるサブスクライバ サーバで行われます。次にサブスクライバ サーバが、これらのデータベース変更をクラスタにある他のすべてのサーバに複製し、ユーザ方向機能に冗長性を提供します（図 8-2 の「コール処理のユーザ方向機能の複製」を参照）。これらの機能には、次のものがあります。

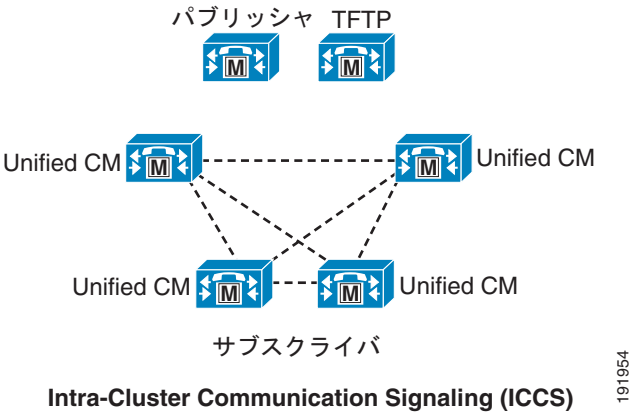
- Call Forward All（CFA）
- Message Waiting indicator（MWI; メッセージ待機インジケータ）
- プライバシーの有効 / 無効
- エクステンション モビリティのログイン / ログアウト
- ハント グループのログイン / ログアウト
- デバイス モビリティ
- エンド ユーザおよびアプリケーション ユーザの Certificate Authority Proxy Function（CAPF）ステータス
- クレデンシャルのハッキングと認証

図 8-2　データベースおよびユーザ方向機能の複製



Intra-Cluster Communication Signaling（ICCS）と呼ばれる、もう 1 つのクラスタ内通信は、デバイスの登録、ロケーションの帯域幅、共有メディア リソースなどのランタイム データの伝搬と複製です（図 8-3 を参照）。この情報は、Cisco CallManager サービス（コール処理サブスクライバ）を実行している、クラスタのすべてのメンバー全体で共有されます。クラスタのメンバーと関連ゲートウェイとの間で、コールの最適なルーティングが確保されます。

図 8-3　Intra-Cluster Communication Signaling（ICCS）

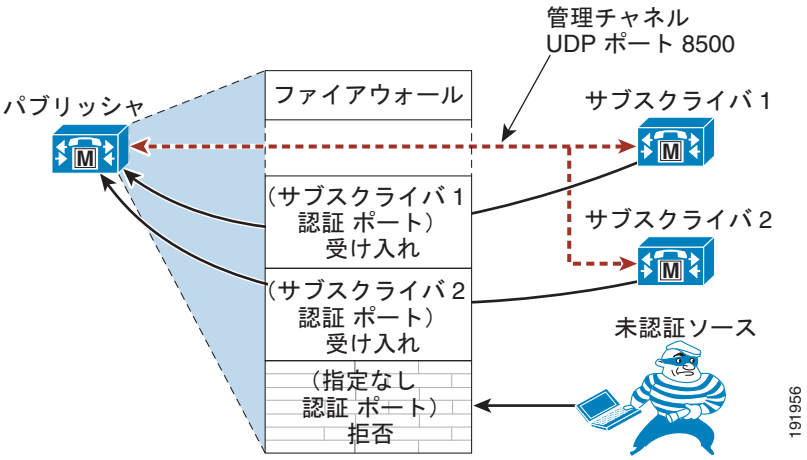


Intra-Cluster Communication Signaling (ICCS)

クラスタ内セキュリティ

Unified CM クラスタ内の各サーバが内部で動的ファイアウォールを実行します。Unified CM のアプリケーション ポートは、送信元 IP フィルタリングによって保護されます。動的ファイアウォールは、認証済みサーバまたは信頼できるサーバに対してだけ、これらのアプリケーション ポートを開きます（図 8-4 を参照）。

図 8-4　クラスタ内セキュリティ



このセキュリティ メカニズムは、単一の Unified CM クラスタ内のサーバ ノード間だけに適用できます。Unified CM のサブスクライバは、パブリッシャのデータベースにアクセスする前に、クラスタ内で認証されます。クラスタ内通信およびデータベース複製は、認証済みサーバ間だけで発生します。インストール時にサブスクライバ ノードは、事前共有キー認証メカニズムでパブリッシャに対して認証されます。認証プロセスに必要な手順は次のとおりです。

1. セキュリティ パスワードを使用してパブリッシャ サーバをインストールします。
2. Unified CM Administration を使用することによって、パブリッシャ上にサブスクライバ サーバを設定します。
3. パブリッシャ サーバのインストール時に使用されたのと同じセキュリティ パスワードを使用して、サブスクライバ サーバをインストールします。

4. サブスクライバのインストール後、サーバは、UDP 8500 を使用する管理チャネル上でパブリッシャとの接続を確立しようとします。サブスクライバは、ホスト名、IP アドレスなどのすべてのクレデンシャルをパブリッシャに送信します。クレデンシャルは、インストール時に使用されたセキュリティ パスワードを使用して認証されます。
5. パブリッシャは、独自のセキュリティ パスワードを使用してサブスクライバのクレデンシャルを確認します。
6. その情報が有効な場合、パブリッシャは、自身の動的ファイアウォール テーブルに、信頼できる送信元としてサブスクライバを追加します。サブスクライバは、データベースへのアクセスを許可されます。
7. サブスクライバは、パブリッシャから他のサブスクライバ サーバのリストを取得します。すべてのサブスクライバが互いに管理チャネルを確立し、メッシュ トポロジが作成されます。

音声アクティビティ検出

Unified CM クラスタ内で Voice Activity Detection（VAD; 音声アクティビティ検出）を使用不可にしておくことを推奨します。デフォルトでは、Unified CM サービス パラメータで VAD は使用不可になっています。Cisco IOS ゲートウェイで設定されている H.323 および SIP ダイヤル ピア上で使用不可にするには、**no vad** コマンドを使用してください。

クラスタリングに関する一般的なガイドライン

すべての Unified CM クラスタに次のガイドラインが適用されます。

（注）　1 つのクラスタに複数のサーバ プラットフォームを組み合せることができますが、クラスタ内のすべてのサーバでは、同じ Unified CM ソフトウェア リリースを実行する必要があります。

- 通常の環境では、同一 LAN または MAN 内にクラスタのすべてのメンバーを入れます。
- クラスタが IP WAN にわたって構築されている場合、「IP WAN を介したクラスタリング」（P.5-46）の項を参照して、IP WAN を介したクラスタリングのガイドラインに従ってください。
- Unified CM クラスタに、20 のサーバを組み込めるようになりました。20 のサーバのうち、コール処理サブスクライバ（Cisco CallManager サービスを実行するノード）は最大で 8 つです。クラスタ内の残りのサーバ ノードは、専用データベース パブリッシャ、専用 TFTP サブスクライバ、またはメディア リソース サブスクライバとして設定できます。
- Cisco MCS 7815、MCS 7816、または同等のサーバで Unified CM を配置するときは、配置内には最大 2 台のサーバという制限があります。1 台をパブリッシャ、TFTP、およびバックアップ呼処理サブスクライバ ノードにし、もう 1 台をプライマリ呼処理サブスクライバにします。Cisco MCS 7816 または同等のサーバでは、この構成で最大 500 台の電話機がサポートされます。
- キャパシティの大きいサーバを使用して 2 サーバ クラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることを推奨します。1,250 ユーザを超える場合は、専用パブリッシャと別個のサーバをプライマリおよびバックアップのコール処理サブスクライバ用に推奨します。
- Unified CMBE 3000 8.5(1) は MCS 7816 サーバ プラットフォームで実行されますが、Unified CMBE 3000 8.6(1) 以降のバージョンは、MCS 7816 または MCS 7890-C1 専用アプライアンスで実行されます。いずれの場合も、Unified CMBE 3000 は Unified CM の単一のインスタンス（パブリッシャとシングル サブスクライバの複合インスタンス）を提供します。セカンダリ サブスクライバ インスタンスは設定できません。

- Unified CMBE 5000 は、単一のハードウェア プラットフォーム（MCS 7828）上で動作し、Unified CM の単一のインスタンス（パブリッシャとシングル サブスクライバの複合インスタンス）を提供します。セカンダリ サブスクライバ インスタンスは設定できません。
- Unified CMBE 6000 は、UCS C200 ラックマウント サーバ上で動作し、Unified CM の単一のインスタンス（パブリッシャとシングル サブスクライバの複合インスタンス）を提供します。増設の UCS C200 サーバは、Unified CMBE コール処理のほか、その他の共存するアプリケーションに対して、サブスクライバの冗長性を提供するためにアクティブ/スタンバイ方式またはロード バランシング方式で配置できます。負荷を 2 つの UCS C200 サーバ間で分散できるよう、ロード バランシングを使用する冗長サーバを配置することを推奨します。また、MCS サーバを使用して、アクティブ/スタンバイ方式またはロード バランシング方式で Unified CM サブスクライバの冗長性を提供できます。
- Cisco UCS B シリーズまたは C シリーズ サーバで Unified CM を展開するときは、MCS サーバのクラスタの場合のように、各 Unified CM ノード インスタンスは、パブリッシャ ノード、コール処理サブスクライバ ノード、TFTP サブスクライバ ノード、またはメディア リソース サブスクライバ ノードのいずれかになります。Unified CM クラスタと同様に、クラスタごとに 1 つのパブリッシャ ノードだけがサポートされます。
- Cisco UCS B シリーズ ブレード サーバおよび C シリーズ ラックマウント サーバは、DB9 シリアル ポート、Video Graphics Array（VGA）モニタ ポート、および 2 つの Universal Serial Bus（USB）ポートを提供するローカルの Keyboard, Video, and Mouse（KVM; キーボード、ビデオ、およびマウス）ケーブル接続をサポートしますが、Unified CM VMware 仮想アプリケーションはこれらの USB ポートおよびシリアル ポートにアクセスできません。そのため、オーディオ カード（MOH-USB-AUDIO=）、シリアル/USB コネクタ（USB-SERIAL-CA=）、またはフラッシュ ドライブなどの USB デバイスは、これらのサーバに接続できません。代わりに、次のオプションを利用できます。
  - MoH ライブ オーディオ ソース フィードの場合は、ライブ オーディオ ソース接続に Cisco IOS ベースのマルチキャスト MoH を使用するか、または MCS サーバに Unified CM クラスタの一部として 1 台の Unified CM サブスクライバ ノード配置して、USB MoH オーディオ カード（MOH-USB-AUDIO=）を接続できるようにすることを検討します。
  - SMDI シリアル接続の場合は、MCS サーバに Unified CM クラスタの一部として 1 台の Unified CM サブスクライバ ノードを配置して、USB シリアル接続に使用します。
  - システムのインストール ログの保存には、仮想フロッピー ソフトメディアを使用します。

コール処理のハイ アベイラビリティ

コール処理サービスは、可用性が高くなるように Unified Communications システム内に配置して、1 つのコール処理コンポーネントの障害によってすべてのコール処理サービスが使用不可にならないようにする必要があります。

ハードウェア プラットフォームのハイ アベイラビリティ

コール処理のプラットフォームは、特定の配置のサイズとスケーラビリティだけでなく、プラットフォーム ハードウェアの冗長性にも基づいて選択する必要があります。

たとえば、可用性の高い配置のために、複数のプロセッサと複数のハードディスク ドライブを備えたプラットフォームを選択する必要があります。このことが重要なのは大規模な配置だけでなく、個別のコンポーネントの障害によって機能またはサービスが失われないようにするためにハイ アベイラビリティを必要とする配置にとっても重要です。

さらに、可能な場合は二重化電源を備えたプラットフォームを選択して、1 つの電源の障害によってプラットフォームが失われないようにします。二重化電源をサポートするプラットフォームを調べるには、表 8-2 を参照してください。二重化電源を備えたプラットフォームを 2 つの異なる電力源に接続して、1 つの電源回路が故障しただけでプラットフォーム全体に障害が発生することを回避します。二重化電源の使用と Uninterruptible Power Supply（UPS; 無停電電源装置）の使用を組み合せると、電力の可用性は最大になります。二重化電源プラットフォームを実現できない配置でも、建物の電力が必要なレベルの電力の可用性を備えていない状況では、UPS の使用を推奨します。

ネットワーク接続のハイ アベイラビリティ

IP ネットワークへの接続性も、最大限のパフォーマンスとハイ アベイラビリティにとって重要な考慮事項です。コール処理プラットフォームを可能な最高速度でネットワークに接続し、最大のスループットを確保します。通常は、プラットフォームに応じて 1000 Mbps または 100 Mbps 全二重です。小規模な配置で 1000 または 100 Mbps のネットワーク アクセスが使用可能でない場合、10 Mbps 全二重を使用してください。可能な場合は常に、全二重を使用してプラットフォームをネットワークに接続してください。全二重接続は、ネットワーク スイッチ ポートおよびプラットフォーム インターフェイス ポートの設定で 10 Mbps と 100 Mbps が可能です。1000 Mbps の場合は、プラットフォーム インターフェイス ポートおよびネットワーク スイッチ ポートの両方で、速度とデュプレックス モードの設定に Auto/Auto を使用することを推奨します。

（注）　プラットフォーム インターフェイス ポートまたはネットワーク スイッチ ポートのいずれか一方が Auto モードのままであり、もう一方のポートが手動で設定される場合、ミスマッチが生じます。ベスト プラクティスは、プラットフォーム ポートとネットワーク スイッチ ポートの両方を手動で設定することです。ただし、ギガビット イーサネット ポートの場合は、Auto/Auto に設定する必要があります。

IP ネットワーク接続の速度とデュプレックス モード以外に、このネットワーク接続の復元性も同じように重要です。ユニファイド コミュニケーションの配置は、実際の冗長性に関して、基盤となるネットワーク接続に大きく依存します。このため、復元性が高い方法で基盤となるネットワーク インフラストラクチャを配置および設定することが重要です。可用性の高いネットワーク インフラストラクチャの設計の詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。すべての場合で、インフラストラクチャ内でスイッチまたはルータの障害が発生しても、ほとんどのユーザは配置内で提供されているほとんどのサービスにアクセスできるように、ネットワークを設計する必要があります。

コール処理の可用性を最大にするには、可能な場合はコール処理プラットフォームを別々の建物および別々のネットワーク スイッチに置いて接続し、建物またはネットワーク インフラストラクチャ スイッチの障害が発生したときのコール処理への影響を最小にします。Unified CM コール処理では、このことは、可能な場合は常に、クラスタ サーバ ノードを LAN または MAN 配置内の複数の建物またはロケーション間で分散させることを意味します。最低限でも、同じロケーション内の異なる物理ネットワーク スイッチ間でネットワーク接続を物理的に分散させることを意味します。

さらに、Unified CME および Unified CMBE はスタンドアロンのコール処理エンティティですが、複数のコール処理エンティティを配置する場合、これらのコール処理タイプに物理的な分散とそれによる冗長性を提供することには意味があります。そのようなシナリオで可能な場合は常に、Unified CME または Unified CMBE の各インスタンスを LAN または MAN 配置内の異なる物理ロケーションにインストールするか、または最低限でも異なるネットワーク スイッチに物理的に接続します。

可用性の高いネットワーク インフラストラクチャを配置し、コール処理プラットフォームをネットワーク コンポーネントおよびロケーション間で物理的に分散させる以外に、各コール処理エンティティからネットワークへの可用性の高い物理接続を設定することも推奨します。可能な場合は常に、1 つのアップストリーム ハードウェア ポートまたはスイッチの障害によってプラットフォームのネットワーク接続が失われないように、2 つのネットワーク接続を使用してプラットフォームを 2 つの物理的

に別々のネットワーク スイッチ上の 2 つの異なるポートに接続します。Unified CME ルータ プラットフォームには複数の物理ネットワーク インターフェイスを設定でき、ネットワークに二重接続できます。同様に、Unified CM および Unified CMBE 5000 コール処理タイプの MCS サーバ プラットフォームも、Network Interface Card（NIC; ネットワーク インターフェイス カード）チーミングを使用して、ネットワークに二重接続できます。

ネットワークの耐障害性に対応する NIC チーミング

NIC チーミング機能は、Cisco MCS（あるいは HP または IBM の同等のサーバ）を 2 枚の NIC、つまり 2 本の物理ケーブルで IP ネットワークに接続できるようにするものです。NIC チーミングは、障害の発生したポートから正常なポートに作業負荷を転送することによって、ネットワークのダウンタイムを防止します。NIC チーミングは、ロード バランシングまたはインターフェイス速度向上用には使用できません。NIC チーミングは、デュアル NIC の Cisco MCS プラットフォーム（あるいは HP または IBM の同等のプラットフォーム）でサポートされます。

（注）　MCS 7815 プラットフォーム（あるいは HP または IBM の同等のプラットフォーム）のネットワーク インターフェイス ポートは 1 つだけのため、NIC チーミングを実行できません。

UCS ネットワークの耐障害性

Cisco UCS B シリーズ ブレード サーバは、UCS ネットワーク接続インフラストラクチャおよび基盤となるネットワーク接続された Storage Area Network（SAN; ストレージ エリア ネットワーク）を利用します。このバックエンドの UCS ネットワーク インフラストラクチャ（冗長な並行スイッチング ファブリック エクステンダおよび相互接続と、ファイバ チャネルまたはギガビット イーサネット アップリンクを含む）は、可用性の高いネットワーク接続およびストレージをこれらのサーバに提供します。UCS ネットワークおよびストレージ インフラストラクチャの可用性の高い仮想データセンター配置の詳細については、『*Designing Secure Multi-Tenancy into Virtualized Data Centers*』（http://www.cisco.com/en/US/docs/solutions/Enterprise/Data_Center/Virtualization/securecldg.html）を参照してください。

Unified CM のハイ アベイラビリティ

基盤となる Unified CM クラスタリングメカニズムのため、Unified Communications システムには、ハードウェア プラットフォームのディスクおよび電力コンポーネントの冗長性、物理ネットワーク ロケーション、および接続の冗長性以外にも、ハイ アベイラビリティに関する考慮事項があります。ここでは、コール処理サブスクライバの冗長性の考慮事項、コール処理のロード バランシング、およびその他のクラスタ サービスの冗長性について説明します。

コール処理の冗長性

Unified CM には、次のコール処理の冗長性設定オプションまたは冗長性方式があります。

- 2:1 冗長性方式：プライマリ コール処理サブスクライバ 2 台ごとに、1 つの共用セカンダリまたはバックアップ コール処理サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ コール処理サブスクライバごとに、1 つのセカンダリまたはバックアップ コール処理サブスクライバを設置します。

これらの冗長性方式は、Unified CM クラスタ アーキテクチャ内の組み込み登録フェールオーバー メカニズムによって実施され、エンドポイントのプライマリ コール処理サブスクライバ ノードに障害が発生したときに、エンドポイントはバックアップ コール処理サブスクライバ ノードに再登録されます。

この登録フェールオーバー メカニズムは、Skinny Client Control Protocol（SCCP）IP Phone のフェールオーバー レート、毎秒約 125 台の登録を実現できます。Session Initiation Protocol（SIP）電話機の登録フェールオーバー レートでは、毎秒約 40 台の登録です。

選択したコール処理の冗長性方式によって、配置の耐障害性だけでなく、アップグレードの耐障害性も決まります。

1:1 冗長性方式では、プライマリ コール処理サブスクライバで複数の障害が発生しても、コール処理機能に影響はありません。それに対して 2:1 冗長性方式では、バックアップ コール処理サブスクライバを共用する 2 つのプライマリ コール処理サブスクライバのうちの 1 つだけで障害が発生した場合、コール処理に影響はありません。

同様に、1:1 冗長性方式では、クラスタのアップグレードは、1 つのエンドポイント登録フェールオーバー期間だけがコール処理サービスに影響するように実行できます。それに対して 2:1 冗長性方式では、クラスタのアップグレードには複数の登録フェールオーバー期間が必要です。

Unified CM クラスタは、サービスへの影響を最小限に抑えてアップグレードできます。2 つのバージョン（リリース）の Unified CM を同じサーバ上に置いて、一方をアクティブ パーティションに、もう一方を非アクティブ パーティションに入れることができます。すべてのサービスとデバイスで、すべての Unified CM 機能に対して、アクティブ パーティションの Unified CM バージョンが使用されます。アップグレード時に、クラスタ操作はアクティブ パーティションにある現在のリリースの Unified CM を使用して続行されながら、アップグレード バージョンが非アクティブ パーティションにインストールされます。アップグレード プロセスの完了後は、サーバをリブートし非アクティブ パーティションをアクティブ パーティションに切り替えて、新しいバージョンの Unified CM を実行できます。

1:1 冗長性方式では、次の手順を使用して、ダウンタイムを最小限に抑えてクラスタをアップグレードできます。

ステップ 1　新しいバージョンの Unified CM を非アクティブ パーティションにインストールします。最初にパブリッシャにインストールしてから、すべてのサブスクライバ（コール処理サブスクライバ、TFTP サブスクライバ、およびメディア リソース サブスクライバ）にインストールします。リブートはしないでください。

ステップ 2　パブリッシャをリブートして、新しいバージョンに切り替えます。

ステップ 3　TFTP サブスクライバ ノードを 1 つずつリブートして、新しいバージョンに切り替えます。

ステップ 4　専用メディア リソース サブスクライバ ノードを 1 つずつリブートして、新しいバージョンに切り替えます。

ステップ 5　バックアップ コール処理サブスクライバを 1 つずつリブートして、新しいバージョンに切り替えます。

ステップ 6　プライマリ コール処理サブスクライバを 1 つずつリブートして、新しいバージョンに切り替えます。デバイス登録は、前にアップグレードおよびリブートされたバックアップ コール処理サブスクライバにフェールオーバーします。各プライマリ コール処理サブスクライバがリブートされると、デバイスはプライマリ コール処理サブスクライバへの再登録を開始します。

このアップグレード方法では、異なるバージョンの Unified CM ソフトウェアを実行しているサブスクライバ サーバにデバイスが登録される期間（登録フェールオーバー期間を除く）がありません。

2:1 冗長性方式では、クラスタ内のサーバ数を少なくできますが、アップグレード時の登録フェールオーバーの発生頻度が多くなり、アップグレードの全体的な時間および特定のエンドポイントのコール処理サービスが使用不可になる時間が長くなります。プライマリ コール処理サブスクライバのペアごとにバックアップ コール処理サブスクライバは 1 つだけであるため、1 つのバックアップ コール処理サブスクライバのオーバーサブスクリプションを回避するために、一度にペアのうちの 1 つのプライマリ コール処理サブスクライバだけで新しいバージョンへリブートできます。その結果、各ペアの最初のプライマリ コール処理サブスクライバが新しいバージョンに切り替わった後、エンドポイント登録

をバックアップ サブスクライバから新しくアップグレードされたプライマリ サブスクライバに移動するための時間が発生し、その後で 2 番めのプライマリ サブスクライバでのエンドポイント登録をバックアップ サブスクライバに移動して新しいバージョンへリブートできるようになります。この間、2 番めのプライマリ コール処理サブスクライバのエンドポイントは、バックアップ サブスクライバへの再登録中に使用不可になるだけでなく、新しいバージョンを実行するノードに再登録されるまでは、すでにアップグレード済みの他のサブスクライバ ノード上のエンドポイントに到達することもできません。

（注）　アップグレードを行う前に、ディザスタ リカバリ フレームワークを使用して、Unified CM および Call Detail Record（CDR; コール詳細レコード）データベースを外部ネットワーク ディレクトリにバックアップすることを推奨します。このようにしておくと、アップグレードが失敗した場合のデータ損失を防止できます。

（注）　Unified CM クラスタのアップグレードでは、一部またはほとんどのデバイスから一時的に登録サービスおよびコール処理サービスが失われるため、アップグレードは前もって計画し、定期保守時に実装する必要があります。1:1 冗長性方式を選択すると、デバイスのダウンタイムおよびサービス停止を最小にできますが、それでも、一部またはすべてのユーザがコール処理サービスを使用できない時間が発生します。

Unified CM のアップグレードの詳細については、次の URL で入手可能なインストールおよびアップグレード ガイドを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_installation_guides_list.html

Survivable Remote Site Telephony（SRST）による Unified CM の冗長性

Cisco IOS SRST は、Unified CM クラスタから離れたロケーションにあるエンドポイントに、可用性の高いコール処理サービスを提供します。Unified CM クラスタリングの冗長性方式は確かに、LAN または MAN 環境内のコール処理などのアプリケーション サービスに高レベルの冗長性をもたらします。ただし、WAN などの低速リンクによって中央の Unified CM クラスタから分離されたリモート ロケーションの場合、冗長性方式として SRST を使用すると、リモート サイトと中央サイトの間でネットワーク接続が失われたときに、基本的なコール処理サービスをこれらのリモート ロケーションに提供できます。コール処理サービスが重要であり、Unified CM クラスタへの接続が失われた場合にもコール処理サービスを維持する必要がある各リモート サイトには、SRST 対応の Cisco IOS ルータを配置することを推奨します。これらのリモート ロケーションのエンドポイントは、Unified CM 内の適切な SRST リファレンスとともに設定する必要があります。Unified CM サブスクライバへの接続を使用できない場合に、コール処理サービス用にどのアドレスを使用して SRST ルータに接続するかをエンドポイントが認識するようにするためです。

Cisco IOS ルータ上の Unified CME をリモート サイトで使用して、中央の Unified CM クラスタへの接続が失われたときに SRST 拡張機能を提供することもできます。Unified CME は、ルータの通常の SRST で使用できる機能よりも多くのバックアップ コール処理機能を IP Phone に提供します。ただし、SRST として機能する Unified CME のエンドポイント キャパシティは、通常は基本的な SRST よりも低下します。

コール処理サブスクライバの冗長性

選択した冗長性方式に応じて（「コール処理の冗長性」（P.8-16）を参照）、コール処理サブスクライバは、プライマリ（アクティブ）サブスクライバまたはバックアップ（スタンバイ）サブスクライバのどちらかになります。ロード バランシングを実装する場合は、サブスクライバがプライマリ サブスクライバとバックアップ サブスクライバの両方を兼ねることもあります。クラスタの設計を計画するときは、通常はコール処理サブスクライバにこの機能を割り当てます。大規模なクラスタや高性能クラスタでは、コール処理サービスをパブリッシャおよび TFTP サブスクライバ ノード上で使用可能にしない

でください。1:1 冗長性方式は、プライマリ サブスクライバとバックアップ サブスクライバの専用ペアを使用します。2:1 冗長性方式は、1 つのバックアップ サブスクライバを共用するプライマリ サブスクライバのペアを使用します。

次の図では、Unified CM でコール処理の冗長性を実現するための一般的なクラスタ構成を示しています。

図 8-5　　基本的な冗長性方式

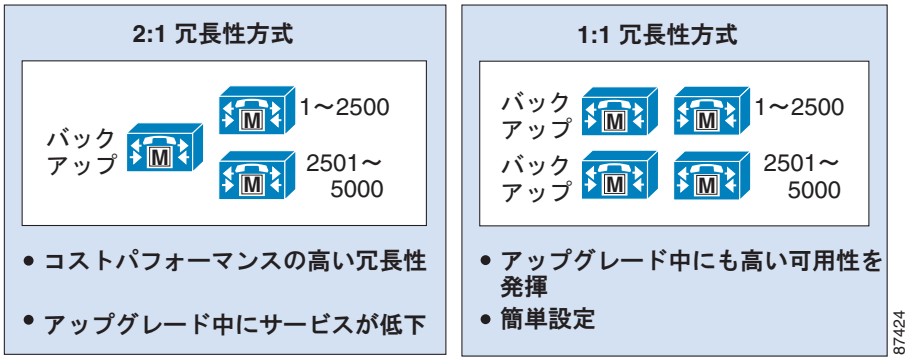


図 8-5 では、利用できる 2 つの基本的な冗長性方式を示しています。どちらの場合でも、バックアップ サーバは、障害の発生するプライマリ コール処理サーバ 1 台分以上の処理能力を備えている必要があります。2：1 冗長性方式の場合、バックアップ サーバは、個々の配置の要件に応じて、障害の発生するコール処理サーバ 1 台分、または両方のプライマリ コール処理サーバに相当する処理能力を備えている必要があります。サーバのキャパシティの選定およびハードウェア プラットフォームの選択については、「コール処理のキャパシティ プランニング」（P.8-25）の項を参照してください。

（注） 7,500 台以上の IP Phone が 2 つのプライマリ サブスクライバに登録される場合は、1:1 冗長性を使用する必要があります。これは、1 つのバックアップ サブスクライバで 7,500 台以上のバックアップ登録はできないからです。

図 8-6　1：1 冗長構成のオプション

図 8-7　2：1 冗長構成のオプション

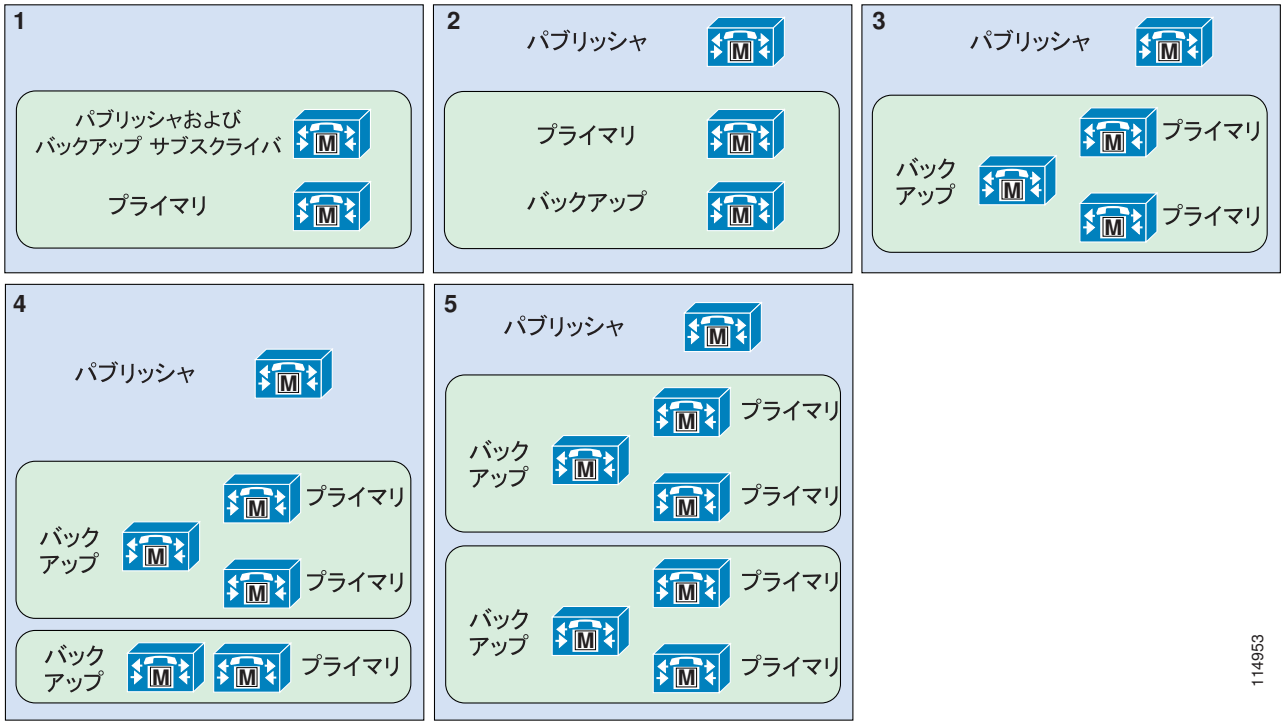


図 8-6 に示した 5 つは、すべて 1 : 1 冗長性のオプションを示しています。図 8-7 に示した 5 つは、すべて 2 : 1 冗長性のオプションを示しています。どちらの場合も、オプション 1 は 1,250 人未満のユーザをサポートするクラスタに使用します。オプション 2 ～ 5 は、それぞれの冗長性方式でクラスタを徐々に拡張した様子を示しています。正確な規模は、選択したハードウェア プラットフォームや必要なハードウェア プラットフォームによって異なります。

これらの図では、パブリッシャとコール処理サブスクライバだけを示していることに注意してください。TFTP やメディア リソースなどの他のサブスクライバ ノードは示していません。

（注）　Unified CM グループあたり最大 3 つのコール処理サブスクライバを定義できます。追加のバックアップ用に 3 次サブスクライバを追加すると、上記の冗長性方式は 2:1:1 または 1:1:1 冗長性に拡張されます。ただし、WAN を介したクラスタリングでの配置（「リモート フェールオーバー配置モデル」（P.5-57）を参照）で 3 次サブスクライバ サーバを使用する場合を除き、リモート サイトに設置するエンドポイント デバイスには 3 次サブスクライバの冗長性は推奨しません。エンドポイントが 3 次サブスクライバへの接続性をチェックする必要があると、SRST へのフェールオーバーがさらに遅延するためです。

図 8-6 または図 8-7 では示していませんが、MCS 7825 以上のサーバを備えたシングル サーバ クラスタを配置することもできます。MCS 7825 または同等のサーバでは、シングル サーバ クラスタのエンドポイント設定および登録の制限は 500 です。これより可用性の高いサーバを使用する場合も、シングル サーバ クラスタのエンドポイント設定および登録が 1,000 を超えないようにする必要があります。シングル サーバ構成では、バックアップ コール処理サブスクライバがないため、クラスタの冗長性メカニズムはありません。このようなタイプの配置では、冗長性メカニズムとして Survivable Remote Site Telephony（SRST）を使用して、Unified CM が使用できない際に最低限のコール処理サービスを提供する必要があります。ただし、シスコでは、実稼動環境でシングル サーバ配置を採用することは推奨しません。

ロード バランシング

1:1 冗長性方式の Unified CM クラスタでは、プライマリ コール処理サブスクライバとバックアップ コール処理サブスクライバ間で、デバイス登録およびコール処理サービスをロードバランスできます。

通常、プライマリが使用可能な場合、バックアップ サーバに登録されたデバイスはありません。このことにより、所定の時間にコール処理の負荷を処理するプライマリ コール処理サブスクライバ ノードは最大で 4 つであるため、配置のトラブルシューティングは容易になります。さらに、Unified CM の冗長性グループとデバイス プールの数を減らすことにより、構成が簡素化される可能性もあります。

ロードバランスされた配置では、Unified CM の冗長性グループとデバイス プールの設定値を使用して、デバイス登録とコール処理にかかる負荷の半分までをプライマリ サブスクライバからセカンダリ サブスクライバに移すことができます。この方法で、各プライマリおよびバックアップ コール処理サブスクライバ ペアは、このコール処理サブスクライバ ペアによってサービスを提供される全デバイスの半数に、デバイス登録およびコール処理サービスを提供します。これは、50/50 ロード バランシングと呼ばれます。50/50 ロード バランシング モデルには、次の利点があります。

- ロード シェアリング：登録コール処理の負荷が複数のサーバ上に分散され、応答時間をより速くできます。
- フェールオーバーとフェールバックが高速：すべてのデバイス（IP Phone、CTI ポート、ゲートウェイ、トランク、ボイスメール ポートなど）がすべてのアクティブ サブスクライバにわたって分散されるため、プライマリ サブスクライバに障害が発生した場合に、セカンダリ サブスクライバにフェールオーバーするデバイスは一部だけです。この方法で、サーバが使用不能になる影響を 50% 減らすことができます。

50/50 ロード バランシングを計画するには、ロード バランシングを使用しない場合のクラスタのキャパシティを計算し、次に、デバイスおよびコールの量に基づいて、負荷をプライマリ サブスクライバとバックアップ サブスクライバに分散します。プライマリ サーバやバックアップ サーバの障害に対処できるようにするには、プライマリとバックアップのサブスクライバの合計負荷が、サブスクライバ サーバ 1 台分の負荷を超えないようにします。

（注）　50/50 ロード バランシングが設定された Unified CM クラスタのアップグレード中、バックアップ コール処理サブスクライバのアップグレードによって、そのサーバに登録されているデバイス（プライマリ サブスクライバとバックアップ サブスクライバのペアによってサービスを提供される全デバイスの半数まで）は、プライマリ コール処理サブスクライバにフェールオーバーします。

TFTP の冗長性

大規模な Unified CM クラスタには複数の専用 TFTP サブスクライバ ノードを配置して、TFTP サービスの冗長性を提供することを推奨します。通常は 2 つの TFTP サブスクライバで十分ですが、クラスタ内に 3 台以上の TFTP サーバを配置できます。ただし、そのような構成ではすべての TFTP サブスクライバ上ですべての TFTP ファイルを再構築するために時間がかかります。

1 つ以上の冗長 TFTP サブスクライバを提供する以外に、これらの冗長 TFTP ノードを利用するためのエンドポイントを設定する必要があります。DHCP を使用するかまたは静的に TFTP オプションを設定する場合、クラスタ内の両方の TFTP サブスクライバ ノードの IP アドレスを含む TFTP サブスクライバ ノード IP アドレス アレイを定義します。この方法では、2 つの異なる IP アドレス アレイで 2 つの DHCP スコープを作成することによって（または、2 つの異なる TFTP サブスクライバ ノード IP アドレスでエンドポイントを手動で設定することによって）、TFTP サブスクライバ A をプライマリ、TFTP サブスクライバ B をバックアップとして使用する半分のエンドポイント デバイスと、TFTP サブスクライバ B をプライマリ、TFTP サブスクライバ A をバックアップとして使用するもう半分のエンドポイント デバイスを割り当てることができます。1 つの TFTP サブスクライバの障害時の冗長性を提供する以外に、複数の TFTP サブスクライバにわたってエンドポイントを分散させるこの方法はロード バランシングをもたらし、1 つの TFTP サブスクライバですべての TFTP サービス負荷を処理しないようにします。

（注）　電話やゲートウェイの個々のバイナリまたはファームウェア ロードを追加する場合は、ファイルをクラスタ内の各 TFTP サブスクライバ ノードに追加する必要があります。

CTI Manager の冗長性

すべての CTI 統合アプリケーションは、CTI Manager サービスを実行しているコール処理サブスクライバ ノードと通信します。さらに、ほとんどの CTI アプリケーションには、冗長 CTI Manager サービス ノードを指定する機能があります。そのため、クラスタ内の少なくとも 2 つのコール処理サブスクライバで CTI Manager サービスをアクティブにすることを推奨します。プライマリとバックアップ両方の CTI Manager が設定されている場合、障害が発生すると、アプリケーションはバックアップ CTI Manager に切り替えて CTI サービスを受けます。

すでに説明したように、CTI Manager サービスはコール処理サブスクライバ上だけで使用可能にできます。したがって、クラスタごとに最大で 8 つの CTI Manager があります。復元性、パフォーマンス、および冗長性を最大限まで高めるには、CTI アプリケーションの負荷をクラスタ内で使用可能な CTI Manager に分散することを推奨します。

一般に、CTI アプリケーションによって制御またはモニタされるデバイスは、CTI Manager サービスに使用するものと同じサーバ ペアに関連付けることを推奨します。たとえば、Interactive Voice Response（IVR; 音声自動応答装置）アプリケーションでは 4 つの CTI ポートが必要になります。1 : 1 冗長性と 50/50 ロード バランシングを使用する場合は、これらを次のように設定します。

- 2 つの CTI ポートは、サーバ A をプライマリ コール処理サブスクライバ、サーバ B をバックアップ サブスクライバとする Unified CM 冗長性グループを持つようにします。残りの 2 つの CTI ポートは、サーバ B をプライマリ サブスクライバ、サーバ A をバックアップ サブスクライバとする Unified CM 冗長性グループを持つようにします。
- IVR アプリケーションは、サブスクライバ A 上の CTI Manager をプライマリ、サブスクライバ B をバックアップとして使用するように設定します。

上の例は、サブスクライバ A 上の CTI Manager で障害が発生した場合の冗長性を備えており、IVR コールの負荷を 2 台のサーバに分散することもできています。この方法では、Unified CM サブスクライバ ノードの障害による影響も最小限に抑えることができます。

CTI および CTI Manager の詳細については、「コンピュータ テレフォニー インテグレーション（CTI）」（P.8-37）を参照してください。

UCS コール処理の冗長性

Cisco UCS B シリーズ ブレード サーバおよび C シリーズ ラックマウント サーバへの Unified CM の配置の場合も、これまでのコール処理、TFTP、および CTI Manager の冗長性方式がすべて適用されます。C シリーズ ラックマウント サーバは MCS サーバと同じ冗長性方式で配置されますが、UCS B シリーズ ブレード サーバには、サーバ ノードの仮想性により、冗長性に関するその他の考慮事項があります。それは、複数のサーバ ブレードにわたる Unified CM サーバ ノード インスタンスのインストールと常駐です。

図 8-8 に示すように、UCS B シリーズ ブレード サーバに Unified CM を配置して最大レベルのコール処理の冗長性を確保する場合は、次のガイドラインに従ってください。

- 各プライマリ コール処理サブスクライバ ノード インスタンスは、バックアップ コール処理サブスクライバ ノード インスタンスとは異なる物理 UCS B200 ブレード上に存在する必要があります。このことにより、プライマリ コール処理ノード インスタンスを含むブレードで障害が発生しても、バックアップ コール処理サブスクライバ ノードへのアクセスをエンドポイントに提供するシステムの機能には影響しません。
- サービスの冗長性のために複数の TFTP またはメディア リソース サブスクライバ ノード インスタンスを配置する場合は、冗長サブスクライバ ノードを常に複数の UCS ブレードに分散させて、1 つのブレードの障害によってそれらのサービスが排除されないようにします。このことにより、TFTP またはメディア リソース サブスクライバを含むブレードで障害が発生しても、エンドポイントは別のブレード上に存在するサブスクライバ ノードで TFTP およびメディア リソース サービスにアクセスできます。障害のないシナリオでは、エンドポイントも冗長 TFTP およびメディア リソース サブスクライバ ノード インスタンス間で分散させて、システムをロードバランスできます。
- CTI アプリケーションを配置する場合は、CTI Manager サービスを実行するコール処理サブスクライバ ノード インスタンスを常に複数の UCS ブレードに分散させて、1 つのブレードの障害によって CTI サービスが排除されないようにします。さらに、CTI アプリケーションは、1 つのブレード上のサブスクライバ ノード インスタンスで実行されている CTI Manager サービスをプライマリ CTI Manager として使用し、別のブレード上のサブスクライバ ノードで実行されている CTI Manager サービスをバックアップ CTI Manager として使用するように設定する必要があります。

図 8-8　UCS での Unified CM サーバ ノードの分散

サーバ ノード インスタンスを複数のブレードに分散させる以外に、サーバ ノード インスタンスを複数の Cisco UCS 5100 ブレード シャーシに分散させて、冗長性とスケーラビリティを追加できます。

仮想マシンのホスト リソースの冗長性とプロビジョニングの詳細については、http://www.cisco.com/go/uc-virtualized にあるドキュメントを参照してください。

Unified CMBE のハイ アベイラビリティ

Unified CMBE のハイ アベイラビリティに関する主な考慮事項は、ネットワーク接続、電源、およびコール処理と登録の冗長性です。

表 8-2 に示すように、Unified CMBE 3000 に使用される MCS 7816 プラットフォームも、Unified CMBE 5000 に使用される MCS 7828 プラットフォームも、冗長なネットワーク接続のために 2 つの IP インターフェイスまたは NIC を搭載しています。ただし、Unified CMBE 5000 のみが、ネットワーク接続の冗長性に対応する NIC チーミングをサポートしています。MCS 7816 サーバにインストールされた Unified CMBE 3000 は、NIC チーミングをサポートしていません。Unified CMBE 3000 用の MCS 7980-C1 専用アプライアンスの IP インターフェイスは 1 つだけのため、冗長なネットワーク接続または NIC チーミングのサポートは提供していません。

Unified CMBE 3000 および CMBE 5000 はそれぞれ、それ自体の単一のスタンドアロン プラットフォーム（セカンダリ サブスクライバ インスタンスを設定できない、パブリッシャとシングル サブスクライバの複合インスタンス）に配置します。これらはノード クラスタリングをサポートしていないため、Unified CM で使用可能なコール処理の冗長性方式を利用できません。したがって、これらの配置タイプのエンドポイントで、コール処理および登録の冗長性を提供する唯一の方法は、SRST または SRST として機能する Unified CME を使用することです。ただし、Unified CMBE 5000 のみが SRST をサポートしています。Unified CMBE 3000 では、可用性の高いコール処理および登録を提供できません。

これに対して、Unified CMBE 6000 は 1 台の増設サーバを使用するノード クラスタリングをサポートしているため、冗長なコール処理サービスおよび登録サービスを提供できます。Unified CMBE 6000 は、コール処理のほか、その他のアプリケーションおよびサービスに対するハイ アベイラビリティを提供するため、別の UCS C200 ラックマウント サーバ（または MCS サーバ）とともに配置できます。

（注）　WAN を介したクラスタの展開の場合と同様に、追加の冗長性と地理的な配信、あるいはそのいずれかを提供するために、Unified CMBE 6000 の展開では 2 台を超える UCS C200 ラックマウント サーバをクラスタリングできます。ただし、クラスタ全体でユーザの合計数が 1,000 を超えることはできず、クラスタ全体で設定されたデバイスの合計数が 1,200 を超えることはできません。ユーザ数が 1,000、設定済みデバイス数が 1,200 を超えるクラスタでの UCS C200 ラックマウント サーバの展開は、通常の Unified CM クラスタと見なされます。このため、展開は、通常の Unified CM クラスタのハイ アベイラビリティ設計ガイダンスに従う必要があります（「Unified CM のハイ アベイラビリティ」（P.8-16）を参照）。

コール処理のキャパシティ プランニング

コール処理のキャパシティ プランニングは、ユニファイド コミュニケーションの配置を成功させるために重要です。コール処理サービスによって多くの機能が提供され、コール処理エンティティによって多くのタイプのデバイスに登録およびトランザクション サービスを提供できるため、特定の配置のキャパシティ要件を満たすようにコール処理インフラストラクチャとその個別のコンポーネントをサイジングすることが重要です。

IP Phone、ソフトウェア クライアント、ボイスメール ポート、CTI（TAPI または JTAPI）デバイス、ゲートウェイ、およびメディア サービスの DSP リソース（トランスコーディングや会議）は、すべてコール処理エンティティに登録されます。これらのデバイスには、登録先のコール処理プラットフォームのリソースが必要です。必要なリソースには、メモリ、プロセッサ使用、およびディスク I/O が含まれます。

コール処理プラットフォームに登録の負荷を追加する以外に、登録後、各デバイスはトランザクション（通常はコールの形態）中に追加のプラットフォーム リソースを消費します。たとえば、1 時間あたり 6 回のコールだけを行うデバイスが消費するリソースは、1 時間あたり 12 回のコールを行うデバイスより少なくなります。

Unified CME のキャパシティ プランニング

Unified CME を配置する場合、必要となるサポート対象エンドポイント数という観点で、目的に合ったキャパシティを提供する Cisco IOS ルータ プラットフォームを選択することが重要です。また、Unified CME ルータが、コール処理以外のサービス（IP ルーティング、DNS ルックアップ、Dynamic Host Configuration Protocol（DHCP）アドレス サービス、VXML スクリプトなど）を提供する場合は、プラットフォームのメモリ キャパシティも考慮する必要があります。

Unified CME は、単一の Cisco IOS プラットフォーム上で最大 450 エンドポイントをサポートできます。ただし、各ルータ プラットフォームのエンドポイントのキャパシティは、システムのサイズによって異なります。Unified CME は Cisco Unified Communications Sizing Tool ではサポートされないため、次の Web サイトで入手可能な製品データ シートに記載されているキャパシティ情報に従う必要があります。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_data_sheets_list.html

Unified CM のキャパシティ プランニング

ここでは、Unified CM のキャパシティ プランニングについて説明します。この項で示す推奨事項は、Unified Communications Sizing Tool を、デフォルトのトレース レベルと Call Detail Record（CDR; コール詳細レコード）を有効にして使用し、その結果として得た計算に基づいています。コール処理に

直接関係しない他の機能を使用不可にしたり、縮小したり、再設定したりすると、より高いレベルのパフォーマンスとキャパシティが得られる場合があります。こうした機能の利用を可能にしたり増やしたりすると、システムのコール処理機能に影響を与える可能性があり、全体的なキャパシティを低下させる場合もあります。これらの機能には、トレース、コール詳細レコード、複雑なダイヤル プラン、および Unified CM プラットフォーム上に共存するその他のサービスが含まれます。複雑なダイヤル プランには、複数のライン アピアランス、多くのパーティション、コーリング サーチ スペース、ルート パターン、変換、ルート グループ、ハント グループ、ピックアップ グループ、ルート リスト、自動転送、共存サービス、およびその他の共存アプリケーションが含まれています。こうした機能はすべて、Unified CM システム内の追加リソースを消費します。

次の手法を使用して、システム パフォーマンスを向上させることができます。

- 特定プラットフォーム用にサポートされている最大量まで、サーバに追加の保証メモリを取り付ける。MCS 7825 および MCS 7835、または同等のサーバ クラスの大規模構成では、これらのサーバの RAM を倍に増やすことを推奨します。このメモリ アップグレードが必要かどうかは、Cisco Real Time Monitoring Tool（RTMT）を使用して検証することでわかります。サーバが物理メモリを最大量近くまで使用すると、オペレーティング システムは、ディスクへのスワップを開始します。このスワッピングが発生した場合は、追加の物理メモリを取り付ける必要があることを示しています。
- 多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランを持つ Unified CM クラスタでは、Cisco CallManager サービスの初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、システム初期化タイマー（Unified CM サービス パラメータ）を変更して、設定を初期化するための時間を追加できます。システム初期化時間の詳細については、Unified CM Administration オンライン ヘルプのサービス パラメータに関する説明を参照してください。

UCS プラットフォームでの Unified CM のキャパシティ プランニング

仮想配置では、Unified CM などの Unified Communications のアプリケーションの大部分は、仮想マシンの仮想ハードウェアの設定を指定する定義済みテンプレートを使用してインストールする必要があります。これらのテンプレートは、仮想マシン テンプレートをパッケージおよび配布するオープン スタンダード ベースの方式である Open Virtualization Archive（OVA）を使用して配布されます。

これらの OVA テンプレートは、仮想 CPU の数、仮想メモリ量、ハード ドライブの数とサイズなどを定義して、アプリケーションのキャパシティを決定します。Unified CM の場合、複数の OVA テンプレートがあり、ほとんどすべてのサーバ クラスに対して、それぞれ 1 つずつ用意されています（ただし MCS 7815 または MCS 7816 に対応するテンプレートはありません）。対応する OVA テンプレートを使用した場合、VMware または Cisco UCS サーバで実行される Unified CM 仮想マシン インスタンスのキャパシティは、Cisco MCS サーバで直接実行される Unified CM ノードのキャパシティと同じになります。たとえば、7,500 のユーザまたはデバイス（または両方）をサポートする Unified CM 用の OVA テンプレートのキャパシティは、MCS 7845-H2/I2 サーバのキャパシティと同じです。

Unified CM のキャパシティ プランニング ガイドラインおよびエンドポイントの制限

Cisco Unified CM には、次のキャパシティ ガイドラインが適用されます。

- クラスタ内では、Cisco CallManager サービスを使用して最大 8 つのコール処理サブスクライバ ノードを使用可能にできます。それ以外のサーバは、パブリッシャ、TFTP サブスクライバ、メディア リソース サブスクライバなどの専用機能に使用できます。
- 各クラスタは、最大 40,000 台のセキュアまたは非セキュア SCCP または SIP 電話機（Unified CM 8.6(1) 以降のリリースを使用）の設定および登録をサポートできます。
- 各クラスタは、最大 30,000 台のセキュアまたは非セキュア SCCP または SIP 電話機（Unified CM 8.5 以前のリリースを使用）の設定および登録をサポートできます。

- MCS 7825 または MCS 7835 サーバで構成されている Unified CM クラスタには、最大 500 のロケーションを構成できます。
- MCS 7825 または MCS 7835 サーバで構成されているクラスタは、最大 600 台の H.323 デバイス（ゲートウェイ、トランク、クライアント）、デジタル MGCP デバイス、および SIP トランクをサポートできます。
- MCS 7845 サーバで構成されているクラスタは、Unified CM クラスタ上で最大 2,000 の設定済みロケーションをサポートできます（「Unified CM によるロケーションおよびリージョンのサポート」（P.8-28）を参照）。
- MCS 7845 サーバで構成されているクラスタは、最大 2100 台の H.323 デバイス（ゲートウェイ、トランク、クライアント）、デジタル MGCP デバイス、および SIP トランクをサポートできます（「Unified CM によるゲートウェイおよびトランクのサポート」（P.8-29）を参照）。
- VMware で実行されるサーバ ノード インスタンスで構成されているクラスタは、選択された OVA テンプレートに応じて、さまざまなキャパシティをサポートできます。ほとんどの Cisco MCS サーバ クラスには、MCS サーバ クラスと同じキャパシティ（電話機、ゲートウェイ、ロケーション、リージョン、CTI 接続などの数）を持つ Unified CM インスタンスを提供する、対応した OVA テンプレートが用意されています。同一のブレードまたはサーバで複数の仮想マシン インスタンスを実行できるため、ブレードまたはサーバの合計キャパシティは MCS サーバよりも大きくなる場合があります。
- Unified CM の推奨される最大トレース設定は、System Diagnostic Interface（SDI）および Signaling Distribution Layer（SDL）の両方のトレースに対して 2 MB のファイルを 2,000 本、合計でファイル 4,000 本です。プロセスごとにファイルの最大数が設定され、各プロセスに許容されるファイル数は SDL に対して 2,000 本、SDI に対して 2,000 本となります。その他すべてのコンポーネントのトレース設定は、126 MB の限度内（たとえば、それぞれ 2 MB のファイルが 63 本）で設定する必要があります。これらの値が上限として推奨されます。コール レートの高い環境での特定のトラブルシューティングでファイルの最大数を増やす必要がある場合を除き、ほとんどの環境ではデフォルト設定で十分なトレースを収集できます。

Unified CM がサポートできるエンドポイントの最大数は、サーバ プラットフォームまたは OVA テンプレートによって異なります（表 8-3 を参照）。

表 8-3　サーバ プラットフォームまたは OVA テンプレートごとの最大エンドポイント数

サーバ プラットフォームの特性	サーバまたは OVA テンプレートごとの最大エンドポイント数[1]	ハイ アベイラビリティ サーバ[2]
Cisco MCS 7845-I3 または同等 OVA[3]	10,000[4]	あり
Cisco MCS 7845（その他のサポートされているモデルすべて）または同等 OVA[3]	7,500	あり
Cisco MCS 7835（サポートされているモデルすべて）または同等 OVA[3]	2,500	あり
Cisco MCS 7825（サポートされているモデルすべて）または同等 OVA[5]	1,000	なし
Cisco MCS 7816（すべてのサポート モデル）[6]	500	なし
Cisco MCS 7815（すべてのサポート モデル）[6]	300	なし

1. ハイ アベイラビリティ サーバでないプラットフォームは、非冗長単一サーバ インストレーションで最大 500 のエンドポイントをサポートできます。ハイ アベイラビリティ サーバは、非冗長単一サーバ インストレーションで最大 1,000 のエンドポイントをサポートできます。
2. ハイ アベイラビリティ サーバは、電源装置とハードディスクの両方の冗長性をサポートします。
3. Cisco UCS C210、B200、または仕様ベースのハードウェアと同等のサーバ上のもの。
4. Cisco Unified Communications Manager 8.6(1) 以降。

5. Cisco UCS C200 または仕様ベースのハードウェアと同等のサーバ上のもの。
6. MCS 7815 サーバおよび MCS 7816 サーバは、1+1 冗長性（最大 2 サーバ）のみをサポートし、他のサーバを含むクラスタのメンバーになることはできません。

サポートされるプラットフォーム、サードパーティ プラットフォーム、個々のハードウェア設定の最新情報については、次の Web サイトにあるオンライン資料を参照してください。

http://www.cisco.com/go/swonly

Unified CM によるロケーションおよびリージョンのサポート

Cisco Unified CM は、MCS 7845 プラットフォームまたは同等 OVA プラットフォームで、2,000 のロケーションおよび 2,000 のリージョンをサポートしています。最大 2,000 のロケーションおよびリージョンを展開するには、[Service Parameter Configuration] ページの [Clusterwide Parameters (System - Location and Region)] および [Clusterwide Parameters (System - RSVP)] セクションで、次の Cisco CallManager サービス パラメータを設定する必要があります。

- [Intraregion Audio Codec Default]
- [Interregion Audio Codec Default]
- [Intraregion Video Call Bandwidth Default]
- [Interregion Video Call Bandwidth Default]
- [Default inter-location RSVP Policy]

リージョンを追加する際は、[Audio Codec] および [Video Call Bandwidth] の値に [Use System Default] を設定します。RSVP コール アドミッション制御を使用している場合は、[RSVP Setting] パラメータにも [Use System Default] を選択します。

個々のリージョンおよびロケーションについてこれらの値をデフォルトから変更すると、サーバの初期化とパブリッシャのアップグレードにかかる時間に影響します。合計 2,000 のリージョンと 2,000 のロケーションを使用する場合、そのうち最大 200 のリージョンおよびロケーションがデフォルト以外の値を使用するように変更できます。合計 1,000 以下のリージョンおよびロケーションを使用する場合、そのうち最大 500 のリージョンおよびロケーションがデフォルト以外の値を使用するように変更できます。表 8-4 は、これらの制限を要約したものです。

表 8-4　デフォルト以外の値を使用できるリージョンおよびロケーションの数

デフォルト以外の値を使用するリージョンおよびロケーションの数	リージョンの最大数	ロケーションの最大数
0 ～ 200	2,000	2,000
200 ～ 500	1,000	1,000

（注） 音声コーデック値は、音声コールと FAX コールの両方に使用されます。リージョン間コーデック値として G.729 を使用する場合、FAX コールには T.38 FAX リレーを使用してください。WAN で FAX パススルーを使用する場合は、[Interregion Audio Codec] をデフォルト値から G.711 に変更するか、デフォルト以外のコーデック値 G.711 を使用する各ロケーションに FAX マシンのリージョンを追加します（表 8-4 内の制限に従います）。

（注）　使用している MCS モデルに関係なく、多数のリモート サイトを包含する設計には、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニアが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。サイジング ツールを使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

Unified CM によるゲートウェイおよびトランクのサポート

Cisco Unified CM は、MCS 7845 プラットフォームまたは同等 OVA プラットフォームを使用する場合で、2,100 のゲートウェイおよびトランク（つまり、H.323 ゲートウェイ、H.323 トランク、デジタル MGCP デバイス、および SIP トランクの合計数）をサポートします。

クラスタ内のアクティブなゲートウェイ、トランク、およびメディア リソースの数を増やす場合は、すべてのコール処理サーバに対してこれらのデバイスの登録を均等に分散させて、クラスタ内の 1 台または複数台のサーバの CPU に対する過負荷を回避することが重要です。

（注）　使用している MCS モデルに関係なく、多数のゲートウェイおよびトランクを包含する設計については、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多く存在するため、シスコ代理店またはシスコのシステム エンジニアが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。サイジング ツールを使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

キャパシティの計算

キャパシティ プランニング ツールはシスコ代理店と従業員が使用でき、Unified CM を使用する大規模構成の Unified Communications システムのキャパシティを計算するのに役立ちます。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

シスコ代理店と従業員は、次の Web サイトで Cisco Unified Communications Sizing Tool を入手できます。

http://tools.cisco.com/cucst

Unified CMBE のキャパシティ プランニング

Unified CM と同様に、多くのタイプのデバイスを Unified CMBE に登録でき、これらの各デバイスには登録先のプラットフォームからの登録とトランザクション リソースが必要です。この項では、Unified CMBE のオーバーサブスクリプションを回避するためのシステム キャパシティ計画に関するルールとガイドラインを提供します。この項では、システムがオーバーサブスクライブしないことを保証するための配置計画の側面として、Busy Hour Call Attempts（BHCA; 最繁時呼数）についても説明します。さらに、Unified CMBE は Cisco Unified Communications Sizing Tool ではサポートされないため、システムのキャパシティ プランニングの決定に役立ついくつかのサンプル デバイスと BHCA 計算が提供されます。

表 8-5 に使用可能な Unified CMBE 製品と最大ユーザ、最大エンドポイント、および最大 BHCA のキャパシティを示します。

表 8-5　Unified CMBE の最大ユーザ、最大エンドポイント、および最大 BHCA のキャパシティ

Unified CMBE タイプ（プラットフォーム）	最大ユーザ	最大エンドポイント	最大 BHCA
Cisco Unified CMBE 3000（MCS 7816）	300	400	2,200
Cisco Unified CMBE 5000（MCS 7828）	500	575	3,600
Cisco Unified CMBE 6000（UCS C200）	1,000	1,200	5,000

Unified CMBE 最繁時呼数（BHCA）

BHCA は、最繁時のデバイスおよび 1 時間あたりの平均コール回数です（たとえば、多くのシステムの最繁時は、午前 10:00 ～ 11:00 または午後 2:00 ～ 3:00 です）。表 8-5 に示すように、Unified CMBE 3000 は最大 2,200 BHCA をサポートし、Unified CMBE 5000 は最大 3,600 BHCA をサポートします。一方、Unified CMBE 6000 は、最大 5,000 BHCA をサポートします。システム使用の計算では、Unified CMBE のオーバーサブスクリプションを回避するため、表 8-5 に示す BHCA 最大数を超えないようにします。

任意の電話機の BHCA が 4 BHCA を超えたときに、BHCA に対する配慮が必要になります。真の BHCA 値は、最繁時における電話機の使用状況の基準測定を実施することによってのみ、決定されます。この使用状況を基準なしで見積もった場合は特に注意が必要です。

Unified CMBE デバイスの見積もり

デバイスの見積もりは、この計算の目的の主な 2 つのカテゴリである電話デバイスとトランク デバイスに分けることができます。

電話デバイスは、単一のコール可能なエンドポイントです。これには、Cisco Unified IP Phone 7900 シリーズなどの単体のクライアント デバイス、Cisco IP Communicator などのソフトウェア クライアント、アナログ電話機ポートや H.323 クライアントなどが含まれます。Unified CMBE は、表 8-5 に示すエンドポイントの最大数をサポートしますが、実際のエンドポイント キャパシティは総システム BHCA によって異なります。

（注）　Unified CMBE 3000 がサポートするエンドポイントのセットには、制限があります。サポートされているエンドポイントのリストについては、http://www.cisco.com/en/US/products/ps11370/prod_maintenance_guides_list.html から入手可能な『*Administration Guide for Cisco Unified Communications Manager Business Edition 3000*』を参照してください。

トランク デバイスは、複数のコールを複数のエンドポイントまで伝送します。これは、SIP トランク、ゲートキーパー制御の H.323 トランク、または Unified CMBE 3000 の場合は MGCP バックホール PRI トランクなど、どのようなトランク デバイスやゲートウェイ デバイスでも可能です。

Unified CMBE 5000 および CMBE 6000 の両方が、H.323 トランク、SIP トランク、および MGCP トランク やゲートウェイならびにアナログ ゲートウェイのようなクラスタの間でクラスタ間トランキングをサポートします。ただし、Unified CMBE 3000 は、クラスタ間トランキングをサポートしていません。Unified CMBE 3000 のトランクおよびゲートウェイ サポートは、最大 2 つの E1/T1 PRI による

MGCP PSTN 接続用の Cisco Integrated Services Router（ISR; サービス統合型ルータ）2901 に制限されます。Unified CMBE 3000 は、アナログ電話機用の Cisco VG224 Analog Voice Gateway もサポートしています。

BHCA を見積もる方法は、両方のタイプのデバイスでほとんど同じですが、一般に、トランク デバイスは、外部のユーザ グループ（公衆網または他の PBX 拡張）にアクセスするためにより大きなエンドポイントのグループで使用されるため、BHCA が高くなります。

BHCA に基づく使用状況の特性を参照してデバイス グループ（電話デバイスまたはトランク デバイス）を定義してから、各デバイス グループの BHCA を加算して、システムの総 BHCA を求めることができます。これによって、表 8-5 に示すサポートされる BHCA 最大数を超えないことを常に確認します。

たとえば、4 BHCA の 100 台の電話機と 12 BHCA の 80 台の電話機の総 BHCA は、次のように計算できます。

4 BHCA の 100 台の電話機：100 * 4 = 400

12 BHCA の 80 台の電話機：80 * 12 = 960

総電話機 BHCA = (100 * 4) + (80 * 12) = 1,360 BHCA

トランク デバイスの場合は、公衆網上で開始または終了するデバイスからのコールの割合がわかっていれば、BHCA を計算できます。この例では、すべてのデバイス コールの半分が公衆網上で開始または終了している場合、ゲートウェイに対するデバイス BHCA の正味効果（この場合は 1360）は、1360 の半分、つまり、680 になります。したがって、この例での電話デバイスとトランク デバイスに関する総システム BHCA は次のようになります。

総システム BHCA = 1,360 + 680 = 2,040 BHCA

複数の電話機で回線を共有している場合は、回線を共有している電話機ごとに 1 つずつのコール レッグ（コールごとに 2 コール レッグ）を BHCA に含める必要があります。複数のデバイス グループで共有されている回線は、そのグループの BHCA に影響します。つまり、シェアド ラインに対する 1 つのコールが、回線インスタンスあたり 1 つのコール レッグ、つまり、1 コールの半分として計算されます。BHCA が異なる複数の電話機グループがある場合は、次の方法で BHCA 値を計算します。

シェアド ライン BHCA = 0.5 *（シェアド ライン数）*（1 回線あたりの BHCA）

たとえば、次の特徴を持つ 2 つのユーザ クラスがあるとします。

8 BHCA の 100 台の電話機 = 800 BHCA

4 BHCA の 150 台の電話機 = 600 BHCA

また、1 グループあたり 10 本のシェアド ラインがあるとして、次の BHCA 値に加算します。

8 BHCA のグループ内の 10 本のシェアド ライン = 0.5 * 10 * 8 = 40 BHCA

4 BHCA のグループ内の 10 本のシェアド ライン = 0.5 * 10 * 4 = 20 BHCA

この場合のすべての電話デバイスに関する総 BHCA は、シェアド ラインの BHCA の合計に加算された電話機グループごとの BHCA の合計になります。

800 + 600 + 40 + 20 = 1,460 総 BHCA

上記の各例の総 BHCA は、表 8-5 に示すシステムの最大 BHCA を下回っているため、許容範囲に含まれることに注意してください。

Unified CMBE 5000 または CMBE 6000 上で、モバイル コネクト（シングル ナンバー リーチまたは SNR とも呼ばれる）用に Cisco Unified Mobility を使用している場合、あるいは、Reach Me Anywhere 機能（SNR とも呼ばれる）を使用している場合、リモート接続先に転送されたコールまたはオフシステム電話機の数が BHCA に影響することに留意してください。アプライアンスがオーバーサブスクライブするのを防ぐには、この SNR リモート接続先またはオフシステム電話の BHCA を考慮する必要があります。これらの SNR 機能の BHCA を計算するには、「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）の項を参照して、その値を総 BHCA 値に加算します。

（注）　Secure RTP（SRTP）を使用したメディア認証と暗号化は、システム リソースとシステム性能に影響を与えます。メディア認証または暗号化の使用を検討している場合は、この事実に留意して適切な調整を行ってください。通常、セキュリティに対応していない 100 台の IP Phone は、セキュリティに対応した 90 台の IP Phone と同じ影響をシステム リソースに与えます（10 対 9 の割合）。

（注）　Cisco Unified CMBE 3000 は、メディア認証または暗号化をサポートしていません。

Unified CMBE のキャパシティ プランニングの考慮すべきもう 1 つの側面がコール カバレッジです。特殊なデバイス グループを作成し、特定のサービスの着信コールを複数のルール（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理できます。これは、Unified CMBE のハント グループまたは回線グループの設定で実現されます。この要素によっても BHCA が影響を受ける可能性がありますが、それはあくまでも回線グループ配信ブロードキャスト アルゴリズム（すべてのメンバーを呼び出す）に関係しているためです。Unified CMBE でブロードキャスト配信アルゴリズムが必要な場合は、1 つのハント グループまたは回線グループのメンバー数を 3 以下にすることを推奨します。システムの負荷によっては、この実施によってシステムの BHCA が大きく影響され、プラットフォームのリソースがオーバーサブスクライブする可能性があります。ブロードキャストの配信アルゴリズムを使用するハント グループまたは回線グループの数も 3 以下に制限する必要があります。

Unified CMBE 5000 Contact Center Integration のサイジングの例

この例では、Cisco Unified Contact Center Express（Unified CCX）が Unified CMBE 5000 と統合され、次のようなシステム特性があるものとします。

- 必要な仕様は、最繁時に 1 時間あたり最大 30 コールの 15 人のコンタクト センター エージェントに関するものです。
- 4 BHCA の平均使用非エージェント ユーザが 96 人いて、各ユーザは Cisco Unified Mobility を使用してシングル ナンバー リーチ用の 1 つのリモート接続先を設定できます。
- また、10 BHCA の大量使用非エージェント ユーザが 36 人いて、各ユーザはシングル ナンバー リーチ用の 1 つのリモート接続先を設定できます。
- 20 本のスタンバイ シェアド ラインがあり、そのうちの 10 本は平均使用プールの 10 ユーザで共有され、残りの 10 本は大量使用プールの 10 ユーザで共有されます。
- 全トランクの合計が 1200 BHCA の 7 個の T1 トランク（最大 161 の同時コールが可能）があります。

（注）　この例では、すべてのゲートウェイ トランクに関する BHCA を 1 つの総トランク BHCA 値にまとめます。この方法は主として、単一サイト配置に適しています。ただし、マルチサイト配置では、さまざまなサイトのトランクによってさまざまな BHCA 要件が設定されるため、複数の BHCA グループ分けが必要になります。

このシステムの BHCA 計算は次のようになります。

30 BHCA の 15 人のコンタクト センター エージェント = 450 BHCA

4 BHCA の 96 人の平均使用ユーザ = 384 BHCA

10 BHCA の 36 人の大量使用ユーザ = 360 BHCA

4 BHCA グループ内の 10 本のシェアド ライン = 20 BHCA

10 BHCA グループ内の 10 本のシェアド ライン = 50 BHCA

すべての T1 トランクの総 BHCA = 1,200 BHCA

4 BHCA の 96 人の平均使用ユーザごとの、シングル ナンバー リーチ用の 1 つのリモート接続先 = 192 BHCA（この計算の詳細については、「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）を参照してください）。

10 BHCA の 36 人の大量使用ユーザごとの、シングル ナンバー リーチ用の 1 つのリモート接続先 = 180 BHCA（この計算の詳細については、「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）を参照してください）。

この場合のすべてのエンドポイント デバイスの総 BHCA は次のとおりです。

(450 + 384 + 360 + 20 + 50 + 192 + 180 + 1200) = 2,836 BHCA

このレベルの使用状況は、システム上限の 3,600 BHCA を下回っているため、許容範囲であり、約 800 BHCA の余裕があります。

このサイジングの例は、Unified CMBE 5000 だけに適用されます。Unified CMBE 3000 では、Unified Contact Center 配置へのトランキングはできません。Unified CMBE 6000 は Unified Contact Center Express 共存で動作します。サイジングに関する考慮事項は同様ですが、この例は特に Unified CMBE 5000 に関連しています。

Cisco Unified CMBE キャパシティ プランニングの詳細については、他のすべての Unified CMBE 製品情報と同様、次のマニュアルを参照してください。

- Cisco Unified CMBE 3000

  http://www.cisco.com/en/US/products/ps11370/tsd_products_support_series_home.html
- Cisco Unified CMBE 5000

  http://www.cisco.com/en/US/products/ps7273/tsd_products_support_series_home.html
- Cisco Unified CMBE 6000

  http://docwiki.cisco.com/wiki/Cisco_Unified_Communications_Manager_Business_Edition_6000

コール処理の設計上の考慮事項

シスコのコール処理を配置する際は、次の設計上の推奨事項およびガイドラインに従ってください。

Cisco Unified CME

- Unified CME は、最大で 450 のエンドポイントをサポートします。ただし、Cisco IOS ルータ モデルによっては、エンドポイント キャパシティは大幅に低下する場合があります。Unified CME のプラットフォームおよびキャパシティの詳細については、次の Web サイトにある Cisco Unified Communications Manager Express の互換性情報を参照してください。
http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_device_support_tables_list.html
- 可能な場合は、複数の IP インターフェイスを使用して Unified CME ルータをネットワークに二重接続し、ネットワークの可用性を最大限まで高めます。同様に、同じ配置で Unified CME の複数のインスタンスが必要な場合は、複数の物理スイッチまたはロケーションに分散します。
- 可能な場合は、二重化電源および Uninterruptible Power Supply（UPS; 無停電電源装置）を備えた Unified CME ルータを配置し、プラットフォームの可用性を最大限まで高めます。

Cisco Unified CMBE

- Unified CMBE 3000 は、MCS 7816 または MCS 7890-C1（バージョン 8.6(1) 以降）で実行され、パブリッシャとシングル サブスクライバの複合インスタンスとして動作します。セカンダリ サブスクライバ インスタンスは設定できません。
- Unified CMBE 5000 は、単一ハードウェア プラットフォーム（MCS 7828）上で、パブリッシャとシングル サブスクライバの複合インスタンスとして動作します。セカンダリ サブスクライバ インスタンスは設定できません。
- Unified CMBE 6000 は、UCS C200 ラックマウント サーバ上で、パブリッシャとシングル サブスクライバの複合インスタンスとして動作します。セカンダリ サブスクライバによってコール処理の冗長性を提供するために、別の UCS C200 サーバを配置できます。また、MCS サーバを冗長性を提供するために使用できます。

（注）　さらなる冗長性と地理的な分散、あるいはそのいずれかを提供するために、Unified CMBE 6000 の展開では 2 台を超える UCS C200 ラックマウント サーバをクラスタリングできます。ただし、クラスタ全体でユーザの合計数が 1,000 を超えることはできず、クラスタ全体で設定されたデバイスの合計数が 1,200 を超えることはできません。

- Unified CMBE 3000 は、最大で 400 のエンドポイントをサポートします。ただし、実際のエンドポイント キャパシティは総システム BHCA によって異なりますが、最大で 2,200 を超えることはできません。
- Unified CMBE 5000 は、最大で 575 のエンドポイントをサポートします。ただし、実際のエンドポイント キャパシティは総システム BHCA によって異なりますが、最大で 3,600 を超えることはできません。
- Unified CMBE 6000 は、最大で 1,200 のエンドポイントをサポートします。ただし、実際のエンドポイント キャパシティは総システム BHCA によって異なりますが、最大で 5,000 を超えることはできません。
- NIC チーミングを使用して Unified CMBE 5000 の MCS 7828 サーバをネットワークに二重接続し、ハイ アベイラビリティを最大限まで高めます。Unified CMBE 3000 は NIC チーミングをサポートしていません。

- 同じ配置で Unified CMBE 5000 または CMBE 6000 の複数のインスタンスが必要な場合は、複数の物理スイッチに分散します。
- Unified CMBE プラットフォーム（MCS 7816、MCS 7828、MCS 7890-C1、および UCS C200）は、二重化電源を備えていない、あるいはサポートしていないため、Uninterruptible Power Supply（UPS; 無停電電源装置）を使用してプラットフォームの可用性を最大限まで高めます。
- ハイ アベイラビリティのために 2 台のサーバで Unified CMBE 6000 を配置する場合（2 台の UCS C200 ラックマウント サーバ、または 1 台の UCS C200 ラックマウント サーバと 1 台の MCS サーバ）、システム負荷を分散するために、2 台のサーバ間でデバイスの登録をロードバランシングする必要があります。スタンバイ冗長性のために 2 台めのサーバを使用することを推奨します。
- Unified CMBE 3000 は、次に示すエンドポイントおよびゲートウェイの特定のタイプのみのサポートを提供します。
  - Unified CMBE 3000 がサポートするエンドポイントのセットには、制限があります。サポートされているエンドポイントのリストについては、次の Web サイトから入手可能な『*Administration Guide for Cisco Unified Communications Manager Business Edition 3000*』を参照してください。

    http://www.cisco.com/en/US/products/ps11370/prod_maintenance_guides_list.html
  - Unified CMBE 3000 PSTN 接続は、Cisco 2901 Integrated Services Router（ISR; サービス統合型ルータ）を通じてのみ、また MGCP バックホール T1/E1 PRI トランクを使用する場合のみサポートされています。
  - Unified CMBE 3000 はクラスタ間トランキングをサポートしていないため、分散コール処理配置もサポートしていません。

Cisco Unified CM

- Cisco Unified CM クラスタ内で最大 8 つのコール処理サブスクライバ ノード（Cisco CallManager サービスを実行するノード）を使用可能にできます。その他のサーバは、パブリッシャ、TFTP、およびメディア リソース サービス専用で使用できます。
- Unified CM 8.6(1) 以降の各クラスタは、MCS 7845-I3 サーバまたは同等 OVA サーバで、最大 40,000 台のセキュアまたは非セキュア SCCP または SIP 電話機の設定および登録をサポートしています。
- Unified CM 8.5 以前の各クラスタは、最大 30,000 台のセキュアまたは非セキュア SCCP または SIP 電話機の設定および登録をサポートしています。
- Unified CM は、MCS 7845 サーバまたは同等 OVA サーバのクラスタで、最大 2,000 のロケーションをサポートします。MCS 7825 または MCS 7835 サーバ モデルのクラスタでは、500 ロケーションをサポートします。
- MCS 7845 サーバまたは同等 OVA サーバのクラスタは、最大 2,100 台の H.323、MGCP、および SIP ゲートウェイまたはトランクをサポートできます。MCS 7825 または MCS 7835 サーバのクラスタは、最大 600 台の H.323、MGCP、および SIP ゲートウェイまたはトランクをサポートします。
- クラスタ内に最大 2 台の MCS 7815 または MCS 7816 サーバを配置できます。1 台をパブリッシャ、TFTP、およびバックアップ コール処理サブスクライバ ノードにし、もう 1 台をプライマリ コール処理サブスクライバにします。この構成では、MCS 7816 で最大 500 台の電話機がサポートされ、MCS 7815 で最大 300 台の電話機がサポートされます。
- キャパシティの大きいサーバを使用して 2 サーバ クラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることを推奨します。1,250 ユーザを超える場合は、専用パブリッシャと別個のサーバをプライマリおよびバックアップのコール処理サブスクライバ用に推奨します。

- クラスタ内のすべてのサーバに対して同じサーバ モデルを使用することを推奨します。ただし、個別のハードウェア バージョンがすべてサポートされており、すべてのサーバで同じバージョンの Unified CM が実行されている場合、クラスタ内にサーバ モデルおよび異なるサーバ ベンダーのモデルを混在させることもサポートされます。
- 7,500 台を超える IP Phone が 2 つのプライマリ サブスクライバに登録される場合は、1:1 コール処理冗長性方式を使用する必要があります。これは、1 つのバックアップ サブスクライバで 7,500 台を超えるバックアップ登録はできないからです。
- NIC チーミングを使用して MCS サーバをネットワークに二重接続し、ハイ アベイラビリティを最大限まで高めます。MCS 7815 のネットワーク インターフェイス ポートは 1 つだけのため、NIC チーミングを実行できません。
- 可能な場合は常に、Unified CM サーバをネットワーク内の複数の物理スイッチおよび同じ LAN または MAN 内の複数の物理ロケーションに分散させて、スイッチの障害または特定のネットワーク ロケーションの損失による影響を最小限に抑えます。
- SRST または SRST として機能する Unified CME をリモート ロケーションの Cisco IOS ルータに配置して、これらのロケーションで Unified CM クラスタへの接続が失われた場合にフォールバック コール処理サービスを提供します。
- Unified CM クラスタ内で Voice Activity Detection（VAD; 音声アクティビティ検出）を使用不可にしておくことを推奨します。Cisco IOS H.323 および SIP ダイヤル ピアでも、**no vad** コマンドを使用して VAD を使用不可にする必要があります。
- Unified CM を Cisco UCS B シリーズ ブレード サーバに配置する場合は、バックアップまたは冗長サブスクライバ ノードがプライマリ サブスクライバ ノードとは異なる物理ブレード上に存在するように、サーバ ノード インスタンスが UCS シャーシ内のブレード サーバ間で分散されるようにします。
- 複数の Open Virtualization Archive（OVA）テンプレートを使用してハーフ幅 UCS B200 B シリーズ ブレード サーバと C210 ラックマウント サーバの両方を設定できます。最も大きい OVA テンプレートは、10,000 のデバイスをサポートし、MCS 7845-I3 サーバと同じキャパシティ（エンドポイント、ゲートウェイ、ロケーション、リージョンなどの数）を提供します。適切な OVA サイジングについては、Cisco Unified Communications Sizing Tool を使用してください。適切なログイン認証を持つシスコの従業員またはパートナーは http://tools.cisco.com/cucst で Cisco Unified Communications Sizing Tool を入手できます。
- UCS B シリーズ ブレード サーバおよび C シリーズ ラックマウント サーバは、KVM ケーブルを介して USB およびシリアル ポートをサポートしますが、Unified CM VMware 仮想アプリケーションはこれらのポートにアクセスできません。そのため、Unified CM を UCS に配置する場合、MoH 用の固定ライブ オーディオ ソースを接続すること、レガシー ボイスメール システムへのシリアル SMDI 接続を行うこと、またはログ ファイルの書き込みのために USB フラッシュ ドライブを接続することはできません。代わりに、次のオプションを利用できます。
  - MoH ライブ オーディオ ソース フィードの場合は、ライブ オーディオ ソース接続に Cisco IOS ベースのマルチキャスト MoH を使用するか、または MCS サーバに Unified CM クラスタの一部として 1 台の Unified CM サブスクライバ ノード配置して、USB MoH オーディオ カード（MOH-USB-AUDIO=）を接続できるようにすることを検討します。
  - SMDI シリアル接続の場合は、MCS サーバに Unified CM クラスタの一部として 1 台の Unified CM サブスクライバ ノードを配置して、USB シリアル接続に使用します。
  - システムのインストール ログの保存には、仮想フロッピー ソフトメディアを使用します。
- シスコは、一部のサブスクライバ サーバ ノード インスタンスを UCS B シリーズ ブレード サーバで実行し、別の一部を C シリーズ ラックマウント サーバで実行して、その他の残りのサブスクライバ サーバ ノード インスタンスを MCS サーバ プラットフォームで実行する Unified CM クラスタをサポートしています。

コンピュータ テレフォニー インテグレーション（CTI）

Cisco Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）を利用すると、Cisco Unified CM で使用可能な豊富な機能セットだけでなく、サードパーティ製のアプリケーションも使用できるようになります。これらの Cisco CTI 対応アプリケーションによって、ユーザの生産性が向上し、コミュニケーションが活発になるとともに、高品質のカスタマー サービスを提供できるようになります。Cisco CTI を使用すると、サードパーティ製デスクトップ アプリケーションで Microsoft Outlook 内から通話を行ったり、着信コールの発信者 ID に基づいてウィンドウを開いたり、アプリケーションを起動したりできます。また、課金のためにコールと連絡先をリモートで追跡することもできます。Cisco CTI 対応のサーバ アプリケーションでは、企業ネットワーク全体での適切な対応先のルーティングや、自動応答や音声自動応答装置（IVR）などの自動発信者サービスの提供に加えて、対応先の記録および分析に役立つメディアの取り込みも行えます。

CTI アプリケーションは一般に、次の 2 つの主なカテゴリに分類できます。

- ファーストパーティ製のアプリケーション：モニタ、制御、メディア ターミネーション

  ファーストパーティ製の CTI アプリケーションは、コールのセットアップ、終了、およびメディア ターミネーション用の CTI ポートおよびルート ポイントなどのデバイスを登録するように設計されています。これらのアプリケーションはメディア パスに直接配置されているので、インバンド DTMF などのメディア レイヤのイベントに応答できます。ファーストパーティ製の CTI アプリケーションには音声自動応答装置や Cisco Attendant Console などがあり、これらのアプリケーションはコールをモニタおよび制御しながら、コール メディアとも対話します。

- サードパーティ製のアプリケーション：モニタおよび制御

  サードパーティ製の CTI アプリケーションもコールをモニタおよび制御しますが、メディア ターミネーションは直接制御しません。

  - モニタリング アプリケーション

    Cisco IP デバイスの状態をモニタする CTI アプリケーションは、モニタリング アプリケーションと呼ばれます。オンフックまたはオフフックのステータスを表示する、またはその情報を使用してユーザの可用性をプレゼンスの形式で示すビジーランプフィールド アプリケーションは、どちらもサードパーティ製の CTI モニタリング アプリケーションの例です。

  - 呼制御アプリケーション

    Cisco CTI を使用して、アウトバンド シグナリングを使用する Cisco IP デバイスをリモート制御するアプリケーションは、呼制御アプリケーションです。Cisco IP デバイスをリモート制御するように設定された Cisco Unified Personal Communicator は、呼制御アプリケーションのよい例です。

  - モニタリング + 呼制御アプリケーション

    これらは、Cisco IP デバイスをモニタおよび制御するすべての CTI アプリケーションです。Cisco Unified Contact Center Enterprise は、エージェントのステータスをモニタして、エージェント デスクトップを介してエージェント電話機を制御するため、モニタと制御を兼ね備えたアプリケーションのよい例です。

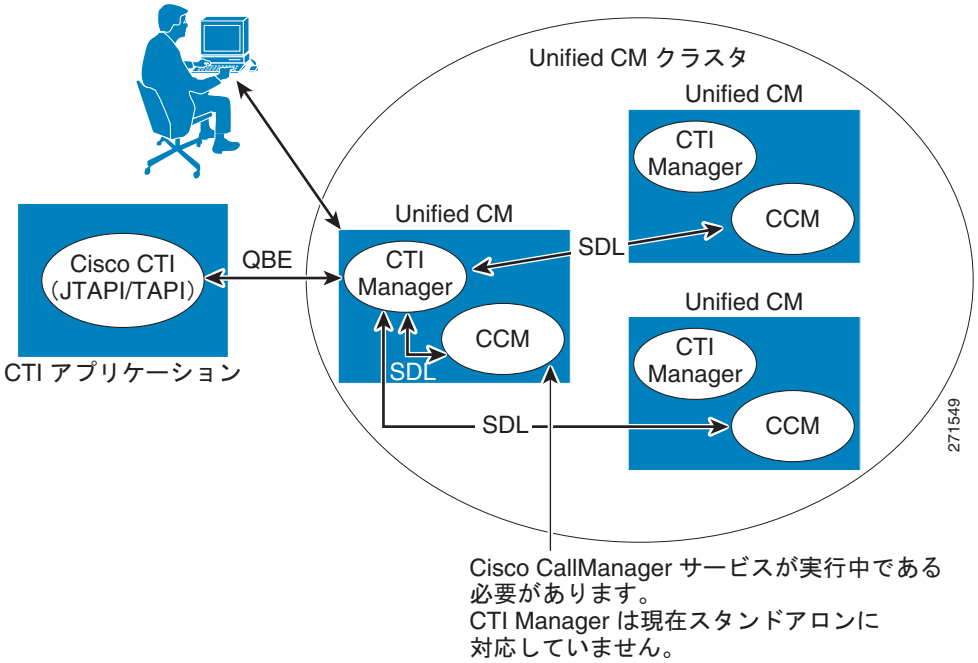
（注） ここでモニタリング アプリケーション、呼制御アプリケーション、モニタリング + 呼制御アプリケーションの違いを列挙しましたが、この細かな違いはアプリケーション開発者には見えないようになっています。Cisco CTI を使用するすべての CTI アプリケーションは、モニタリングおよび制御の両方に有効です。

CTI のアーキテクチャ

Cisco CTI は、次のコンポーネントで構成されます（図 8-9 を参照）。これらは互いに対話し、Cisco Unified CM で使用可能なテレフォニー機能セットを各アプリケーションで利用できるようにします。

- CTI 対応アプリケーション：特定のテレフォニー機能を提供するために作成されたシスコ製またはサードパーティ製のアプリケーション。
- JTAPI および TAPI：Cisco CTI でサポートされる 2 つの標準インターフェイス。開発者は、好みの方式のライブラリを使用してアプリケーションを作成できます。
- Unified JTAPI および Unified TSP クライアント:外部メッセージを Cisco Unified CM で使用される内部の Quick Buffer Encoding（QBE）メッセージに変換します。
- Quick Buffer Encoding（QBE）：Unified CM の内部通信メッセージ。
- プロバイダー：アプリケーションと CTI Manager との接続の論理的な表現であり、通信を容易にするために使用されます。プロバイダーは、アプリケーションにデバイス イベントおよびコール イベントを送付しながら、アプリケーションによるデバイスのリモート制御を可能にする制御命令を受け付けます。
- Signaling Distribution Layer（SDL）：Unified CM の内部通信メッセージ。
- パブリッシャおよびサブスクライバ：Cisco Unified Communications Manager（Unified CM）サーバ。
- CCM：Cisco CallManager サービス（ccm.exe）。テレフォニー処理エンジンです。
- CTI Manager（CTIM）：プライマリまたはセカンダリ モードで動作する 1 つ以上の Unified CM サブスクライバで実行され、Cisco IP デバイスを制御およびモニタできるようにテレフォニー アプリケーションを認証および許可するサービス。

図 8-9　Cisco CTI のアーキテクチャ



アプリケーションを認証および許可すると、CTIM は、テレフォニー アプリケーションと Cisco CallManager サービスの仲介者として機能します（このサービスは呼制御エージェントです。全体の製品名である Cisco Unified Communications Manager と混同しないでください）。CTIM はテレフォニー アプリケーションから送信される要求に応答し、その要求を Unified CM システムで内部的に使用される Signaling Distribution Layer（SDL）メッセージに変換します。Cisco CallManager サービスからのメッセージも CTIM によって受信され、処理のために適切なテレフォニー アプリケーションに転送されます。

CTIM は、Cisco CallManager サービスがアクティブになっているクラスタの Unified CM サブスクライバ サーバでアクティブにできます。これによって、Unified CM クラスタ内で 8 つまでの CTIM をアクティブにできます。スタンドアロンの CTIM は現在サポートされていません。

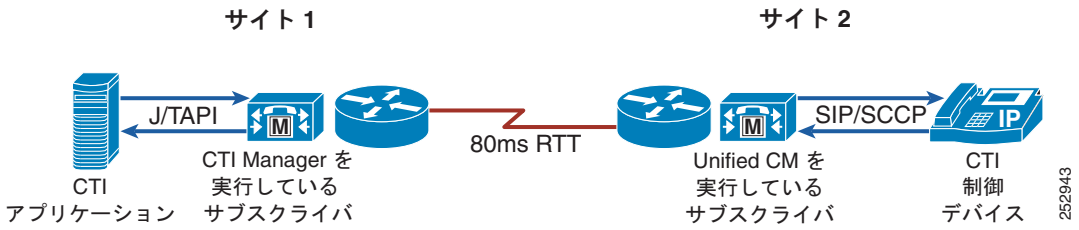
WAN を介した CTI アプリケーションおよびクラスタリング

WAN を介したクラスタリングを採用した配置では、次の 2 つのシナリオがサポートされます。

- WAN を介した CTI Manager（図 8-10 を参照）

  このシナリオでは、CTI アプリケーションとそれに関連付けられた CTI Manager が WAN の一方の側（サイト 1）に配置され、Unified CM サブスクライバに登録されるモニタおよび制御対象のデバイスが他方の側（サイト 2）に配置されます。WAN を介したクラスタリングの Round-Trip Time（RTT; ラウンドトリップ時間）は、現在サポートされている限度値 80 ms を超えることはできません。CTI トラフィックに必要な帯域幅を計算するには、「ローカル フェールオーバー配置モデル」（P.5-51）にある公式を使用します。この帯域幅は、「ローカル フェールオーバー配置モデル」（P.5-51）の説明に従って計算した Intra-Cluster Communication Signaling（ICCS）帯域幅や、音声に必要な帯域幅（RTP トラフィック）とは別に必要であることに注意してください。

図 8-10　　WAN を介した CTI



- WAN を介した TAPI および JTAPI アプリケーション（WAN を介した CTI アプリケーション）（図 8-11 を参照）

  このシナリオでは、CTI アプリケーションが WAN の一方の側（サイト 1）に配置され、関連付けられた CTI Manager が他方の側（サイト 2）に配置されます。このシナリオでは、CTI アプリケーション開発者またはプロバイダーの責任において、アプリケーションが実装された RTT に適応できるかどうかを確認します。場合によっては、アプリケーションが CTI Manager と同じ場所にある場合よりも、フェールオーバー時間およびフェールバック時間が長くなることがあります。このような場合、アプリケーション開発者またはプロバイダーは、そのような状況におけるアプリケーションの動作に関するガイダンスを示す必要があります。

図 8-11　WAN を介した JTAPI

（注）　WAN を介した TAPI および JTAPI のサポートは、アプリケーションに依存します。ユーザとアプリケーション開発者またはプロバイダーの両者が、使用するアプリケーションに WAN を介したクラスタリングが含まれる配置との互換性があることを確認する必要があります。

CTI のキャパシティ プランニング

Unified CM は、次のような CTI のキャパシティをサポートしています。

CTI 接続の制限

CTI 接続のキャパシティ制限は、次のとおりです。

- Cisco MCS 7825-H3/I3 は、専用サブスクライバとして使用する場合にサーバごとに 900 の CTI 接続、またはクラスタごとに 3,600 の CTI 接続をサポートします。パブリッシャおよびサブスクライバ ノードが組み合された Cisco MCS 7825-H3/I3 は、800 の CTI 接続をサポートします。
- Cisco MCS 7825-H5/I5 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 1,000 の CTI 接続、またはクラスタごとに 4,000 の接続をサポートしています。
- Cisco MCS 7835-H2/I2 は、サーバごとに 2,000 の CTI 接続またはクラスタごとに 8,000 の CTI 接続をサポートします。
- Cisco MCS 7835-H3/I3 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 2,500 の CTI 接続、またはクラスタごとに 10,000 の接続をサポートしています。
- Cisco MCS 7845-H2/I2 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 5,000 の CTI 接続、またはクラスタごとに 20,000 の接続をサポートしています。
- Unified CM 8.6(1) 以降のリリースでは、Cisco MCS 7845-I3 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 10,000 の CTI 接続、またはクラスタごとに 40,000 の接続をサポートしています。

注：

- Cisco CTI 対応の IP デバイスは常に、クラスタ内のすべてのノードに対して均等に分散させる必要があります。
- JTAPI アプリケーションの場合、CTI 接続は各 JTAPI アプリケーションと Unified CM サーバ間の単一の TCP/IP 接続です。

- TAPI アプリケーションの場合、CTI 接続は TAPI アプリケーション サーバにある Cisco TSP と Unified CM サーバ間の単一の TCP/IP 接続です。単一の TSP に接続している TAPI アプリケーションが（同じサーバ上に）複数ある場合があります。その場合、それらのすべての TAPI アプリケーションでは 単一の CTI 接続が使用されます。
- 各 CTI 接続は、1 つのアプリケーションまたは CTI の「プロバイダー」セッションを処理します。
- CTI パフォーマンス モニタ（perfmon）の CTI Connection Active を使用すると、特定の Unified CM サーバ上の CTI 接続の合計数を確認できます。

CTI に関連付けられる制御されるデバイスの制限

制御される関連デバイスに対する CTI のキャパシティ制限は、次のとおりです。

- Cisco MCS 7825-H3/I3 は、専用サブスクライバとして使用する場合にサーバごとに 900 台の CTI デバイス、またはクラスタごとに 3,600 台の CTI デバイスをサポートします。パブリッシャおよびサブスクライバ ノードが組み合された Cisco MCS 7825-H3/I3 は、800 台の CTI デバイスをサポートします。
- Cisco MCS 7825-H5/I5 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 1,000 の CTI デバイス、またはクラスタごとに 4,000 のデバイスをサポートしています。
- Cisco MCS 7835-H2/I2 は、サーバごとに 2,000 台の CTI デバイスまたはクラスタごとに 8,000 台の CTI デバイスをサポートします。
- Cisco MCS 7835-H3/I3 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 2,500 の CTI デバイス、またはクラスタごとに 10,000 のデバイスをサポートしています。
- Cisco MCS 7845-H2/I2 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 5,000 の CTI デバイス、またはクラスタごとに 20,000 のデバイスをサポートしています。
- Unified CM 8.6(1) 以降のリリースでは、Cisco MCS 7845-I3 サーバまたは同等 OVA サーバは、サーバまたは OVA テンプレートごとに 10,000 の CTI デバイス、またはクラスタごとに 40,000 のデバイスをサポートしています。

注：

- Cisco CTI 対応の IP デバイスは常に、クラスタ内のすべてのノードに対して均等に分散させる必要があります。
- 制御されるデバイスの制限は、アクティブなアプリケーションにのみ適用されます。非アクティブ（無効）なアプリケーションに関連付けられている制御されるデバイスは、制限にはカウントされません。
- 制御されるデバイスの制限では、デバイスごとに最大 5 つの CTI 制御回線が想定されています（CTI アプリケーションの影響を正しくサイジングするには、http://tools.cisco.com/cucst で適切なログイン認証を持つシスコの従業員とパートナーが入手できる Cisco Unified Communications Sizing Tool を使用します）。同じデバイス上の追加の各 CTI 制御回線は、CTI キャパシティ プラニングのために個別のデバイスとしてカウントされます（たとえば、デバイスごとに 2 つの CTI 制御回線を持つ 400 台のデバイスは、400 台の CTI 制御デバイスと同じカウントになりますが、3 つの CTI 制御回線を持つ 400 台のデバイスは 800 台の CTI デバイスとしてカウントされます）。
- 制御されるデバイスの制限では、各 CTI 制御デバイスには最大 5 つのシェアド ラインがあることも想定されています。同じデバイスに 2 つ以上のシェアド ラインがある場合、CTI のキャパシティ プランニングではそれぞれが別個のデバイスとしてカウントされます。
- さらに、制御されるデバイスの制限では、各デバイスが最大 5 つの CTI アプリケーションによってモニタまたは制御されることも想定されています。

- 制御されるデバイスの制限には、デバイスにある CTI 制御回線が 1 つであるか 2 つであるかに関係なく、デバイスごとに 1 時間で 6 件のコールという基本コールが想定されています。これ以上のコールがシナリオに含まれる（転送や会議など）場合や、コール レートが高い場合は、制限に影響します（適切なサイジングについては、Cisco Unified Communications Sizing Tool を使用してください。適切なログイン認証を持つシスコの従業員またはパートナーが http://tools.cisco.com/cucst で入手できます）。
- CTI アプリケーションに関連付けられている制御されたデバイスの数が多くなるほど、アプリケーションの初期化と Unified CM フェールオーバー / フェールバック処理時間が長くなります。これは、アプリケーションがアクティブにデバイスを制御していない場合でも当てはまります。
- CTI パフォーマンス モニタ（perfmon）の Devices Open と Lines Open を使用すると、特定の Unified CM サーバ上でアプリケーションによって現在制御されているデバイスと回線の合計数を確認できます。

Cisco Unified Communications Manager Business Edition では、このサーバの CTI デバイスの最大数は 500 です。

Unified CM クラスタに必要な CTI リソースの決定

Unified CM クラスタに必要な CTI リソースの数を調べる作業には、次の 4 段階のプロセスが含まれます。

ステップ 1　総 CTI デバイス数を調べます。

CTI で制御され、クラスタ上で使用される予定のデバイスの数を数えます。

ステップ 2　CTI 回線係数を調べます。

次の表に従って、クラスタ内のすべてのデバイスの CTI 回線係数を決定してください。

CTI デバイスごとの回線数	CTI 回線係数
1 ～ 5 回線 / デバイス	1
6 回線 / デバイス	1.2
7 回線 / デバイス	1.4
8 回線 / デバイス	1.6
9 回線 / デバイス	1.8
10 回線 / デバイス	2

（注）　クラスタ内のデバイスの回線係数がばらついている場合は、システム内のすべての CTI デバイスでの平均回線係数を求めます。

ステップ 3　アプリケーション係数を調べます。

次の表に従って、クラスタ内のすべてのデバイスのアプリケーション係数を決定してください。

デバイスごとの CTI アプリケーションの数	CTI アプリケーション係数
1 ～ 5 アプリケーション / デバイス	1
6 アプリケーション / デバイス	1.2

デバイスごとの CTI アプリケーションの数	CTI アプリケーション係数
7 アプリケーション/デバイス	1.4
8 アプリケーション/デバイス	1.6
9 アプリケーション/デバイス	1.8
10 アプリケーション/デバイス	2

（注）　クラスタ内のデバイスのアプリケーション係数がばらついている場合は、システム内のすべての CTI デバイスでのアプリケーション係数を求めます。

ステップ 4　総 CTI リソースを求める次の式に従って、クラスタに必要な総 CTI リソースを決定します。

総 CTI リソース = CTI デバイスの総数 * 最大値 {回線係数またはアプリケーション係数}

次の例の計算で、このサイジング プロセスの 4 つの手順を示します。

例 1 : デバイスごとの平均回線数が 9、平均アプリケーション数が 4 で、500 台の CTI デバイスが配置されています。ステップ 2 とステップ 3 にリストされている係数に従うと、デバイスごとの回線数 9 の場合の回線係数は 1.8、デバイスごとのアプリケーション数が 4 の場合のアプリケーション係数は 1.0 になります。これらの値をステップ 4 の式に代入すると、次の値が得られます。

500 CTI デバイス * 最大値 {回線係数 1.8 またはアプリケーション係数 1.0}

500 CTI デバイス * 回線係数 1.8 = 900 の総 CTI リソースが必要

例 2 : デバイスごとの平均回線数が 5、平均アプリケーション数が 9 で、2,000 台の CTI デバイスが配置されています。ステップ 2 とステップ 3 にリストされている係数に従うと、デバイスごとの回線数 5 の場合の回線係数は 1.0、デバイスごとのアプリケーション数が 9 の場合のアプリケーション係数は 1.8 になります。これらの値をステップ 4 の式に代入すると、次の値が得られます。

2000 CTI デバイス * 最大値 {回線係数 1.0 またはアプリケーション係数 1.8}

2000 CTI デバイス * アプリケーション係数 1.8 = 3,600 の総 CTI リソースが必要

例 3 : デバイスごとの平均回線数が 2、平均アプリケーション数が 3 で、5,000 台の CTI デバイスが配置されています。前述のステップ 2 とステップ 3 にリストされている係数に従うと、デバイスごとの回線数 2 の場合の回線係数は 1、デバイスごとのアプリケーション数が 3 の場合のアプリケーション係数は 1 になります。これらの値をステップ 4 の式に代入すると、次の値が得られます。

5,000 CTI デバイス * 最大値 {回線係数 1 またはアプリケーション係数 1}

5,000 CTI デバイス * 回線係数またはアプリケーション係数 1 = 5,000 の総 CTI リソースが必要

CTI のハイ アベイラビリティ

ここでは、ハイ アベイラビリティのための CTI プロビジョニングについて、いくつかのガイドラインを提供します。

CTI Manager

CTI Manager は、Unified CM クラスタ内の少なくとも 1 つ（おそらくすべて）のコール処理サブスクライバで有効にする必要があります。クライアント側のインターフェイス（TAPI TSP または JTAPI クライアント）では IP アドレスを 2 つずつ使用できます。これらの IP アドレスは、CTIM サービスを実行している Unified CM サーバを指します。CTI アプリケーションの冗長性を確保するため、図 8-12 のとおり、クラスタの少なくとも 2 つの Unified CM サーバで、CTIM サービスをアクティブにすることを推奨します。

冗長性、フェールオーバー、およびロード バランシング

冗長性が必要な CTI アプリケーションでは、TAPI TSP または JTAPI クライアントは 2 つの IP アドレスで設定できるため、障害発生時には代替の CTI Manager を使用できます。ここで注意すべきは、2 つの CTI Manager 間で情報が共有されていないため、この冗長性はステートフルではありません。そのため、フェールオーバーの際に、再初期化が必要になることがあります。

CTI Manager がフェールオーバーした場合、必要な処理は、現在アクティブになっている CTI Manager で CTI アプリケーションのログイン プロセスをやり直すことだけです。ただし、Unified CM サーバ自体に障害が発生した場合は、障害が発生した Unified CM や現在アクティブになっている Unified CM などのすべてのデバイスを再登録し、その後で CTI アプリケーションのログイン プロセスを実行する必要があるため、再初期化プロセスは時間がかかります。

ロード バランシングが必要な CTI アプリケーションや、この設定を利用できる CTI アプリケーションは、図 8-12 に示すように、2 つの CTI Manager に同時に接続できます。

図 8-12　　冗長性とロード バランシング

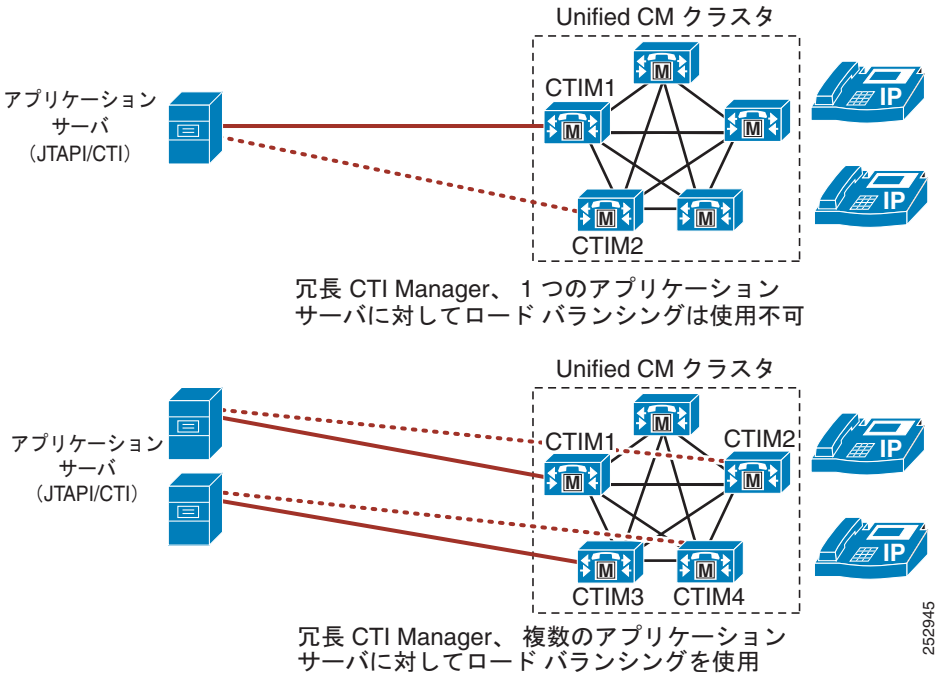


図 8-13 は、このタイプの Cisco Unified Contact Center Enterprise（Unified CCE）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCE は冗長性のために 2 つの Peripheral Gateway（PG; ペリフェラル ゲートウェイ）を使用します。
- 各 PG は異なる CTI Manager にログインします。
- 一度に 1 つの PG しかアクティブになりません。

図 8-13　Cisco Unified Contact Center Enterprise での CTI の冗長性

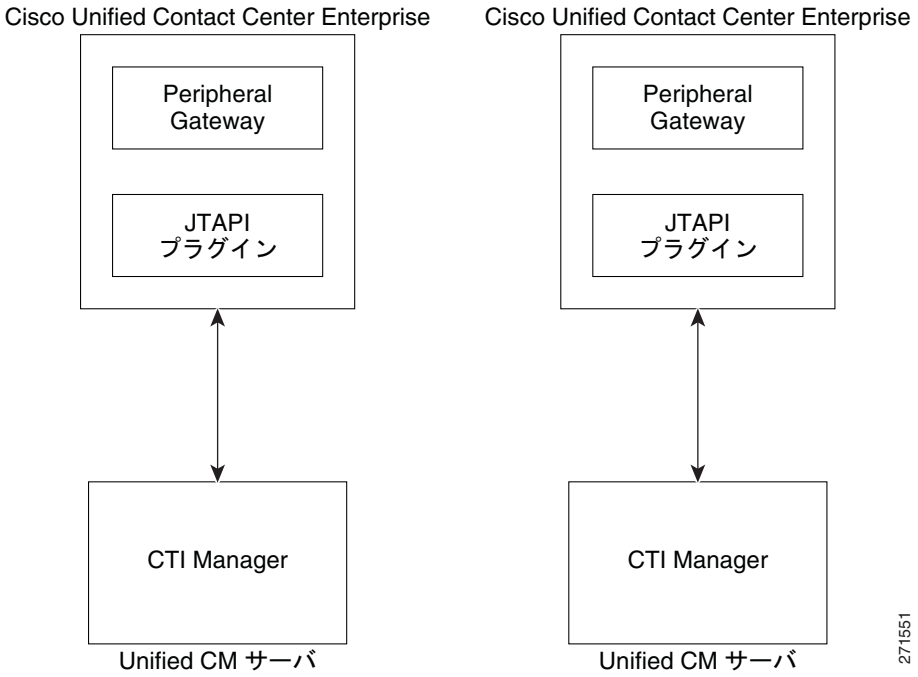
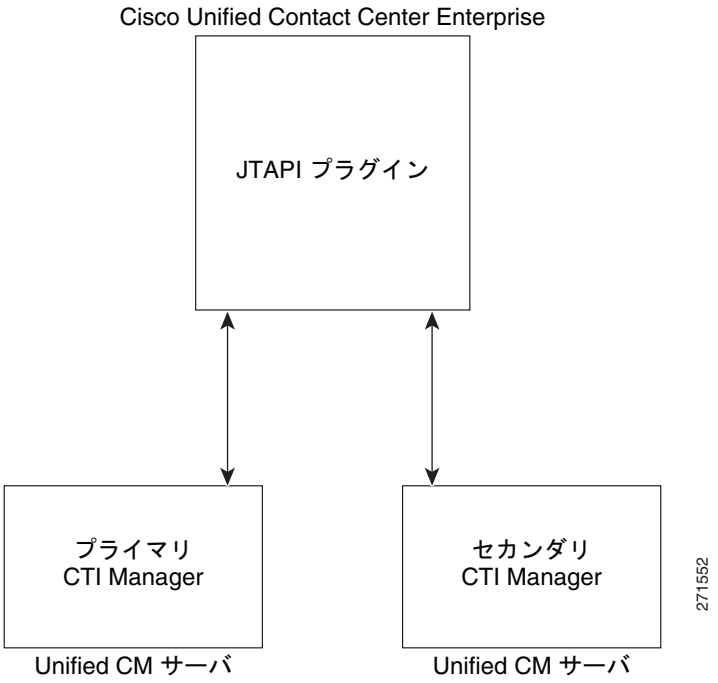


図 8-14 は、このタイプの Cisco Unified Contact Center Express（Unified CCX）の設定例を示しています。このタイプの設定には、次の特性があります。

- Unified CCX では、各 CTI Manager 用に 1 つずつ、合計で 2 つの IP アドレスを設定できます。
- プライマリ CTI Manager への接続が失われた場合、Unified CCX はセカンダリ CTI Manager にフェールオーバーします。

図 8-14　Cisco Unified Contact Center Express での CTI の冗長性



実装

アプリケーションの作成に関するガイダンスとサポートについて、アプリケーション開発者は次の Web サイトの Cisco Developer Connection で相談してください。

http://developer.cisco.com/web/cdc/community

ゲートキーパーの設計上の考慮事項

1 台の Cisco IOS ゲートキーパーで、分散型コール処理環境で最大 100 の Unified CM クラスタに対してコール ルーティングとコール アドミッション制御をサポートできます。複数のゲートキーパーを設定すると、数千の Unified CM クラスタをサポートできます。Cisco IOS ゲートキーパーを使用して、H.323 ゲートウェイと Unified CM 間の通信とコール アドミッション制御をサポートすることによって、ハイブリッド Unified CM とトール バイパス ネットワークを実装することもできます。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、ハブアンドスポーク トポロジに制限されます。

ほとんどの Cisco IOS ルータは、ゲートキーパー機能をサポートします。ゲートキーパー機能の特定のプラットフォーム サポートについては、次の Web サイトで入手可能な『*Cisco IOS H323 Gatekeeper Data Sheet*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4139/data_sheet_c78_561921.html

冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。この項では、ゲートキーパー ネットワークを構築するための設計要件について検討します。ただし、コール アドミッション制御やダイヤル プラン解決については扱いません。これらについては、「コール アドミッション制御」（P.11-1）と「ダイヤル プラン」（P.9-1）の章でそれぞれ説明しています。

ゲートキーパーの詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10591/products_installation_and_configuration_guides_list.html

ハードウェア プラットフォームの選択

ゲートキーパーのプラットフォームは、1 秒間あたりのコール数、および同時発生コール数に基づいて選択します。1 秒間あたりのコール数が多いほど、高性能な CPU が必要になります。同時発生コールの数が大きいほど、より多くのメモリが必要になります。設計要件に大量のコールと大量の同時コールが含まれている場合には、大量のメモリ キャパシティがある Cisco IOS ルータとパフォーマンスの高い CPU を選択します。

ゲートキーパーのプラットフォームの詳細については、次の Web サイトで入手できる『*Cisco IOS H323 Gatekeeper Data Sheet*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4139/data_sheet_c78_561921.html

ゲートキーパーの冗長性

ゲートキーパーが、クラスタ間通信にすべてのコール ルーティングとアドミッション制御機能をサポートする場合は、冗長性が必要です。ゲートキーパーの冗長性をサポートするには、ゲートキーパー クラスタリングとディレクトリ ゲートキーパーという 2 つの方法があります。

（注）　可能な場合、ゲートキーパーの冗長性をサポートするには、ゲートキーパー クラスタリングを使用することを推奨します。ソフトウェア機能セットでゲートキーパー クラスタリングが利用できない場合以外は、ゲートキーパーの冗長性に Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用しないでください。

ゲートキーパー クラスタリング（代替ゲートキーパー）

ゲートキーパー クラスタリング（代替ゲートキーパー）により、「ローカル」ゲートキーパー クラスタの設定が可能になります。各ゲートキーパーは、一部の Unified CM トランクのプライマリ、およびその他のトランクの代替として機能します。Gatekeeper Update Protocol（GUP）は、ローカル クラスタ内のゲートキーパー間で状態情報を交換するために使用されます。GUP は、クラスタ内のゲートキー

パーごとに CPU 使用率、メモリ使用率、アクティブ コール数、および登録されたエンドポイント数をトラッキングし、報告します。GUP メッセージングで次のパラメータにしきい値を設定すると、ロード バランシングがサポートされます。

- CPU 使用率
- メモリ使用率
- アクティブ コール数
- 登録されたエンドポイント数

ゲートキーパー クラスタリング（代替ゲートキーパー）のサポートにより、ステートフル冗長性とロード バランシングが使用可能になります。ゲートキーパー クラスタリングは、次の機能を提供します。

- ローカルとリモートのクラスタ
- ローカル クラスタ内の最大 5 つのゲートキーパー
- ローカル クラスタ内のゲートキーパーを、別々のサブネットまたはロケーションに配置可能
- フェールオーバーの遅延なし（代替ゲートキーパーはすでにエンドポイントを認識しているので、完全な登録プロセスを実行する必要はありません）
- クラスタ内のゲートキーパーは、状態情報を渡し、ロード バランシングを行う

図 8-15 では、Unified CM 分散型コール処理を行う 3 つのサイト、およびローカル クラスタで設定された 3 つの分散型ゲートキーパーを示しています。

図 8-15　ゲートキーパー クラスタリング

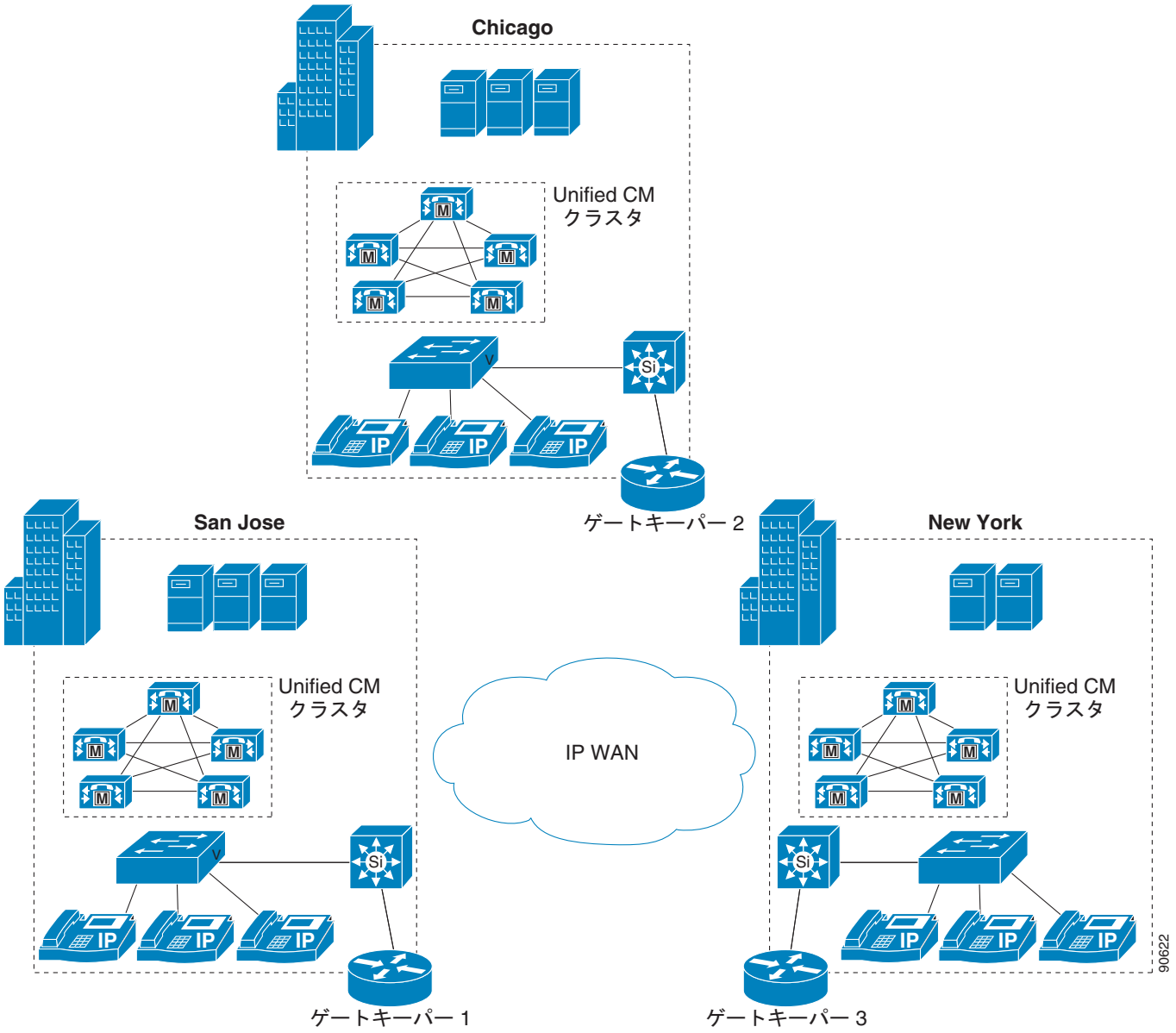


図 8-15 では、各サイトの Unified CM クラスタはローカル ゲートキーパーに登録されます。ローカル ゲートキーパー サービスは、各ローカル ゲートキーパーが別のサイトにあるゲートキーパーでバックアップされるように、ゲートキーパー クラスタリングを使用して冗長にします。

ゲートキーパー クラスタリングを配置する場合は、次のガイドラインを考慮してください。

- Unified CM トランク登録をサポートするために、各 Unified CM クラスタにはローカル ゾーンが設定されます。このローカル ゾーンは、Unified CM 内と、Unified CM クラスタと一緒に配置されたゲートキーパーに設定されます。図 8-15 に示す例では、San Jose サイトにある Unified CM クラスタに、San Jose のゲートキーパー（Gatekeeper 1）に設定されたローカル ゾーン名と一致するゾーン名でゲートキーパー制御トランクが設定されます。同様に、Chicago および New York の

Unified CM クラスタに、それぞれのロケーション（Chicago の場合は Gatekeeper 2、New York の場合は Gatekeeper 3）に配置されたゲートキーパーのローカル ゾーン名と一致するゾーン名が設定されます。

- ローカル ゾーンごとにゲートキーパーが定義され、**element** コマンドを使用して他のゲートキーパー上にバックアップ ゾーンが設定されます。図 8-15 に示す例では、San Jose のゲートキーパー（Gatekeeper 1）に、Chicago のゲートキーパー（Gatekeeper 2）と New York のゲートキーパー（Gatekeeper 3）の両方のエレメントでローカル ゾーンが設定されます。同様に、Chicago および New York のゲートキーパーに、San Jose のゲートキーパーと互い（それぞれ）の両方のエレメントでローカル ゾーンが設定されます。
- **gw-type-prefix** コマンドを使用して、ローカルで解決されないすべてのコールをローカル ゾーン内で設定されたテクノロジー プレフィックスに登録されたデバイスに転送できます。図 8-15 に示す例では、各 Unified CM ゲートキーパー制御トランクは 1#* のテクノロジー プレフィックスで設定され、各サイトのゲートキーパーは 1#* の default-technology gw-type-prefix で設定されます。
- クラスタリング ゲートキーパー間のロード バランシングは、**load-balance** コマンドを使用して設定されます。図 8-15 に示す例では、各サイトのゲートキーパーを設定して、CPU 使用率、メモリ使用率、エンドポイント数、およびコール数のしきい値に基づいてロード バランスしたり、エンドポイント / ゲートウェイ登録をローカルのゲートキーパーからクラスタ内の代替ゲートキーパーへ移したりできます。たとえば San Jose のゲートキーパー（Gatekeeper 1）を、上限が 80% に設定された CPU およびメモリしきい値に基づいてエンドポイントまたはゲートウェイ登録が Chicago のゲートキーパーに移るように設定できます。この場合、San Jose のゲートキーパーのメモリおよび CPU の使用率が 80% に達すると、トランク登録状態を維持するために、そのゲートキーパーは San Jose の Unified CM クラスタに送信する Registration, Admission, and Status（RAS）メッセージへの Chicago のゲートキーパー情報の送信を開始します。同様に、Chicago および New York の他のゲートキーパーも設定し、それらのサイトのローカル Unified CM トランク登録の負荷を他のサイトにあるゲートキーパーにロードバランスできます。
- 図 8-15 の 3 つの Unified CM クラスタ間でコールをルーティングするときに、そのロケーションとコールがルーティングされているロケーション間のネットワークで適切な帯域幅を使用できることを確認するために、各サイトのゲートキーパーを設定する必要があります。十分な帯域幅がないと、コールがルーティングされません。分散型 Unified CM のロケーション間のゾーン間コール帯域幅を指定するには、**bandwidth interzone** コマンドを推奨します。
- **arq reject-unknown-prefix** コマンドを使用して、クラスタ内の冗長 Unified CM トランク上にできるコール ルーティングを回避します。このコマンドを使用すると、ダイヤルされたプレフィックスが定義されたプレフィックスと一致しないときに、ゲートキーパーからコール ルーティング要求がローカル ゲートウェイまたは Unified CM トランクに転送されるのを防止します。

ゲートキーパーの配置および設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10591/products_installation_and_configuration_guides_list.html

ディレクトリ ゲートキーパーの冗長性

HSRP を使用するか、複数の同じディレクトリ ゲートキーパーを設定すると、ディレクトリ ゲートキーパーの冗長性を実装できます。同じゾーン プレフィックスを使用して、複数のリモート ゾーンを持つゲートキーパーを設定するとき、このゲートキーパーには、次のいずれかの方法が使用できます。

- シーケンシャル LRQ

  冗長リモート ゾーン（ゾーン プレフィックスが一致）にコストが割り当てられ、LRQ は、コスト値に基づいた順序で、一致するゾーンに送信されます。順次 LRQ を使用すると、一致するすべてのゲートキーパーに LRQ を送信しないので、WAN 帯域幅の節約になります。

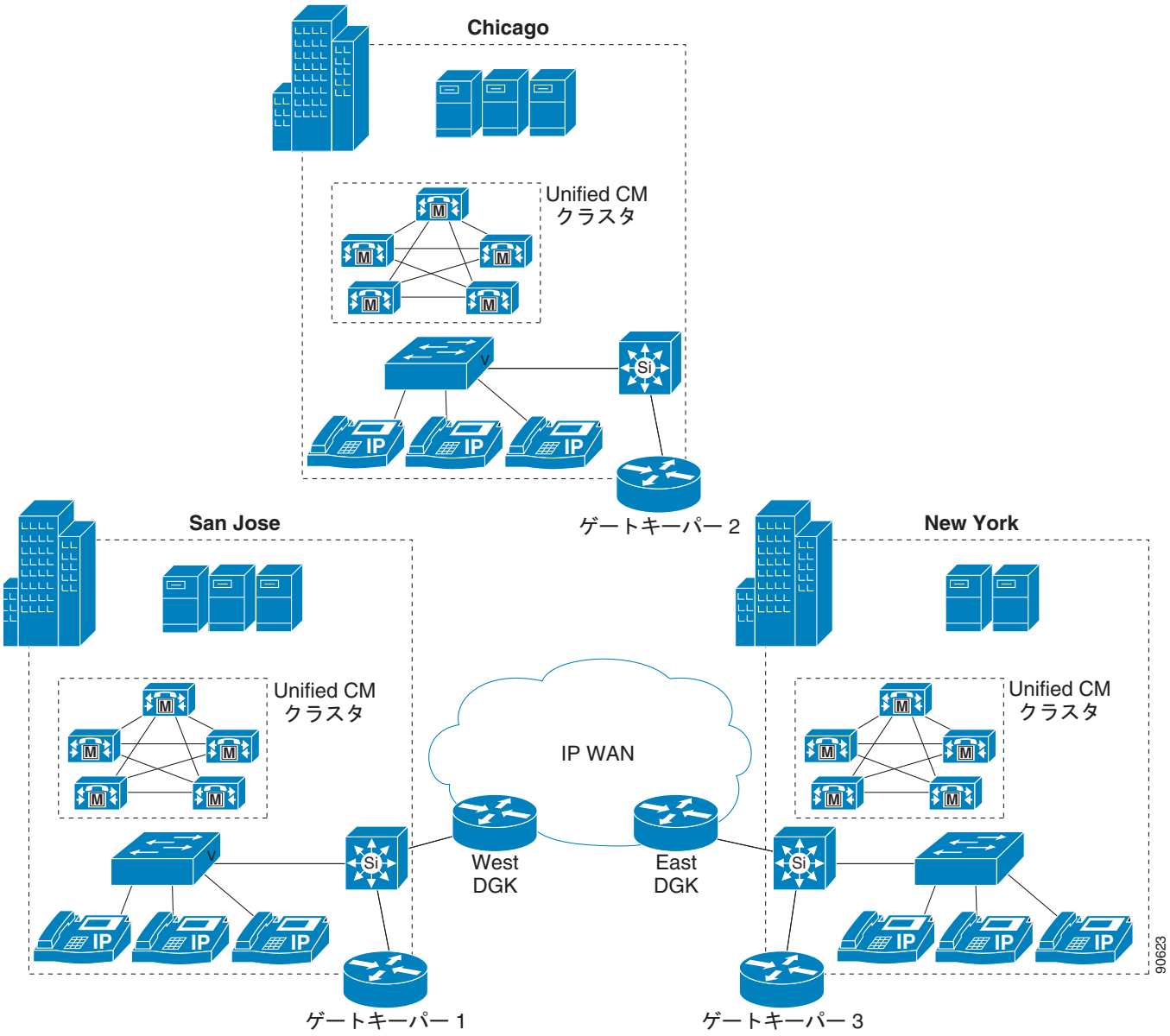
- LRQ ブラスト

  LRQ は、冗長ゾーン（ゾーン プレフィックスが一致）に同時に送信されます。ロケーション確認（LCF）で応答する最初のゲートキーパーが、使用されます。

順次 LRQ を使用して複数のアクティブ ディレクトリ ゲートキーパーを使用することを推奨します。これによって、ディレクトリ ゲートキーパーを別々のロケーションに配置できます。HSRP を使用するには、両方のディレクトリ ゲートキーパーを同じサブネットに置く必要があります。この場合常に 1 つのゲートキーパーしかアクティブにすることができません。

図 8-16 では、図 8-15 に示すように 3 つの分散型ローカル ゲートキーパーを備えた、3 つのサイトの同じ Unified CM 分散型コール処理配置を示しています。ただし、図 8-15 に示した配置とは異なり、図 8-16 の配置は、冗長サイト間コール ルーティングの 2 つのアクティブ ディレクトリ ゲートキーパーに依存する 3 つの分散型ローカル ゲートキーパー（代替ゲートキーパーまたはクラスタリング ゲートキーパーに依存するのではなく）を示します。

図 8-16　冗長ディレクトリ ゲートキーパー



冗長ディレクトリ ゲートキーパーを配置する場合は、次のガイドラインを考慮してください。

- ディレクトリ ゲートキーパーの冗長性を設定するときは、各ディレクトリ ゲートキーパーをローカル ゾーンで設定します。図 8-16 に示す例では、San Jose（West DGK）にあるディレクトリ ゲートキーパーは 1 つのローカル ゾーン名と IP アドレスで設定されますが、New York（East DGK）にあるディレクトリ ゲートキーパーはもう 1 つのローカル ゾーン名と IP アドレスで設定されます。
- ディレクトリ ゲートキーパーは、ネットワーク上の各ゲートキーパーに対応するリモート ゾーンで設定する必要があります。図 8-16 に示す例では、San Jose（West DGK）にあるディレクトリ ゲートキーパーと New York（East DGK）にあるゲートキーパーの両方は、San Jose サイト（Gatekeeper 1）のゲートキーパーに対応するリモート ゾーン、Chicago サイト（Gatekeeper 2）

のゲートキーパーに対応するリモート ゾーン、および New York サイト（Gatekeeper 3）のゲートキーパーに対応するリモート ゾーンで設定されます。これらのリモート サイトの設定は、両方のディレクトリ ゲートキーパー上で同一です。

- 各ディレクトリ ゲートキーパーは、ゾーン間コール ルーティングの各リモート ゾーンに対応する着信番号のプレフィックスで設定されます。図 8-16 に示す例では、両方のディレクトリ ゲートキーパーは、各サイトのゲートキーパーによってサービスが提供されるローカル エリア コードに対応するプレフィックスで設定されます。たとえば、San Jose のゲートキーパー（Gatekeeper 1）のリモート ゾーンには、プレフィックス 408 が設定され、Chicago のゲートキーパー（Gatekeeper 2）のリモート ゾーンには、プレフィックス 720 が設定され、New York のゲートキーパー（Gatekeeper 3）のリモート ゾーンには、プレフィックス 212 が設定されます。他の着信番号のプレフィックスに対応する必要に応じて各リモート ゾーンに対して、追加のプレフィックスを設定できます。コールはローカル ディレクトリ ゲートキーパー ゾーンにルーティングされないので、これらのゾーンにはプレフィックスは必要ありません。特定のプレフィックスの設定に加え、ワイルドカード文字 * を使用して、can be 明示的に定義されていないすべてのプレフィックスに対応付けることができます。
- 各ディレクトリ ゲートキーパーで **lrq forward-queries** コマンドを設定し、1 つのゲートキーパーから受信したコール セットアップ ロケーション要求（LRQ）がダイヤルされたプレフィックスに基づいたサービスに応じて他のゲートキーパーの 1 つに転送されるようにします。図 8-16 に示す例では、LRQ 照会を転送するために、San Jose（West DGK）にあるディレクトリ ゲートキーパーと New York（East DGK）にあるディレクトリ ゲートキーパーの両方を設定する必要があります。

（注） ディレクトリ ゲートキーパーは、アクティブ エンドポイント登録を含まず、いかなる帯域幅管理も行いません。

- 前の例（図 8-15）と同様に、図 8-16 の各サイトに示されているローカル サイト ゲートキーパーが、各サイトにある Unified CM クラスタ トランクにサービスおよび登録を提供します。
- 各ローカル サイトのゲートキーパーは、各ディレクトリ ゲートキーパーのリモート ゾーンで設定されます。図 8-16 に示す例では、San Jose サイト（Gatekeeper 1）にあるローカル ゲートキーパーに、San Jose（West DGK）にあるディレクトリ ゲートキーパーと New York（East DGK）にあるディレクトリ ゲートキーパーの両方に設定されたリモート ゾーンがあります。Chicago（Gatekeeper 2）および New York（Gatekeeper 3）にあるローカル ゲートキーパーは同じように設定されます。
- ローカル ゲートキーパーと設定されたリモート ゾーンとの間の帯域幅を制限するために、各ローカル サイトのゲートキーパーを設定する必要があります。図 8-16 に示す例では、各ローカル ゲートキーパーは、リモート ゾーンのディレクトリ ゲートキーパーへのコールのルーティングに使用できる帯域幅の量を決定する **bandwidth remote** コマンドを使用して設定されます。たとえば、**bandwidth remote** コマンドは、San Jose（West DGK）にあるディレクトリ ゲートキーパーに定義されたリモート ゾーンおよび New York（East DGK）にあるディレクトリ ゲートキーパーに定義されたリモート ゾーンへのコールのルーティングに使用できる帯域幅を制限するために、San Jose のゲートキーパー（Gatekeeper 1）に設定されます。これにより、San Jose サイトのゲートキーパー（Gatekeeper 1）と他のサイトのゲートキーパーのいずれか（Gatekeeper 2 または Gatekeeper 3）との間のコール ルーティングに使用できる帯域幅が制限されます。この同じ設定は、他のローカル サイトのゲートキーパーに複製されます。
- 各ローカル サイトのゲートキーパーは、ローカル ゲートキーパーに対応するローカル ゾーンのゾーン プレフィックスと 2 つのディレクトリ ゲートキーパーの両方のリモート ゾーンのゾーン プレフィックスで設定されます。前者のローカル ゾーン プレフィックスはローカル Unified CM クラスタへのコール ルーティングを処理するのに対し、後者のリモート ゾーン プレフィックスは他のゲートキーパー サイトへのゾーン間コール ルーティングを処理します。図 8-16 に示す例では、San Jose サイトにあるローカル ゲートキーパー（Gatekeeper 1）はローカル ゾーン プレフィクス

408 およびリモート ゾーン プレフィクスである 10 個のドット（.）で設定されていて、2 つのディレクトリ ゲートキーパー（East DGK および West DGK）に対応しています。これらの 10 個のドット（.）のプレフィクスは、ローカル ゾーン プレフィクス 408 で始まらない正規化された 10 桁の E.164 着信番号すべてと一致します。したがって、Gatekeeper 1 によってルーティングされた、408 で始まらないすべてのコールは、ディレクトリ ゲートキーパーの 1 つを経由して他のゲートキーパー サイトの 1 つにルーティングされます。Chicago（Gatekeeper 2）および New York（Gatekeeper 3）のサイトにあるローカル ゲートキーパーは、同一の一般的なリモート ゾーンの 10 個のドット プレフィックスと同時に、それぞれローカル ゾーン プレフィックス 720、212 で設定されます。

- 一致するゾーン プレフィックスが設定されるとき、デフォルトで順次ロケーション要求（LRQ）が使用されます。図 8-16 に示す例では、408 で始まらない着信番号にルーティングされたすべてのコールについて、まず San Jose サイトにあるローカル ゲートキーパー（Gatekeeper 1）は、San Jose にあるディレクトリ ゲートキーパー（West DGK）に、LRQ を West DGK に対応するリモート ゾーンに設定された一般的な 10 個のドット（.）のプレフィクスに基づいて送信します。West DGK から応答を受け取らなかった場合、Gatekeeper 1 は、次に New York にあるディレクトリ ゲートキーパー（East DGK）に、LRQ を East DGK に対応するリモート ゾーンに設定された一般的な 10 個のドット（.）のプレフィクスに基づいて送信します。同様に、まず Chicago および New York のサイトにあるローカル ゲートキーパー（それぞれ Gatekeeper 2、Gatekeeper 3）は、ディレクトリ ゲートキーパーの 1 つに、LRQ をリモート ゾーンと 10 個のドット（.）のプレフィクス設定に基づいて送信します。このディレクトリ ゲートキーパーから応答を受け取らなかった場合は、次に 2 番めのディレクトリ ゲートキーパーに LRQ を送信します。
- 前のゲートキーパー クラスタリングの例（図 8-15）と同様に、**gw-type-prefix** コマンドを使用して、ローカルで解決されないすべてのコールをローカル ゾーン内に設定されたテクノロジー プレフィックスに登録されたデバイスに転送できます。**arq reject-unknown-prefix** コマンドは、クラスタ内の冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

ディレクトリ ゲートキーパーの配置の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10591/products_installation_and_configuration_guides_list.html

Unified CM と Unified CM Express の相互運用性

この項では、H.323 または SIP トランキング プロトコルを使用している Cisco Unified CM と Cisco Unified Communications Manager Express（Unified CME）に関して、マルチサイト IP テレフォニー配置における相互運用性およびインターネットワーキングの要件について説明します。ここでは、Unified CM の制御する電話機と Unified CME の制御する電話機との間での推奨する配置を中心に説明します。

この項では、次のトピックについて取り上げます。

Unified CM と Unified CME 間の相互運用性の概要

H.323 または SIP をトランキング プロトコルとして使用して、Unified CM と Unified CME を相互接続できます。本社または中央サイトに Unified CM を配置して、支店の Unified CME システムと連携させる場合、ネットワーク管理者は、プロトコルの仕様と WAN トランク全体でサポートされる機能を慎重に検討して、SIP または H.323 のいずれかのプロトコルを選択する必要があります。以前は、H.323 トランクを使用して Unified CM と Unified CME を接続する方法が主流でしたが、SIP 電話機と SIP トランクのより高度な機能が Unified CM と Unified CME に追加されたことで、この状況は変わりました。この項ではまず、Unified CM と Unified CME の相互運用性のトランキング プロトコルとは無関係のいくつかの機能について説明し、次に SIP トランクと H.323 トランクを使用するための最も一般的な設計シナリオとベスト プラクティスを紹介します。

コール タイプとコール フロー

一般に、Unified CM と Unified CME のインターワーキングを使用すると、SIP トランクまたは H.323 トランク全体で、SCCP IP Phone から SIP IP Phone へのコール、またはその逆のコールをすべて組み合せることができます。コールは、Unified CM と Unified CME SIP 間、または SCCP IP Phone との間で、転送（ブラインドまたは打診）または自動転送できます。

H.323 トランク経由で Unified CM に接続していると、Unified CME は Unified CM のコールを自動検出できます。Unified CME を終端とするコールが転送または自動転送されると、Unified CME はコールを再生成し、ヘアピン コールによって他の Unified CME または Unified CM に適切にコールをルーティングします。Unified CME は必要に応じて、SIP トランクまたは H.323 トランク全体の VoIP コールについて、Unified CM からのコール レッグをヘアピンします。H.450 以外でサポートされる Unified CM ネットワークで自動検出を可能にする方法と、H450.2、H450.3、または SIP の付加サービスを有効または無効にする方法の詳細については、次の Web サイトで入手可能な Unified CME の製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html

SIP トランク経由で Unified CM に接続すると、Unified CME は Unified CM のコールを自動検出しません。デフォルトでは、Unified CME は常に、コール転送の SIP Refer メッセージまたは自動転送の SIP 302 Moved Temporarily メッセージを使用して、コールをリダイレクトしようとします。リダイレクトが失敗すると、Unified CME はヘアピン コールを試みます。

保留音

Unified CM では G.711 形式と G.729 形式の両方で MoH ストリームを有効にできますが、Unified CME で MoH をストリームできるのは G.711 形式のみです。そのため、保留になったコールの MoH オーディオを Unified CME で制御する場合は、G.711 MoH ストリームと G.729 コール レッグの間でトランスコーディングするためのトランスコーダが必要です。

Ad Hoc および Meet-Me のハードウェア会議

Ad Hoc 会議と Meet-Me 会議の両方に、ハードウェアの DSP リソースが必要です。SIP、H.323、PSTN のいずれを経由して接続している場合でも、Unified CM 電話機と Unified CME 電話機は、ネットワークから到達できる限り、Ad Hoc 会議に招待または追加されて、会議の参加者になることができます。アクティブな会議のセッション中にコールを保留にしても、その会議のセッションの参加者には音楽は聞こえません。

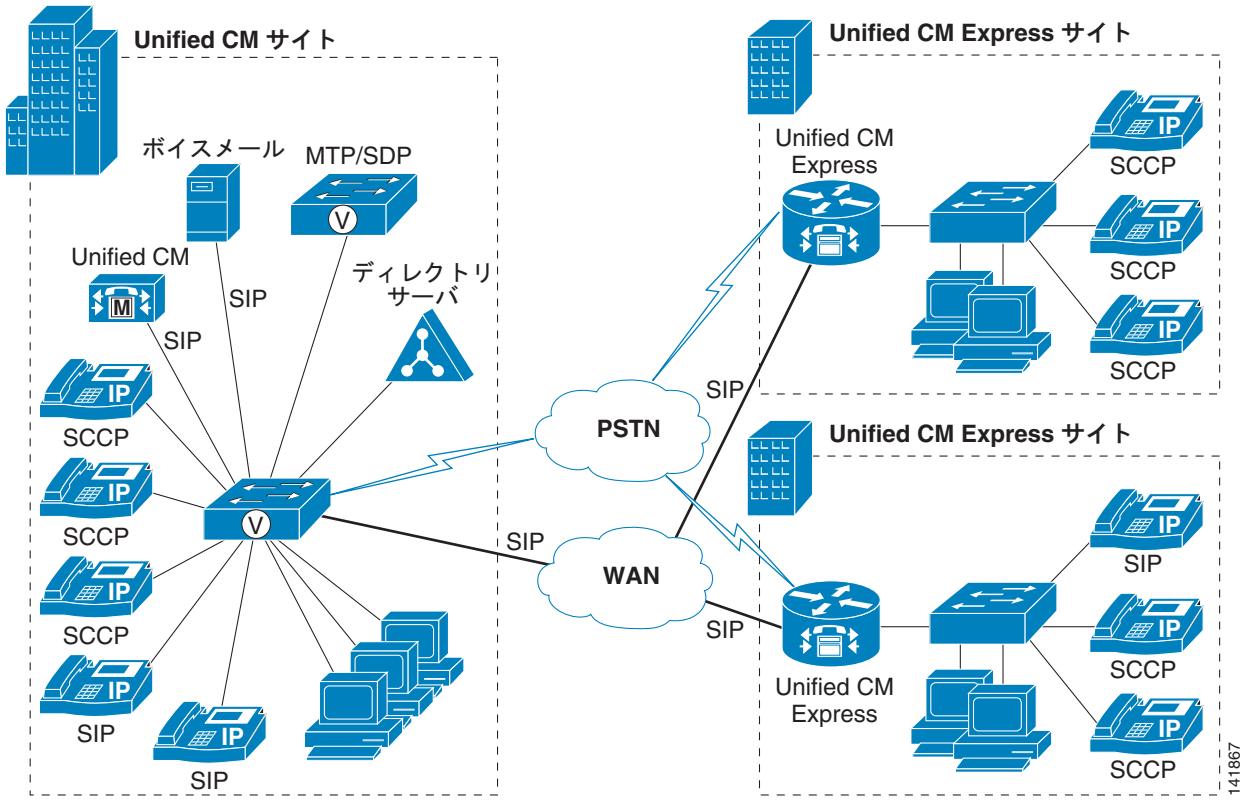
Ad Hoc 会議と Meet-Me 会議に必要でサポートされる DSP リソースと、会議に参加できる最大人数については、次の Web サイトで入手可能な Unified CME の製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/tsd_products_support_series_home.html

分散型コール処理を使用したマルチサイト配置における SIP 経由の Unified CM と Unified CME の相互運用性

Unified CM は、SIP インターフェイスを使用する Unified CME と直接通信できます。図 8-17 に、SIP トランクを使用して Unified CM が Cisco Unified CME と直接ネットワーク接続されている Cisco Unified Communications マルチサイト配置を示します。

図 8-17　SIP トランクを使用して Unified CM と Unified CME を接続したマルチサイト配置



ベスト プラクティス

図 8-17 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- [Accept Replaces Header] を選択した SIP トランク セキュリティ プロファイルを設定します。
- 作成した SIP トランク セキュリティ プロファイルを使用して SIP トランクを Unified CM 上に設定し、再ルーティング CSS も指定します。再ルーティング CSS は、どこで SIP ユーザ（転送者）が別のユーザ（被転送者）を第三者ユーザ（転送先）に振り向けることができるか、および SIP 302 Redirection Response と Replaces を持つ INVITE を使用して SIP ユーザがどの機能を呼び出せるかを決定するために使用します。

- SIP トランクの場合、Unified CME 上で SCCP エンドポイントを使用しているときに、Media Termination Point（MTP; メディア ターミネーション ポイント）を使用可能にする必要はありません。ただし、Unified CME 上に SIP エンドポイントがある場合は、メディア ターミネーション ポイントを Unified CM 上で使用して、SIP プロトコルでディレイド オファー / アンサー交換の処理（Session Description Protocol なしの INVITE 受信）ができるようにする必要があります。
- Unified CM ダイヤル プラン設定（ルート パターン、ルート リスト、ルート グループ）を使用して、SIP トランク経由で Unified CME にコールをルーティングします。
- Unified CM のデバイス プールとリージョンを使用して、サイト内では G.711 コーデックを設定し、リモートの Unified CME サイトに対しては G.729 コーデックを設定します。
- Unified CME の **voice services voip** で **allow-connections sip to sip** コマンドを設定して、SIP-to-SIP コール接続を許可します。
- SIP エンドポイントの場合は、**voice register global** で **mode cme** コマンドを設定し、Unified CME の SIP 電話機ごとに **voice register pool** コマンドで **dtmf-relay rtp-nte** を設定します。
- SCCP エンドポイントの場合は、Unified CME の **telephony-service** で **transfer-system full-consult** コマンドと **transfer-pattern .T** コマンドを設定します。
- Unified CME の **session protocol sipv2** および **dtmf-relay [sip-notify | rtp-nte]** により、SIP WAN インターフェイスの voip ダイヤル ピアを設定し、Unified CM を宛先としてコールを転送またはリダイレクトします。

設計上の考慮事項

この項ではまず、一部の主要な領域における SIP 経由での Unified CM と Unified CME の相互運用性に関するいくつかの特徴と設計上の考慮事項について説明します。主要な領域には、コール転送や自動転送のための付加サービス、スピード ダイヤル ボタンや電話帳のコール リストの Busy Lamp Field（BLF）通知のためのプレゼンス サービス、パートナー アプリケーションとの統合や、Unified CM 電話機と Unified CME 電話機間のクリックダイヤルに対するサードパーティ製電話による制御のための Out-Of-Dialog Refer（OOD-Refer）などが含まれます。この項では、SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項についても説明します。

付加サービス

SIP Refer メッセージや SIP 302 Moved Temporarily メッセージを Unified CME または Unified CM でのコール転送や自動転送などの付加サービスに使用して、転送先または自動転送先に対して新しいコールを開始するよう、被転送者または自動転送される電話機（被転送者）に指示できます。SIP Refer メッセージまたは SIP 302 Moved Temporarily メッセージがサポートされている場合、コール転送や自動転送のシナリオにはヘアピンは不要です。

ただし、DID マッピングがない内線が存在する場合や、Unified CM または Unified CME に、SIP 302 Moved Temporarily メッセージの DID にコールをルーティングするダイヤル プランがない場合は、**supplementary-service** を無効にする必要があります。**supplementary-service** が無効になっていると、Unified CME はコールをヘアピンするか、re-INVITE の SIP メッセージを Unified CM に送信して、新しい着信者 ID へメディア パスを置き換えます。それ以降のコール転送に複数の Unified CME が関係する場合でも、シグナリングとメディアの両方がヘアピンされます。転送されたコールでも、**supplementary-service** は無効にできます。この場合、SIP Refer メッセージ は Unified CM に送信されませんが、被転送者と転送先がヘアピンされます。

（注）　付加サービスを無効にするには、**voice service voip** または **dial-peer voice xxxx voip** で **no supplementary-service sip moved-temporarily** コマンドか **no supplementary-service sip refer** コマンドを実行します。

次の例は、付加サービスが無効になっているときのコール フローを示しています。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A は電話機 C（Unified CM 電話機、同一または異なる Unified CME 上にある Unified CME 電話機、公衆網電話機のいずれか）に自動転送（[Forward All]、[Forward Busy]、[Forward No Answer]）するように設定されています。

  Unified CME は Unified CM に SIP 302 Moved Temporarily メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

- Unified CM の電話機 B が Unified CME の電話機 A にコールします。電話機 A はコールを電話機 C（Unified CM 電話機、Unified CME 電話機、公衆網電話機のいずれか）に転送します。

  Unified CME は Unified CM に SIP Refer メッセージを送信しませんが、Unified CM 電話機 B と電話機 C の間でコールをヘアピンします。

SIP 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項

- SIP 302 Moved Temporarily メッセージまたは SIP Refer メッセージが Unified CM でサポートされていない場合は、**supplementary-service** を無効にします。無効にしないと、Unified CM はコールを転送先または自動転送先にルーティングできません。
- SIP-to-SIP コール シナリオでは、Refer メッセージがデフォルトで転送者から被転送者に送信され、被転送者は転送先への新しいコールをセットアップします。コールが転送先につながるまで、転送者にはデフォルトでリングバック トーンが聞こえます。Unified CME の **supplementary-service** が無効になっている場合、Unified CME は、被転送者と転送先の間でコールが接続されるとすぐにインバンドのリングバック トーンを提供します。
- プレゼンス サービスは、SIP トランク経由の Unified CM と Unified CME でのみサポートされます。
- OOD-Refer 機能を使用すると、サードパーティ製アプリケーションで SIP REFER メソッドを使用して、Unified CM または Unified CME の 2 つのエンドポイントを接続できます。OOD-Refer を使用する場合は、次の点を考慮してください。
  - Unified CM と Unified CME はどちらも、OOD-Refer 機能が有効になるよう設定する必要があります。
  - 保留、転送、および会議は、OOD-Refer トランザクション中はサポートされませんが、Unified CME によってブロックされることもありません。
  - コール転送がサポートされるのは、OOD-Refer コールが接続状態になった後のみで、コールの接続前はサポートされません。そのため、接続前はコールの transfer-at-alert はサポートされません。
- TLS のシグナリング制御はサポートされますが、SRTP は SIP トランク経由ではサポートされません。
- ビデオは、SIP 電話機でも SIP トランク経由でもサポートされません。
- SIP トランク経由の SRTP は、Unified CM 用 Cisco IOS のゲートウェイ機能です。SRTP サポートは、SIP トランク経由での Unified CM と Unified CME のインターワーキングでは使用できません。

（注）　複数の公衆網接続（Unified CM に 1 つと Unified CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Unified CM エンドポイントと Unified CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

（注）　Cisco Unified CME は、SIP トランクを介した複数の Unified CME 間のビデオ コールをサポートします。この機能は、Unified CME だけを使用する分散型コール処理配置で適用されます。SIP トランクを介した Unified CM と Unified CME との間のビデオ コールはサポートされていません。設定の詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html で入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

分散型コール処理を使用したマルチサイト配置における H.323 経由の Unified CM と Unified CME の相互運用性

分散型コール処理を使用したマルチサイト WAN 配置で、H.323 接続経由の Unified CM と Unified CME の相互運用性を実現する配置オプションは 2 つあります。1 番めのオプションは、Cisco Unified Border Element を Unified CM のフロントエンド デバイスとして配置する方法で、リモートの Unified CME システムとはピアツーピア H.323 で接続します。Cisco Unified Border Element が Unified CM と Unified CME との間のダイヤル プラン解決を実行し、同時に両者間のコール シグナリング メッセージを終端し、再発信します。Cisco Unified Border Element は、Unified CM など、付加サービスの H.450 をサポートしないシステムのためにプロキシ デバイスとして機能し、Empty Capability Set（ECS）を使用して付加サービスを呼び出します。また、Cisco Unified Border Element は、Unified CM クラスタ用の公衆網ゲートウェイとしても動作できるため、公衆網ゲートウェイを別に用意する必要がありません。

2 番めのオプションは、中継ゾーン ゲートキーパー経由で配置する方法です。Unified CM、Unified CME、および Cisco Unified Border Element はすべて、VoIP ゲートウェイ デバイスとして中継ゾーン ゲートキーパーに登録されます。中継ゾーン ゲートキーパーが Unified CM と Unified CME 間のダイヤル プラン解決と帯域幅制限を実行します。また、中継ゾーン ゲートキーパーは、ECS と H.450 との間で相互作用するコール パスに Cisco Unified Border Element を挿入し、付加サービスを呼び出します。中継ゾーン ゲートキーパーと Cisco Unified Border Element の詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください。

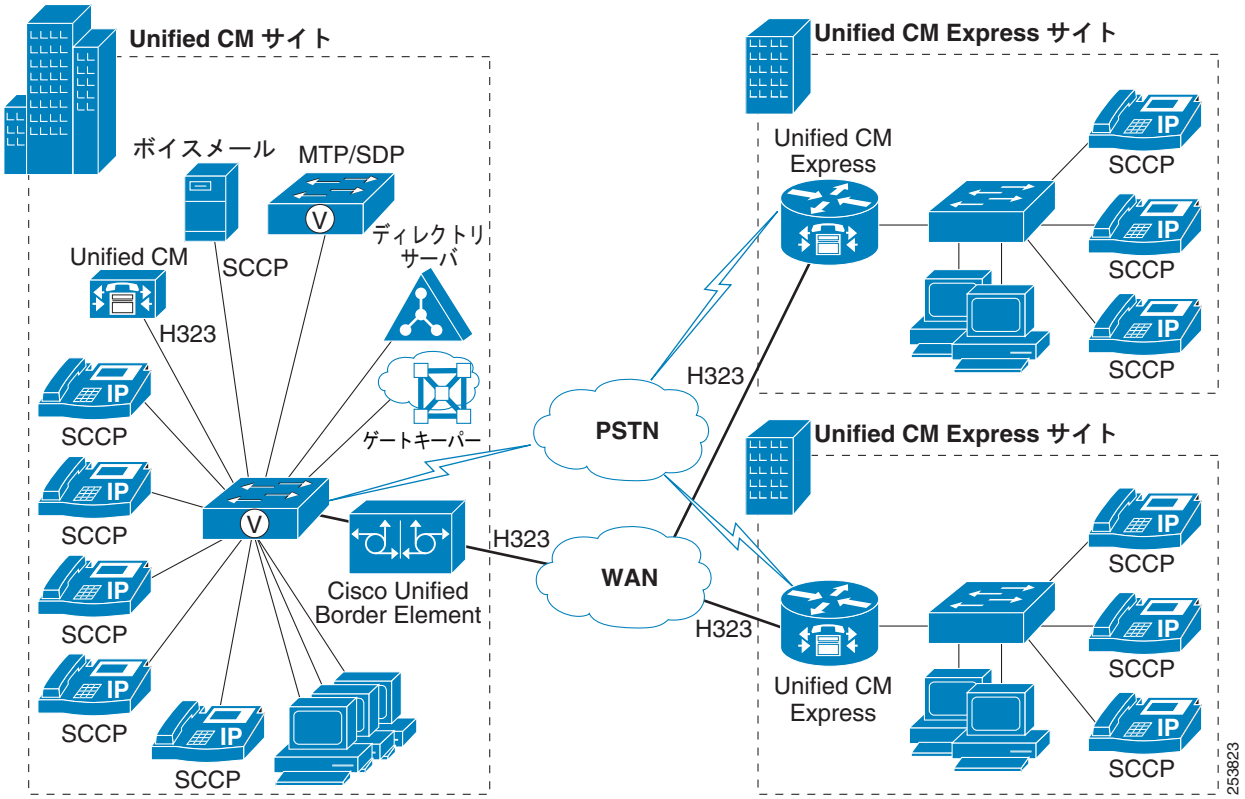
これらの 2 つの配置オプションには、次の相違点があります。

- 1 番めのオプションでは、Cisco Unified Border Element は H.323 ゲートウェイ デバイスとして Unified CM に登録され、2 番めのオプションでは、VoIP ゲートウェイ デバイスとして中継ゾーン ゲートキーパーに登録されます。
- 1 番めのオプションでは、Cisco Unified Border Element が Cisco Unified Border Element の VoIP ダイヤル ピア設定に基づくダイヤル プラン解決を実行し、2 番めのオプションでは、中継ゾーン ゲートキーパーがゲートキーパーのダイヤル プラン設定に基づくダイヤル プラン解決を実行します。
- 1 番めのオプションでは、両方のコール レッグを監視するコール アドミッション制御メカニズムがなく、2 番めのオプションでは、中継ゾーン ゲートキーパーがゲートキーパー ゾーンベースのコール アドミッション制御を実行します。

- 2 番めのオプションでは、中継ゾーン ゲートキーパーは Unified CM のインフラストラクチャ ゲートキーパーとして機能し、Unified CM クラスタ間、Unified CM クラスタと H.323 VoIP ゲートウェイのネットワーク間、および Unified CM クラスタとサービス プロバイダーの H.323 VoIP 転送ネットワーク間のすべてのダイヤル プラン解決および帯域幅制限を管理することもできます。

図 8-18 は、中継ゾーン ゲートキーパーと Cisco Unified Border Element を使用する Unified CM と Unified CME 間の H.323 統合を示しています。

図 8-18　Cisco Unified Border Element または中継ゾーン ゲートキーパーを使用して Unified CM と Unified CME を接続するマルチサイト配置



ベスト プラクティス

この項では、2 番めの配置オプション（中継ゾーン ゲートキーパー）で、図 8-18 に示した配置モデルを使用する場合のガイドラインとベスト プラクティスについて説明します。

- Unified CM と中継ゾーン ゲートキーパーとの間にゲートキーパー制御の H.225 トランクを設定します。Media Termination Point（MTP; メディア ターミネーション ポイント）のリソースがトランクに必要になるのは、Unified CME が 発信 H.323 fast-start コールを開始しようとしたときのみです。
- トランクの両端の H.323 デバイスが、遠端デバイスによって先に TCS が送信されるのを待っていて、H.245 接続が数秒後にタイムアウトになる場合、デッドロック状態が発生しないようにするため、[Wait For Far End H.245 Terminal Capability Set]（TCS）オプションをオフにする必要があります。

- Unified CM サービス パラメータ [Send H225 user info message] を [H225 info for Call Progress Tone] に設定し、Unified CM から Unified CME に H.225 Info message を送信して、リングバック トーンまたは保留トーンを再生できるようにします。
- Unified CM ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、Unified CME を宛先とするコールをゲートキーパー制御の H.225 トランクに送信します。
- Unified CME と Cisco Unified Border Element を H.323 ゲートウェイとして中継ゾーン ゲートキーパーに登録します。
- Cisco Unified Border Element 上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 コール接続を許可します。このコマンドは、Unified CME に対して設定するためのオプションです。Cisco Unity Connection を Unified CME で使用する場合は、**allow-connection h323 to sip** を設定します。
- コール転送や自動転送などの付加サービスでは、2 つのエンドポイントが同じ Unified CME 支店ロケーションに存在する場合に、コールのメディア ヘアピンが発生します。

（注）　2 つの配置オプションにおける設定の違いは、1 番めのオプションでは、Unified CM で Cisco Unified Border Element を H.323 ゲートウェイ デバイスとして設定する必要があることだけです。上記のその他の設定ガイドラインは、どちらのオプションも同じです。

（注）　複数の公衆網接続（Unified CM に 1 つと Unified CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Unified CM エンドポイントと Unified CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

設計上の考慮事項

H.323 配置では、Unified CME はコール転送、H.450.2、および H.450 標準の一部としての H.450.3 を使用した自動転送をサポートします。ただし、Unified CM は H.450 をサポートしません。また、コール転送、自動転送、保留または保留解除などの付加サービスは、Empty Capabilities Set（ECS）を使用して行われます。そのため、コールが Unified CM と Unified CME との間で転送または自動転送されると、Cisco Unified Border Element を使用して、コールはヘアピンされ、ルーティングされます。前の項の 2 つの配置モデルとして説明したように、ゲートキーパーは使用される場合と使用されない場合があります。この項では、H.323 経由の Unified CM と Unified CME の相互運用性の設計上の考慮事項とベスト プラクティスを示します。

コール転送および自動転送などの付加サービス

Unified CME は、H.450.12 プロトコルを使用して H.450.*x* 機能を自動的に検出することで、H.450 をサポートしない Unified CM を自動検出します。Unified CME は、Unified CM と Unified CME 間のコールに VoIP ヘアピン ルーティングを使用します。コールが終端すると、Unified CME は必要に応じてコールを再発信およびルーティングして、Unified CM 電話機からのコールをヘアピンします。

（注）　Unified CME は、Unified CM が H.450 をサポートしないことを検出すると、Unified CME でシグナリングとメディアの両方をヘアピンして、コールをヘアピンします。そのため、コールを WAN を介して転送または自動転送すると、消費される帯域幅の量は 2 倍になります（たとえば、Unified CM 電話機が Unified CME 電話機にコールして、Unified CME 電話機がコールを別の Unified CM 電話機に転送すると、Unified CME は、2 台の Unified CM 電話機間のコールでも、シグナリングとメディアの両

方をヘアピンします)。この WAN での 2 倍の帯域幅消費を避けるために、Cisco Unified Border Element を使用して H.450 タンデム ゲートウェイとして機能させ、コール転送または自動転送などの付加サービスで H.450-to-ECS マッピングを可能にすることを推奨します。

サポートされるコール フロー

Unified CME は Back-To-Back User Agent（B2BUA; バックツーバック ユーザ エージェント）なので、コール フローは SCCP 電話機から SCCP 電話機へ、および SCCP 電話機から SIP 電話機へと機能します。SIP 電話機のコールは H.323 トランク経由で機能しますが、付加機能はサポートされません。

セキュリティ

Unified CME は、TLS を使用するセキュア シグナリングと SRTP を使用するメディア暗号化を提供します。Unified CM はまた、TLS 経由でセキュア シグナリング、および SRTP 経由でセキュア メディアをサポートします。ただし、セキュア Unified CM とセキュア Unified CME との間のインターワーキングはサポートされていません。

ビデオ

Unified CME を使用してビデオ機能を実装する場合は、次の設計上の考慮事項に従ってください。

- Unified CM と Unified CME のすべてのエンドポイントは、ビデオ対応エンドポイントとして設定する必要があります。ビデオ コーデックとビデオ形式は、すべてのビデオ対応エンドポイントで一致する必要があります。
- Unified CM と Unified CME は基本的なビデオ コールをサポートしますが、コール転送や自動転送などの付加サービスは、Unified CM と Unified CME 間のビデオ コールではサポートされません。Unified CME で付加サービスをサポートするには、すべての Unified CME と音声ゲートウェイで H.450 を有効にする必要があります。Unified CM は H.450 をサポートしないため、Unified CM 電話機と Unified CME 電話機間で付加サービスが必要な場合、ビデオ コールは音声専用コールに戻ります。
- 電話会議は音声専用に戻ります。
- ビデオ トラフィックが WAN を通過するには、WAN 帯域幅は 384 kbps の最小ビデオ ビットレートを満たす必要があります。
- ビデオの基本的なコールは SCCP 電話機でのみサポートされ、SIP 電話機ではサポートされません。

ISDN 経由の H.320 ビデオ

ISDN 経由で H.320 ビデオ機能を実装する場合は、次の設計上の考慮事項に従ってください。

- PRI または BRI インターフェイス経由で H.320 エンドポイントに直接接続する場合、Unified CME および Cisco IOS ルータは現在、128 kbps のビデオ コールのみをサポートしています。
- Unified CME および PSTN ゲートウェイで H.320 を有効にして、Unified CM と相互作用するようにするには、音声専用コールと区別するために、ビデオ コールには別個のダイヤル ピアを使用します。Unified CME の **voice-port** 設定で **bear-cap speech** を設定します。
- H.320 は付加サービスをサポートしません。

H.323 経由での Unified CM と Unified CME の相互運用性に関する設計上の一般的な考慮事項

- H.450.12 を使用して Unified CM を自動検出するように Unified CME を設定し、Unified CM 電話機と Unified CME 電話機間のコールをヘアピンします。
- SCCP-to-SCCP コールまたは SCCP-to-SIP コールの場合は、H.323 トランクを Unified CM と Unified CME との間に配置できます。

- Unified CME は、TLS を使用するセキュア シグナリングと SRTP を使用するセキュア メディアをサポートしますが、会議コール フローは保護できません。さらに、Unified CM 電話機と Unified CME 電話機間のセキュリティの相互運用性もサポートされていません。
- ビデオを配置するのは SCCP 電話機用（基本的なコールのサポートを使用）で、SIP 電話機用ではありません。
- MTP 機能はビデオと互換性がありません。ビデオ コールを機能させるには、MTP 機能を無効（オフ）にする必要があります。
- Unified CM と Unified CME 間の IP 接続が正常に機能することを確認します。
- Unified CME の各ローカル ゾーンと Unified CM のロケーション（ローカル SCCP）で、ローカル ビデオのセットアップが正常に機能することを確認します。
- 既存の音声ダイヤル プランのインフラストラクチャを使用します。
- ビデオ トラフィック シェーピングの場合は、次のガイドラインに従ってください。
  - CoS 4 を使用するビデオ コールのビデオ チャネルと音声チャネルが、リップシンクを維持し、ビデオと音声専用コールを区別するようにします。
  - 音声トラフィックとビデオ トラフィックを異なるキューに配置します。
  - 音声トラフィックとビデオ トラフィックに Priority Queuing（PQ; プライオリティ キューイング）を使用します。音声専用コールとビデオ（音声ストリーム + ビデオ ストリーム）コールには、分類に基づいて 2 つの異なるポリシーが必要です。ビデオ コールの音声ストリームには、ビデオ コールのビデオ ストリームと同じマークが付けられているため、ビデオ コールの音声コールは保護されています。
- ビデオは、帯域幅が 768 kbps 未満のリンクには配置しないでください。
- リンク速度が 768 kbps 以上で、オーバーサブスクリプションを防止する適切なコール アドミッション制御を使用している場合は、PQ にビデオ トラフィックを配置しても、音声パケットの遅延が大幅に改善されることはありません。
- スピードが 768 kbps 以上の場合はフラグメンテーションを設定する必要はありません。
- ビデオ パケットには cRTP は推奨しません（ビデオ パケットは大きいため、cRTP はビデオには役立ちません）。
- 音声トラフィックとビデオ トラフィックがリンク容量に占める割合が 33% を超えないようにします。
- ビデオ帯域幅を計算する場合、オーバーヘッドを考慮して、コールの合計ビデオ データ レートに 20% を加算します。

H.323 を使用して Unified CME を Unified CM に統合する方法の詳細については、次の Web サイトで入手可能な『*Cisco Unified CME Solution Reference Network Design Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_implementation_design_guides_list.html

CHAPTER 9

ダイヤル プラン

ダイヤル プランは、Unified Communications システムの重要な要素の 1 つであり、すべてのコール処理エージェントにとって不可欠となる部分です。概説すると、ダイヤル プランは、コールをどのようにルーティングするかをコール処理エージェントに指示する役割を果たします。具体的には、ダイヤル プランは次の機能を実行します。

- エンドポイントのアドレッシング

  システム内部の宛先への到達は、すべてのエンドポイント（IP Phone、FAX マシン、アナログ電話機など）とアプリケーション（ボイスメール システム、自動アテンダント、会議システムなど）にディレクトリ番号（DN）を割り当てることで実現しています。

- パスの選択

  発信側デバイスによっては、同じ宛先に到達する場合でも、複数のパスから選択できます。また、プライマリ パスが使用不可になっている場合にはセカンダリ パスを使用できます。たとえば、IP WAN に障害が発生した場合は、コールを公衆網を介して透過的に再ルーティングできます。

- コール特権

  特定の宛先へのアクセスを許可または拒否することによって、複数のデバイス グループにそれぞれ別のサービス クラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の公衆網宛先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に公衆網アクセスできるようにします。

- 番号操作

  特定の状況では、ダイヤルされたストリングをコールのルーティング前に操作する必要があります。たとえば、オンネットのアクセス コードを使用してダイヤルされたコールを公衆網を通じて再ルーティングするときや、短縮コード（オペレータにつなぐ場合の 0 など）を内線番号に展開するときです。また、番号操作は、ユーザのローカル ダイヤリング手順を、コールのパスを選択するために使用されるグローバル ルートに適合させるためにも使用されます。たとえば、フランスのユーザは、New York の番号にコールする場合に 0 00 1 212 555 1234 のようにダイヤルします。Chicago にいる発信者は、同じ番号にコールする場合に 9 1 212 555 1234 とダイヤルします。これら両方のローカル化されたユーザ入力は、+1 212 555 1234 というグローバル形式に変換され、コールのパスの選択に単一のルートが使用されます。

- コールのカバレッジ

  特殊なデバイス グループを作成し、特定のサービスの着信コールを複数のルール（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理できます。この章で説明するダイヤル プラン情報は、Unified Communications の任意の配置モデルに当てはまります。特に、マルチサイト システムを配置する場合、システム設計者は、サイト固有のダイヤリング手順に加えて、ユーザの特定のグループに対してゲートウェイを使用するなどの、サイト固有のコールのルーティングについて特別に注意する必要があります。

この章では、システム設計者が、連絡先からのダイヤル、コンピュータやスマート フォンからのクリックコール アクション、モビリティ関連機能の採用などの、コンピューティング テクノロジーとテレフォニーがより緊密に統合された新機能を利用しつつ、テレフォニー ユーザの従来のダイヤリング手順に対応するダイヤル プランを設計するために役立つ情報を示します。この章では、次の主要な領域に関する情報を示します。

- 「プランニングの考慮事項」（P.9-4）

  この項では、IP テレフォニー ダイヤル プランのプランニングに関係するプロセスを詳しく説明します。取り扱う範囲は、内線番号に使用される桁数から、企業内部のダイヤル プラン アーキテクチャ全般までです（前提条件：ダイヤル プラン一般について、ある程度の知識があること）。

- 「設計上の考慮事項」（P.9-11）

  この項では、マルチサイト IP テレフォニー ネットワーク、エンドポイントのアドレッシング方式、サービス クラスを作成するためのアプローチ、およびコール カバレッジ機能について、設計と配置のガイドラインを示します（前提条件：Cisco Unified Communications Manager および Cisco IOS の操作知識があることを推奨）。

- 「ダイヤル プランの要素」（P.9-73）

  この項では、Cisco Unified Communications ダイヤル プランの要素について詳しく説明します。取り扱うトピックには、コール ルーティングのロジック、コール特権、および各種シスコ製品における番号操作の方法が含まれています（前提条件：Cisco Unified Communications Manager および Cisco IOS の操作知識があることを推奨）。この項は、製品固有のマニュアルの代替となるものではなく、また Cisco Unified Communications Manager ヘルプ ファイルに記載されているすべての情報が示されているわけでもありません。この項では、ここで示されている設計関連の概念を理解するために不可欠な、いくつかの基本的な機能的要素について重点的に説明します。

詳細については、次の Web サイトから入手可能な『*Cisco Unified Communications Manager System Guide*』、『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』、およびその他の製品マニュアルを参照してください。

http://www.cisco.com

この章の新規情報

表 9-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

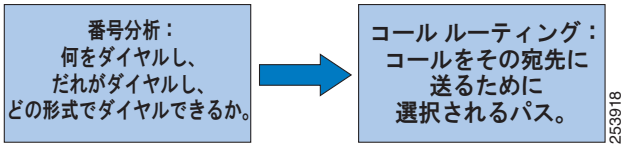
表 9-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
+ ダイヤリング	「電話機での + ダイヤリングのサポート」（P.9-75）	2011 年 2 月 28 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）3000	「Unified CMBE 3000 のダイヤル プランに関する考慮事項」（P.9-143）	2011 年 2 月 28 日
Intercompany Media Engine（IME）	「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）	2010 年 4 月 2 日
Service Advertisement Framework（SAF）Call Control Discovery（CCD; コール制御ディスカバリ）	「コール制御ディスカバリ」（P.9-23） 「Service Advertisement Framework（SAF）Call Control Discovery（CCD）」（P.9-141）	2010 年 4 月 2 日

ダイヤル プランのアーキテクチャ

図 9-1 に、Cisco Unified Communications Manager（Unified CM）に基づくダイヤル プランの基本的なアーキテクチャを示します。

図 9-1　　ダイヤル プランの基本的なアーキテクチャ



番号分析機能によって、ユーザ、ゲートウェイ、またはアプリケーションに対してどのコールが許可されるかが制御されます。コール特権（サービス クラスとも呼ばれます）は、この機能に実装されます。番号分析は、次の基本的な構成要素を使用して実装されています。

- パターン（ディレクトリ番号パターンやトランスレーション パターンなど）

  パターンとは、電話番号の数値表現であり、これに一致するとコール ルーティングがトリガーされます。

- パーティション

  パーティションは、パターンを論理グループに分割するために使用されます。たとえば、パーティションを使用すると、1000 に設定された 2 つの内線番号を異なるパーティションにプロビジョニングできます。

- コーリング サーチ スペース

  コーリング サーチ スペースを使用すると、（電話機などの）デバイスがアクセス可能なパターンのグループを制御できます。たとえば、あるサイトのデバイスに対して、内線番号 1000 を含むローカル パーティションへのアクセスを許可する一方で、異なるサイトの内線番号 1000 へのアクセスを禁止できます。

コール ルーティング機能によって、コールのパス選択が制御されます。この機能において、特定のコールを伝送するための IP トランク、公衆網トランク、または従来型の PBX への接続が選択されます。また、コール ルーティング機能では、たとえば帯域幅を使用できないため、またはネットワークの特定の部分が利用できないために IP 接続を使用できない場合に、最初の選択肢としての IP 接続からバックアップ用の選択肢としての公衆網接続にコールを自動的にフェールオーバーできます。

これら両方の機能において、Unified CM には、システム設計者用の数多くのツールが用意されています。システム設計者は、これらのツールを使用して、番号操作を有効にしたり、さまざまな状況におけるコール処理の制御を実行したりできます。たとえば、システム管理者は、電話機が異なるサイト間をローミングする際に許可するコールのタイプ、電話機が通話中または呼出音は鳴るが応答しない場合のコールの処理方法、あるいはすべてのコールを自動転送する場合に電話機が使用できる転送先を設定できます。

このアーキテクチャの個別機能の基本的要素は、複数のマニュアルで説明されています。製品固有のマニュアル、および Unified CM のヘルプ ファイルには、機能に関する最も基本的な事項が説明されています。この章の「ダイヤル プランの要素」（P.9-73）の項では、機能についてさらに詳細に説明しています。このマニュアルの「設計上の考慮事項」（P.9-11）の項では、システム設計者がダイヤル プランを設計する場合に考慮する必要があるトップダウンのアーキテクチャ情報を示します。

ダイヤル プランのハイ アベイラビリティ

Cisco Unified CM では、ダイヤル プラン機能は、Unified CM サーバのクラスタリング機能によってデフォルトで可用性が確保されています。すべてのダイヤル プラン設定は、他の Unified CM サービスが冗長化されるのと同じメカニズムで冗長化されます。具体的には、電話機、ルート リスト、およびゲートウェイの制御に Unified Communications Manager グループが使用されて、1 つの Unified CM サーバで単一の障害が発生してもダイヤル プラン機能の可用性が確保されます。

外部トランクに依存するコール パスでは、代替ルートを使用することによってより高いレベルの可用性を確保できます。たとえば、ルート リストを使用して、特定のオフクラスタの宛先への 1 次パス、2 次パス、および 3 次パスを確立できます。優先順位の高い選択肢（IP トランクなど）が使用できない場合は、コールが正常に確立されるか、または事前に設定されたすべての選択肢が試みられるまで、次に優先順位の高い選択肢が試みられます。

オンクラスタ エンドポイント間のコール（2 つの IP Phone 間のコールなど）において、ネットワーク障害のために IP パスが使用できない場合には、Call Forward Unregistered 機能が呼び出されて、公衆網などの代替ネットワークを経由してコールをルーティングできます。ネットワークの帯域幅が不足しているために IP パスが使用できない場合には、Automated Alternate Routing（AAR; 自動代替ルーティング）機能が呼び出されて、代替ネットワークを経由してコールがルーティングされます。

さらに高いレベルの可用性を確保するには、H.323 ゲートキーパーや SIP プロキシなどの外部ダイヤル プラン解決サブシステムをプロビジョニングする場合にも、適用可能な冗長性機能を設定する必要があります。

ダイヤル プランのキャパシティ プランニング

通常、ダイヤル プランの設定は、ゲートウェイ数、CTI 接続数、コール試行（BHCA）のレートなどの、キャパシティに影響がある他の Unified CM 設定と比較して、キャパシティへの影響は大きくありません。Cisco Unified Communications Sizing Tool では、システム プロビジョニングの計算において、ダイヤル プラン情報が組み込まれます。シスコの従業員および代理店は、適切なログイン認証を経て http://tools.cisco.com/cucst からこのツールを利用できます。

プランニングの考慮事項

ダイヤル プランは、テレフォニー システムの根本となる構成要素です。ユーザがどのように宛先に到達するかを規定する規則を定義しているので、まさにユーザ エクスペリエンスの中心部分になります。このような規則には、次のものがあります。

- 内線番号ダイヤリング：システム上の内線番号に到達するために、何桁ダイヤルする必要があるか。
- 内線番号アドレッシング：内線番号の識別に何桁を使用するか。
- ダイヤリング権限：特定のタイプのコールを許可するかどうか。
- パスの選択：たとえば、オンネット コールには IP ネットワークを使用する。または、国内公衆網コールにはあるキャリアを使用し、国際コールには別のキャリアを使用する。
- ネットワークが輻輳した場合の代替パス自動選択：たとえば、優先使用する国際キャリアがコールを処理できない場合に、国際コールに国内キャリアを使用する。
- 特定番号のブロック：たとえば、有料情報サービスへのコール。
- 着信番号の変換：たとえば、10 桁の番号としてダイヤルされたコールの最後の 5 桁のみを保持する。
- 発信番号の変換：たとえば、公衆網に発信するとき、発信者の内線番号をオフィスのメイン番号に置き換える。

IP テレフォニー システムに適したダイヤル プランは、従来の TDM テレフォニー システム用に設計するダイヤル プランと基本的には違いません。ただし、IP ベースのシステムによって、ダイヤル プランの構造にいくつかの新しい選択肢が生まれています。たとえば、個々のサイトにいるテレフォニー ユーザは、以前はそれぞれ別の独立 TDM システムによって処理されていましたが、IP ベースのテクノロジーは柔軟であるため、1 つの IP ベース システムに包含できるようになりました。このような新しい選択肢が IP ベースのシステムによってもたらされたため、ダイヤル プランの見方を再検討する必要があります。この項では、ダイヤル プランの設計にかかわる要件を正しく導き出すために、システムの設計担当者が検討する必要のあるいくつかの要素について説明します。

ダイヤルされたパターンの認識

ユーザが電話機でダイヤルする番号並びは、一般的にパターンに従っています。たとえば、多くの企業では、同じオフィス ロケーション内で行われるコールに 5 桁の短縮ダイヤル パターンを使用しています。また、多くの企業では、外部へのダイヤリングを表すのに 1 桁のアクセス コードを用い、その直後に何桁かの番号をダイヤルして、ローカル公衆網の番号または長距離公衆網の番号に到達します（たとえば、ローカル番号への到達には 9 に続く 7 桁の番号を使用し、長距離の通話先への到達には 9 の後に 1 と 10 桁の番号をダイヤルします）。

システム管理者は、このようなパターンのシステムによる認識を計画し、あらかじめ決められたパターンに対応するストリングが検出されると同時にシステムが素早く反応し、ユーザがダイヤル後に遅延を感じない（または、その遅延が最小になる）ようにする必要があります。

Skinny Client Control Protocol（SCCP）を使用する電話機、およびダイヤル時に Key Press Markup Language（KPML）を使用する SIP 電話機の場合、Cisco Unified Communications Manager（Unified CM）にパターン認識を実装するには、ルート パターン、トランスレーション パターン、電話機の DN などを設定します。ユーザが 1 つの桁をダイヤルするたびに、電話機から Unified CM へシグナリング メッセージが送信され、一致するパターンを認識する差分処理が行われます。ユーザ入力に含まれる個々のキー操作が収集されるたびに、Unified CM の番号分析は次のような適切なユーザ フィードバックを提供します。

- 電話機が最初にオフフックになったときにダイヤル トーンを再生する。
- 番号がダイヤルされたらダイヤル トーンを停止する。
- 特定の番号のシーケンスがダイヤルされた場合、たとえば、オフネット アクセス コードの 9 がダイヤルされたときなどに、2 次ダイヤル トーンを提供する。

番号のダイヤリングが完了すると、Unified CM はユーザ フィードバックとしてコール プログレス トーンを提供します。たとえば、通話先がアラート段階ならばリングバック トーン、通話先が無効であればリオーダー トーンを再生します。

Session Initiation Protocol（SIP）を実行する IP Phone には、設定に SIP ダイヤル規則というパターン認識命令を使用できます。この命令を使用すると、電話機内でパターン認識の大部分のタスクを実行できます。あるパターンが認識されると、SIP 電話機はユーザの入力に対応する番号にコールを発信するために、Unified CM に発信要求を出します。この動作は SIP INVITE と呼ばれ、SCCP プロトコルを実行している IP Phone からのコールと同じように、Unified CM のダイヤル プランによる制御対象となります。ただし、Unified CM の番号分析は完全なダイヤル ストリングを使用して行われます（ユーザが入力したすべての桁が、1 つのブロックとして Unified CM に渡されて処理されます）。この動作モードでは、番号ストリングのダイヤル中のユーザ フィードバックは、電話機が提供できるものだけに制限されます（「SIP ダイヤル規則」（P.9-80）を参照）。ストリングが合成された後も、Unified CM はユーザ フィードバックとしてコール プログレス トーンを提供できます。

ダイヤリング手順によるグループ分け

ほとんどのテレフォニー ユーザは、ローカル手順に従って電話番号をダイヤルするのに慣れています。これらはオフィス ロケーション内の宛先へのコール（サイト内コール）、企業内の宛先で異なるサイト間（サイト間コール）、企業外部の宛先（オフネット コール）に適用されるさまざまなダイヤリング ルールで構成されます。これらのさまざまなタイプのコールで使用される形式は、ユーザのプリファレンスおよび地域の公衆網のダイヤリング要件によって異なります。

オンネットとオフネットのダイヤリング

同じテレフォニー ネットワーク上で発信され、終端するコールは、オンネットワーク（オンネット）と見なされます。これとは逆に、A 社で発信され、B 社で終端するコールは、通常は最初に A 社のネットワーク、次に公衆網、最後に B 社のネットワークというように、複数のテレフォニー ネットワークを通じてルーティングする必要があります。発信者から見ると、コールはオフネットワーク（オフネット）でルーティングされています。着信側から見ると、コールはオフネットで発生しています。

TDM システムでは、PBX または Centrex システムがテレフォニー システムのオンネット境界になります。TDM システムは、通常は 1 つのサイトの外側まで伸びていることはありません。伸びている場合も、その TDM システムは、大規模なシステム ハブの外周上に配置されていないサイトを含んでいないのが普通です。

IP テレフォニーの重要な特性の 1 つは、オンネットと見なすことのできるコール境界を拡張する機能です。たとえば、6 つの支店を保有している企業に所属するテレフォニー ユーザが、着信側が同じサイトにいる場合は短縮ダイヤル（4 桁の内線番号など）を使用して同僚にコールし、他のサイトにいる別の同僚にコールするときは、完全な公衆網番号をダイヤルしているとします。IP ベース システムを使用すると、すべてのユーザが同じ IP ネットワークで処理されるため、6 つの支店を 4 桁の短縮ダイヤル プランで経済的に結ぶことが可能になります。IP ネットワークを優先パスとして使用し、IP ネットワークが輻輳した場合のセカンダリ パスとして、公衆網への自動オーバーフローを使用します。

短縮ダイヤル

公衆網から直接到達可能な、ダイヤルイン（DID）機能を使用した内線番号があるとします。オフネットの公衆網発信者が DID 内線番号に到達するには、完全修飾公衆網番号（たとえば、1 415 555 1234）をダイヤルする必要があります。しかし、オンネットの発信者については、DID 番号の最後のいくつかの桁をダイヤルするだけでこの内線番号に到達する機能を利用することを考えています。4 桁の短縮ダイヤル プランを使用すると、この例のオンネットの発信者は、1234 のみダイヤルすればこの内線番号に到達します。

ダイヤリングは通常、次の 4 種類に分けられます。

- サイト内、オンネットの内線番号ダイヤリング

  多くのシステムで、サイト内での 4 桁または 5 桁のダイヤリングに対応しています。たとえば、カリフォルニア州の San Jose にいるシスコ従業員は、5 桁の番号ストリング 64000 を使用して、シスコの受付番号にコールできます。

- サイト間、オンネットの内線番号ダイヤリング

  たとえば、すべてのシスコ オフィスのシスコ従業員は San Jose の受付番号に 8 526 4000 でダイヤルできます。数字の 8 は、サイト間アクセス コードです。52 は San Jose のサイト コードです。

  この形式は、オンネットでコールをルーティングする、オフネット形式を使用する代替方法よりも短いです（たとえば、カナダにいるシスコ従業員が、オンネットでコールをルーティングして、9 1 408 526 4000 とダイヤルして San Jose のシスコの受付番号に到達できるようになります）。ダイ

ヤリング形式はオフネットの宛先への到達に使用される形式によく似ていますが、システム内のオフネット形式でダイヤルされたオンネットの宛先へのコールを保持するようにシステムは設定されています。

- サイト間、オフネット ダイヤリング

  サイト間のコールのルーティングは公衆網に渡すことができます。たとえば、San Francisco のあるサイトからの、New York の別のサイトへのコールは、上記で説明したオンネットまたはオフネット形式のいずれかでダイヤルできますが、公衆網を介してオフネットでルーティングされます。

- オフネット ダイヤリング

  宛先がオフネットで、会社のダイヤル プランの外部にあるコールの場合、Unified Communications システムでは、ユーザにとってシンプルで、地域で有効なダイヤリング形式を提供する必要があります。

内線ダイヤリングの重複の防止

テレフォニー システムは、どの内線番号にも明確な方法で到達できるように設定する必要があります。この目標を達成するには、ダイヤル プランが次の要件を満たす必要があります。

- すべてのオンネット内線ダイヤリングを、グローバルに一意なものにする。たとえば、4 桁の短縮オンネット ダイヤル プランを使用するシステムで、サイト A とサイト B のどちらの内線番号についても、サイト C から 4 桁のみダイヤルして到達することが要件である場合、サイト A に内線番号 1000 があり、サイト B の別の内線番号も 1000 である状態は許されません。
- 個々のダイヤル ストリングは、部分的にも重複していない。
  - たとえば、4 桁の短縮ダイヤル プランにおいて、9 をオフネット アクセス コードとして使用する場合（公衆網コールを発信する場合など）、内線番号を 9XXX にすることはできません。このように設定すると、コールがすぐにはルーティングされない状況が発生します。たとえば、ユーザが 9141 をダイヤルしたとします。システムは、追加の数字が入力されるか（ユーザが 9 1 415 555 1234 をダイヤルしようとしている場合など）、桁間タイムアウトに達するまで待機し、その後でコールを内線番号 9141 にルーティングします。同様に、オペレータ コード（たとえば 0）を使用する場合にも、0XXX の内線番号範囲全体を 4 桁の定型ダイヤル プランから除外する必要があります。
  - 長さが異なっていても、ストリングが重複していることは許されません。たとえば、システムで内線番号 1000 と 10000 を使用すると、1000 にダイヤルする場合、ユーザは桁間タイムアウトに達するまで待たされることになります。

ダイヤリング ストリングの長さ

内線番号にダイヤルするときの必要桁数は、ダイヤル可能な内線番号の数によって決まります。たとえば、4 桁の短縮ダイヤル プランでは、内線番号が 10,000 個（0000 ～ 9999）を超える場合には対応できません。0 と 9 をオペレータ コードおよびオフネット アクセス コードとしてそれぞれ予約する場合、この番号範囲は、さらに 8,000 個（1000 ～ 8999）まで減ります。

固定オンネット ダイヤル プラン

ダイヤル プランは、システム内のすべての内線番号に一定の方法で到達するように設計できます。つまり、任意のオンネット発信地点から、特定の内線番号に一定の桁数で到達できます。ユーザにとって簡潔であるため、定型ダイヤリングを使用することを推奨します。各種のオンネット ロケーションから発信するときに、番号をダイヤルするための方法をユーザがいくつも覚えておく必要がありません。

たとえば、任意のオンネット ロケーションから 1234 をダイヤルすると電話機 A に着信するとします。この場合、発信側の電話が同じオフィスまたは別のサイトのどちらにあっても、企業のダイヤル プランは定型と見なすことができます。

企業のサイト数が少ない場合は、このアプローチを容易に採用できます。企業の内線番号とサイトの数が多くなるほど、定型ダイヤル プランを設計するときに次の点が問題になってきます。

- 内線番号の数は、ダイヤル プラン用に予定した桁数で対応できる範囲を超える場合もあります。たとえば、8,000 個（内線番号 0XXX と 9XXX を除外するものと想定）を超える内線番号が必要になった場合は、5 桁以上使用する短縮ダイヤル プランが必要になります。
- オンネット短縮内線番号を DID 番号と同じものにする場合、地域通信事業者から新しい DID 範囲を取得するときに、その範囲が既存のオンネット短縮ダイヤルの範囲と競合してはなりません。たとえば、4 桁の定型短縮ダイヤル プランを使用しているシステムに、DID 範囲 415 555 1XXX があるとします。DID 範囲 650 556 1XXX の取得も検討している場合は、オンネット ダイヤリングの桁数を 5 に増やすことが望ましくなります。この例では、5 桁のオンネット範囲 51XXX と 61XXX は重複することがありません。
- ほとんどのシステムでは、一定の範囲をオフネット アクセス コードとオペレータ ダイヤリング用に除外する必要があります。9 と 0 が予約コードになっているシステムで、9 または 0 で始まるオンネット内線番号ダイヤリングに対応できるダイヤル プランは、（定型もそれ以外も）存在しません。つまり、ダイヤル プランで最初の数字として 9 または 0 を使用する必要がある場合は、最初の数字が 9 または 0 である DID 範囲を使用できません。たとえば、5 桁の短縮ダイヤル プランを使用する場合、DID 範囲 415 559 XXXX（およびこのサブセット）は使用できません。この例では、代替策として、短縮ダイヤルの長さを 6 桁以上に増やすか、末尾の 5 桁が 9 で始まる DID 範囲を使用しないようにするという方法があります。または DID 番号がオンネットの内線番号と一致させる必要もありません。

桁数を選定し、必要な範囲（たとえば、9 または 0 で始まる範囲）を除外したら、残りのダイヤリング スペースをすべてのサイトに分配する必要があります。

ほとんどのシステムでは、2 つの範囲を除外する必要があります。このため、ダイヤル範囲の先頭となる可能性が残っている数字は、8 つです。表 9-2 では、一般的な 4 桁の定型ダイヤル プランにおける、ダイヤリング スペースの分配例を示しています。

表 9-2　一般的な 4 桁定型ダイヤル プランでの番号割り当て

範囲	用途	DID 範囲	DID 以外の範囲
0XXX	除外（0 はオフネット アクセス コードとして使用される）		
1XXX	サイト A の内線番号	418 555 1XXX	適用対象外
2XXX	サイト B の内線番号	919 555 2XXX	適用対象外
3XXX	サイト C の内線番号	415 555 30XX	3[1-9]XX
4[0-4]XX	サイト D の内線番号	613 555 4[0-4]XX	適用対象外
4[5-9]XX	サイト E の内線番号	450 555 4[5-9]XX	適用対象外
5XXX	サイト A の内線番号	418 555 5XXX	適用対象外
6XXX	サイト F の内線番号	514 555 6[0-8]XX	69XX
7XXX	将来的にサポート	XXX XXX 7XXX	7XXX
8XXX	将来的にサポート	XXX XXX 8XXX	8XXX
9XXX	除外（9 はオフネット アクセス コードとして使用される）		

表 9-2 の例では、さまざまなサイトが次の方法に従って番号を割り当てられています。

- サイト A（企業の本社）では、必要な内線番号が 1,000 個を超えるため、2 つの番号範囲（1XXX と 5XXX）全体を確保しています。対応する DID 範囲も、このサイトの地域通信事業者から取得する必要があります。
- サイト B は、1 つの範囲全体（2XXX）を割り当てられているため、内線番号を 1,000 個まで使用できます。
- サイト C も 1 つの範囲全体を割り当てられていますが、100 個の DID 内線番号（415 555 30XX）と 900 個の DID 以外の内線番号に分割されています。DID 内線番号がさらに必要になった場合は、DID 以外の範囲にある、まだ割り当てられていない番号を使用できます。
- サイト D と E は、4XXX 範囲からそれぞれ 500 個ずつ番号を割り当てられています。対応する DID 範囲は、それぞれのサイトの 4XXX 範囲の部分と一致している必要があります。DID 範囲がサイトごとに異なっているため（おそらく、別の公衆網サービス プロバイダーから取得したことが原因）、サイト間で範囲を分割するには、密接な連携作業が必要です。特定の範囲内で割り当てられるサイトの数が多くなるほど、範囲全体をすべて使用することは困難になり、場合によっては不可能になります。
- サイト F の範囲は、900 個の DID 番号（6[0-8]XX）と 100 個の DID 以外の番号（69XX）に分割されています。
- 範囲 7XXX と 8XXX は、将来の使用に備えて予約されています。

新しいダイヤル プランを実装する場合、プラン立案者の主な目標の 1 つは、電話番号の変更が必要になるのを避けることです。また、既存の電話システムで内線番号範囲が重複している場合、過去に問題がなくても、定型ダイヤル プランでは許容されない場合があります。

可変長のオンネット ダイヤル プラン

サイトの数が多いシステムや、サイトの内線番号範囲が重複しているシステムでは、次の特性を備えた可変長ダイヤル プランを使用すると効果的です。

- サイトの内部では、オンネット内線番号へのコールに対して、短縮ダイヤル（4 桁の内線番号など）を引き続き使用できる。
- サイト間では、ユーザはアクセス コードをダイヤルし、次にサイト コードと宛先のオンネット内線番号をダイヤルする。
- オフネット コールの場合は、アクセス コードの次に公衆網番号をダイヤルする必要がある。

アクセス コードとダイヤル コードを使用すると（表 9-3 を参照）、定型短縮ダイヤル プランであれば重複となる内線番号を、オンネット ダイヤル プランで区別できるようになります。

表 9-3　サイト コードの一般的な使用方法

サイト コード	範囲	用途	DID 範囲	DID 以外の範囲
1	1XXX	サイト A の内線番号	418 555 10XX	1[1-9]XX
2	1XXX	サイト B の内線番号	919 555 1XXX	適用対象外
3	1XXX	サイト C の内線番号	907 555 1XXX	適用対象外

表 9-3 では、サイト A、B、C はそれぞれ独自に 4 桁範囲 1XXX を割り当てられています。従来のテレフォニー システムでは、サイト A からサイト B へのコールはオフネット コールとしてルーティングする必要がありました。新しいシステムでは、これらのコールをオンネット コールとしてダイヤルできます。

サイト A からは、ユーザは 1234 をダイヤルするだけで内線番号 1234 に到達できます。一方で、サイト B からサイト A の内線番号 1234 に対して、サイト B にある内線番号 1234 と競合することなく到達するには、ダイヤル プラン側で対応する必要があります。このため、各サイトにサイト コードが割り当てられています。

サイト B から、単にサイト A のコードを目的の内線番号と組み合せてダイヤルすることだけでは不十分です。この場合、11234 はサイト B の内線番号 1123 と部分的に重複しているため、桁間タイムアウトの問題が発生します。代わりに、サイト間オンネット アクセス コードとして 8 を割り当てると、サイト B から 81234 をダイヤルしてサイト A の内線番号 1234 に着信できるようになります。

オンネットのオフサイト内線番号にダイヤルするために必要な桁数は、次の要素によって決まります。

- サイト間アクセス コードに使用する 1 桁
- サイト コードに使用する N 桁（N は、必要となるサイト コードの数に見合う数値。たとえば、システムに 13 のサイトがある場合、サイト コードには少なくとも 2 桁が必要）
- 宛先サイトのローカル ダイヤル プランで必要となる桁数

たとえば、システムに 75 のサイトがあり、各サイトが 4 桁の短縮ダイヤルを使用している場合は、8 + SS + XXXX という形式が必要になります。8 はオンネット アクセス コード、SS は 2 桁のサイト コード、XXXX は 4 桁の内線番号で、合計 7 桁です。

オンネットとオフネットのアクセス コード

ほとんどの企業のテレフォニー システムでは、オフネットの宛先にコールを振り分けるためのオフネット アクセス コード専用として、1 つの数字（たとえば 9）を割り当てることが一般的です。可変長のオンネット ダイヤル プランでは、他のサイトにあるオンネット内線番号宛てのコールをダイヤルするために、オンネット アクセス コードとして、振り分け用の数字（たとえば 8）がもう 1 つ必要です。これらの 2 つのアクセス コードをオペレータ アクセス コード（たとえば 0）とともに使用するので、ダイヤルされたストリングの先頭の数字となる可能性のある 10 個の数字からは、3 つが暗黙的に除外されます。この制限事項は、次の両方の理由から、好ましいものとは言えません。

- ユーザは、オンネットとオフネットの違いを理解し、適切なアクセス コードを選択する必要がある。
- 3 つのダイヤリング範囲全体を除外することによって、著しい制約や、一部の割り当て済み内線番号範囲との競合が生じるおそれがある。たとえば、サイトですでに 8 で始まる短縮ダイヤル範囲を使用している場合、この数字をアクセス コードとして使用するには、変更作業が必要になります。

同じオフネット アクセス コード（たとえば 9）をすでにすべてのサイトで使用しているシステムでは、同じコードをオフネットとオンネットの両方のオフサイト宛先に使用することを推奨します。このアプローチには、主に次の 2 つの暗黙的要件があります。

- 部分的な重複や待ちが発生することを避けるには、アクセス コードの後に続く桁数を一定にする必要がある。
- テレフォニー システムは、ダイヤルされるすべてのオンネット番号をオフネット番号として認識し、IP ネットワーク経由でルーティングできる必要がある。このタスクは、Unified CM クラスタが 1 つしかない小規模システムの場合は単純ですが、複数の Unified CM クラスタがある大規模システムでは複雑なものになります。

事前の計画

IP ベースのシステムを実装するときは、ユーザの普段の操作手順を変更する必要が生じる場合もあります。新しいシステムのプランニングでは、この実装をできる限りユーザから見えないようにすることが望ましいのですが、それぞれ別のテレフォニー システム上にあった複数のサイトの統合に対応するには、ダイヤリング手順の調整が必要になることもあります。たとえば、企業全体にわたる新しいグローバルなダイヤル プランに対応するには、ユーザが他のサイトにいる別のユーザに到達する方法、サイト内コールに使用している桁数、ときには内線番号までも変更することが必要な場合もあります。ユーザが何度もダイヤル プラン変更を経験することを避けるには、企業規模の拡大を見越しておくようにします。企業が成長すると、複数のダイヤリング リージョンへのサイトの追加、オンネット内線番号の必要数の増加、公衆網番号の再割り当て（たとえば、エリア コードの分割など）、他国への事業展開が発生する可能性があります。

設計上の考慮事項

この項では、マルチサイト配置について、ダイヤル プランの設計に関する次の考慮事項について説明します。

- 「グローバル化デザイン アプローチ」（P.9-12）では、Cisco Unified Communications Manager のグローバル化ダイヤル プラン機能を使用した配置に当てはまるガイドラインとベスト プラクティスを示します。
- 「コール制御ディスカバリ」（P.9-23）では、クラスタが、Service Advertisement Framework（SAF）Call Control Discovery（CCD; コール制御ディスカバリ）サービスによって、それぞれにホストされた DN 範囲をどのようにネットワークにアドバタイズできるか、およびネットワーク内の他のコール エージェントによって生成されたアドバタイズメントにどのようにサブスクライブできるかについて説明します。
- 「Intercompany Media Engine のダイヤル プランに関する考慮事項」（P.9-33）では、参加する企業間でインターネットを経由してコールをルーティングできる Cisco Intercompany Media Engine（IME）について説明します。
- 「マルチサイト配置用の設計ガイドライン」（P.9-35）では、すべてのマルチサイト配置モデルに当てはまるガイドラインとベスト プラクティスを示します。
- 「ダイヤル プラン アプローチの選択」（P.9-39）では、固定オンネット ダイヤリングおよび可変長オンネット ダイヤリングのダイヤル プランを作成するためのさまざまなアプローチを紹介し、この 2 番めのオプションについては、分割アドレッシングとフラット アドレッシングを紹介します。
- 「SIP 電話機でのダイヤルされたパターン認識の導入」（P.9-52）では、SIP ダイヤル規則を利用して、SIP 電話機が特定のダイヤリング パターンを認識できるようにする方法について説明します。
- 次の各項では、2 つのダイヤル プラン アプローチについて詳しく分析し、それぞれの設定ガイドラインを示します。
  - 「固定オンネット ダイヤル プランの配置」（P.9-40）
  - 「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.9-43）
- 次の各項では、Unified CM でサービス クラスを設定する方法について、2 つの代替方法を示します。
  - 「従来のアプローチによる Unified CM のサービス クラスの構築」（P.9-55）
  - 「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.9-59）
- 「H.323 を使用している Cisco IOS でのサービス クラスの構築」（P.9-67）では、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを実装する方法を説明します。
- 「コール カバレッジの配置」（P.9-70）では、ハント リストと回線グループを使用して Unified CM にコール カバレッジ機能を実装する場合の、ガイドラインとベスト プラクティスを示します。

グローバル化デザイン アプローチ

この項では、グローバル化された番号に基づいて簡素化されたコール ルーティングを実装するために使用されるダイヤル プラン機能について説明します。主に、オフネット コールに対して発信元にかかわらず単一のルーティング構造を使用することによって、ルーティングが簡素化されます。たとえば、異なる国にいる 2 人のユーザは、それぞれのダイヤリング手順に一致するように設定されたサイト固有のルート パターンの代わりに、同じルート パターンを使用して、それぞれのローカル ゲートウェイに対してコールを伝送できます。

このようなグローバル化を実現するためのアーキテクチャ上の主要なアプローチは、次のようにまとめることができます。

- コールがシステムに着信する場合、宛先番号および発信番号はローカル形式で受け付けられますが、すぐにシステムによってグローバル化されます。
- グローバル形式で表現されたルート パターンを使用してコールを宛先にルーティングするために、グローバル化された着信番号が使用されます。グローバル形式は、81001234 のようなグローバルな企業固有の内部形式や、+E.164 形式（たとえば +12125551234）などの DID 番号のグローバル化された公衆網表現の組み合せとなります。
- 宛先が特定されると、発信番号および着信番号は、コール伝送先のエンドポイント、ネットワーク、またはシステムで必要とされる形式にローカル化されます。

したがって、設計指針は次のようになります。

> コールの着信では、ローカル化された形式で受け付け、それらをグローバル化します。グローバル化された形式に基づいてコールをルーティングし、宛先で必要とされる形式に従ってコールをローカル化します。

Cisco Unified Communications Manager（Unified CM）には、次のダイヤル プラン グローバル化機能が備えられています。

- 「ローカル ルート グループ」（P.9-13）
- 「+ ダイヤリングのサポート」（P.9-13）
- 「発番号変換」（P.9-13）
- 「着番号変換」（P.9-14）
- 「着信側の設定（ゲートウェイ別）」（P.9-14）
- 「論理パーティション設定」（P.9-15）

また、これらの新機能により Unified CM システムで次のことができるようになりました。

- 発信者の物理的な場所に基づいたコールのルーティング。
- International Telecommunication Union（ITU; 国際電気通信連合）の E.164 勧告に記載されているようなグローバル形式で発番号および着番号を表示する。
- ローカル ダイヤリング手順に基づいた形式でユーザへのコールを表示する。
- 発番号、着番号、それらに対応する番号タイプのローカル要件に適合する形式で外部ネットワークへのコール（たとえば公衆網）を表示する。
- 発信番号の数字と番号タイプに基づき、ゲートウェイからの着信コールについての発番号をグローバル形式で生成する。
- 一部の国の法的要件に準拠するため、各エンドポイントのジオロケーションに適用されるポリシーに基づいて、エンドポイント間のコールの確立と通話切替機能の開始を制御する。

ローカル ルート グループ

ローカル ルート グループでは、ゲートウェイへのオフネット コールのパターンを作成する機能を提供します。このパターンは、発信側への近さで選択されます。たとえば、ルート オフネット、特定の国のすべてのサイトに対する国内通話に対して、1 つのパターンを定義できます。すべてのサイトの電話機をこのパターンに一致するように設定できます。このパターンはその後、発信側電話機に関連付けられたローカル ルート グループに基づいて、コールをルーティングします。これによって、サイト 1 の電話機がサイト 1 のゲートウェイを介してコールをルーティングできるようにします。一方、サイト 2 の電話機（こちらも同じパターンを使用）はサイト 2 のゲートウェイを介してコールをルーティングします。この機能は、Unified CM 7.0 よりも前のリリースと比較した場合、オフネット コールのサイト固有のルーティング設定を簡素化します。

+ ダイヤリングのサポート

電話番号には、他の国から宛先に到達するのに必要な国際ダイヤル アクセス コードを表すために、+ 記号を使用できます。たとえば、+1 408 526 4000 は、米国にあるシスコ本社の国際表記です。この番号にコールするには、フランスの企業テレフォニー ユーザは通常 0 00 1 408 526 4000 とダイヤルする必要がありますが、英国の発信者は 9 00 1 408 526 4000 とダイヤルする必要があります。いずれの場合でも、+ をそれぞれの発信者に関連のある、適切なオフネット アクセス コード（企業テレフォニー システムで定められているとおり）に、また国際アクセス コード（公衆網キャリアで定められているとおりに）に置き換える必要があります。

システムは + で定義された宛先に直接、コールをルーティングできます。たとえば、ユーザは、シスコの米国本社の WiFi 電話のスピード ダイヤル エントリを + 1 408 526 4000 とプログラムし、フランス、英国、または企業内の任意の場所でローミングしているときに、直接ダイヤルできます。それぞれの場所で、システムは宛先番号を地域で定められた番号ストリングに変換して、コールが正しくルーティングされるようにします。

同様に、着信番号が +E.164 形式で表現されている場合、デュアルモードの電話機からダイヤルされた電話番号は、電話機が GSM モードの場合には携帯電話通信業者ネットワーク経由で、電話機が Wi-Fi モードの場合には企業ネットワーク経由で、直接ルーティングできます。これにより、ユーザは、特定の連絡先エントリに対して宛先番号を 1 つ保存するだけで済み、電話機が現在接続されているネットワークにかかわらずその番号にダイヤルできます。

この機能によりユーザは、システムを使用して ITU E.164 勧告に記述されている形式で表現される電話番号に変換し、正しくルーティングできます。ユーザが番号を手動で編集してローカル ダイヤリング手順に適合させる必要はありません。

発番号変換

Unified CM を介してルーティングされるコールに関連付けられている発番号は、電話機または公衆網に表示される前に適合させることが必要な場合があります。たとえば、+1 408 526 4000 からのコールは、宛先の電話機が米国またはカナダにある場合は、発信元が 408 526 4000 と表示されるようにする必要があります。一方、同じ番号からのコールで、宛先の電話機がフランスにある場合は、発信元が 00 1 408 526 4000 と表示されるようにする必要があります。これは主に、地域の公衆網によって定められる慣習的形式で発信側番号が表示されるようにするのが目的で、慣れ親しんだ形式でコールの発信元を識別できます。

ゲートウェイに配信されるコールでは、ゲートウェイが接続している電話通信業者が定める番号に、発番号を適合させる必要があります。たとえば、フランスにあるゲートウェイに提示される +1 408 526 4000 からのコールでは、発信番号を 00 1 408 526 4000 と表し、発番号タイプを International に設定することが必要な場合があります。同様に、カナダにあるゲートウェイに提示される同じ番号からのコールでは、発信側番号を 408 526 4000 とし、発番号タイプを National に設定することが必要な場合があります。

この機能では、発番号を Unified CM システム内のコール ルーティングで使用される形式から、電話機のユーザまたはオフクラスタ ネットワークで定められる形式に適合させることができます。

（注）　一部のサービス プロバイダーでは、機器に技術的な制限、または企業ポリシーや政府の規制の理由から、外国の電話番号を表す発番号を受け付けない場合があります。

着番号変換

Unified CM を介してルーティングされるコールに関連付けられている着信番号は、公衆網に提示される前に適合させる必要がある場合があります。たとえば、カナダにあるゲートウェイを介して公衆網に出る場合、+1 408 526 4000 に対して発信されるコールでは、着番号を 1 408 562 4000 に変換し、番号タイプを National に設定する必要があります。同じコールがフランスのゲートウェイに対して再ルーティングされた場合、着番号を 00 1 408 526 4000 に変換し、番号タイプを International に設定する必要があります。

着番号を操作し、着信番号の番号タイプを設定することによって、この機能では着番号がオフクラスタ ネットワークで定められる形式に適合するようにします。

着信側の設定（ゲートウェイ別）

デジタル インターフェイス（たとえば、ISDN PRI）を介してゲートウェイに着信するコールには、発番号、および発信番号の番号タイプを Unknown、Subscriber、National、または International のいずれかに区別する属性が関連付けられています。組み合せると、着信コールの発信番号と、それに関連付けられた番号タイプにより、発信者の識別情報を特定できます。これは、着信コールの発番号に対して適切な数字を除去したり、プレフィックスを付加したりすることにより実行されます。着信側の設定では、4 つの発信番号タイプのそれぞれで、発番号に対して数字を除去したり、プレフィックスを付加したりする個別の組み合せを適用できるようにします。

たとえば、2 つのコールがドイツのハンブルグにあるゲートウェイに入るとします。どちらのコールも発番号は 691234567 です。最初のコールは、番号タイプ Subscriber に関連付けられています。これは、発信者がハンブルグにいることを意味します。このためシティ コードはハンブルグの（40）となり、国コードはドイツの（49）になります。そのため、着信コールを完全に表すと +49 40 69 1234567 となります。この番号は、番号タイプ Subscriber の着信コールの発番号に対して +49 40 をプレフィックスとして付加することにより得られます。

2 つめのコールは、番号タイプ National に関連付けられています。これは、発信者がドイツにいることを意味します。そしてこの番号にはすでに適切なシティ コード（69 がフランクフルトのシティ コード）が含まれていますが、国コードはドイツ（49）になります。2 つめの着信コールを完全に表すと +49 69 1234567 となります。この番号は、番号タイプ National の 2 つめの着信コールの発番号に対して +49 をプレフィックスとして付加することにより得られます。

この機能によりシステムは、着番号と番号タイプに基づいて着信コールの発番号をグローバル化できます。Unified CM の以前のバージョンでは、これらの設定はクラスタ全体のサービス パラメータを使用することによって実行されました。Unified CM 7.0 では、この機能でゲートウェイごとの設定を取り入れたことにより、番号タイプごとのさまざまなプレフィックスを、異なるゲートウェイに入るコールに適用できるようになりました。設定は、優先順位順にゲートウェイ上、ゲートウェイのデバイス プール上、またはクラスタ全体のサービス パラメータ上で設定できます。空白のエントリはプレフィックスとして数字が付加されないことを意味します。より優先順位の低い設定から設定を継承するには、エントリを [Default] に設定する必要があります。

所定の番号タイプ内のすべてのコールに対しては、最初に受信された発番号に関係なく、プレフィックスの付加および番号削除の動作が適用されます。

（注）　SIP トランク、または SIP ゲートウェイからのコールはすべて発番号タイプ Unknown に関連付けられています。

特に、SIP ゲートウェイおよび SIP トランクに実装された SIP プロトコルによって、実質的にすべてのコールの着番号の番号タイプが Unknown になります。このため、Unified CM では、異なる発番号カテゴリに異なる発番号変更を適用できません。

Unified CM 7.1 以降のリリースでは、着信側の設定に Calling Search Space（CSS; コーリング サーチ スペース）の使用が導入されました。これらの CSS を使用することで、発信側トランスフォーメーション パターンに基づいて発信側に変更を適用できます。これらのパターンでは、正規表現を使用して大文字と小文字を区別したサブセットが照合され、各サブセットに別個の番号操作が実施されます。この新しい機能によって、Unified CM は異なる発番号カテゴリに異なる発番号変更を適用できます。たとえば、公衆網への接続に使用される SIP トランクから、番号タイプが Unknown に設定されたローカル、国内、および海外からのコールが送信されることがあります。このような場合、各コールの発番号を使用して、番号タイプ Unknown に関連付けられたトランクの CSS 内の発信側トランスフォーメーション パターンが照合され、Unified CM で異なる発番号カテゴリに異なる発番号変更が適用されます。

論理パーティション設定

インドなどの一部の国には、企業外部でコールを接続するときに、企業の音声インフラストラクチャにローカル公衆網だけを使用することを義務付けた電気通信規制があります。このため、音声システムを 2 つのシステムに論理的にパーティション化する必要があります。2 つのシステムとは、企業内の Closed User Group（CUG; 非公開ユーザ グループ）通信用とローカル公衆網へのアクセス用です。ロケーション A の企業ユーザからロケーション B の別の企業ユーザへのコールは、CUG システム内で確立できますが、ロケーション A の企業ユーザから公衆網の宛先へのコールは、そのロケーションにかかわらず、ロケーション A の公衆網へのローカル アクセスを経由する必要があります。

既存のダイヤル プラン ツールを使用すると、コールが CUG の外側のエンドポイント間で行われる場合にそのコールを防止できますが、コールが進行しているときにはその新しいコール レッグの確立を防止できません。たとえば、英国ロンドンの企業ユーザが企業ネットワークを介してインドのデリにある同僚にコールするとします。コールが確立されると、デリのユーザは、ロンドンからのコールを受信した回線と同じ回線からインドのカスタマーとの会議に切り替えることになります。この非公開ユーザグループ以外の宛先への通話切替（同じ回線上）は、Unified CM 内の既存のダイヤル プラン ツール（コーリング サーチ スペースやパーティションなど）を使用するだけでは防止できません。
Unified CM 7.1 以降のリリースには、論理パーティション機能が導入されています。この機能を利用することにより、発信側だけでなく、会議や転送などの通信切替機能にも適用されるポリシーを確立し、実施できます。

Unified CM で使用可能なグローバル化機能の組み合せにより、発信元ユーザと通信事業者で定められるローカル形式のコールを受け入れることができるようになり、着信番号と発信番号のグローバル表現を使用してコールをオンネットでルーティングできるようになります。また、宛先のユーザまたはネットワークで定められるローカル形式で電話機またはゲートウェイにコールを送信できます。ダイヤル デザイン アプローチの 3 つの側面は、次のように要約できます。

- 「ローカル化されたコールの着信」（P.9-16）
- 「グローバル化されたコールのルーティング」（P.9-20）
- 「ローカル化されたコールの発信」（P.9-20）

ローカル化されたコールの着信

Unified Communications システム（複数のサイトがさまざまなリージョンまたは国に存在する）では、ユーザのさまざまなダイヤリング手順や、ゲートウェイの接続先のサービス プロバイダーのさまざまなシグナリング要件を満たす必要があります。各地域で異なる場合があるため、システムはローカル ダイヤリング手順とシグナリング要件を、コールが正しくルーティングされる形式に「変換」できるようにする必要があります。そのため、システムは多くのローカル化された着信要件を満たすだけではなく、あらゆる宛先パターンをグローバル化した 1 つの形式も作成する必要があります。

ローカル化されたコールの電話機への着信

電話機またはビデオ端末などのエンドポイントから発信されるコールは通常、ローカル ダイヤリング手順に慣れているユーザによってダイヤルされます。米国内の企業ユーザは、カリフォルニア州 San Jose にあるシスコ本社に到達するために 9 1 408 526 4000 とダイヤルするのに慣れていますが、一方で英国のユーザは 9 00 1 408 526 4000 とダイヤルし、フランスのユーザは 0 00 1 408 526 4000 とダイヤルします。これら 3 つのダイヤル形式は、企業のオフネット アクセス コード（9 は米国、英国、0 はフランス）、国際アクセス コード（00 は英国とフランス、米国の場合、宛先は国内のため必要なし）、宛先番号の表現（国コード（1）を含む）を表します。これら 3 つのグループのユーザは、それぞれ独自のローカル ダイヤリング手順を使用して、同じグローバル化された宛先番号（+1 408 526 4000）にダイヤルします。これら 3 つの各手順で、ローカル ダイヤリング手順のグローバルな記号として + を使用できます。

企業テレフォニー システムでは、ユーザのローカル ダイヤリング手順を正しく解釈できる必要があります。上記の 3 つの手順すべてで、ユーザはローカル ダイヤリング形式を使用して共通の宛先に到達します。ユーザ入力を認識するようにシステムを設定し、コールが正しい宛先にルーティングされ、送信されるようにします。コールはさまざまな形式で発信される可能性があるため、システムはそれらのさまざまな各形式に一致するパターン認識を用意する必要があります。

Unified CM のトランスレーション パターンはローカル化されたユーザ入力を電話機からダイヤルされたものとして、Unified Communications システム内のコールのルーティングに使用するグローバル形式に変換します。これらのパターンでは、次のものを含む、ローカル化されたすべてのダイヤリング手順が認識されるようにする必要があります。

- サイト内、オンネットのダイヤリング
- オフネットのローカル、国内、国際ダイヤリング
- 緊急コール、ディレクトリおよびオペレータ サービスなどのローカル サービス
- 通信事業者選択コードなど

上で説明した 3 つのコール例の場合、次のトランスレーション パターンが別々のパーティションに設定され、次のコーリング サーチ スペース（CSS）に配置されます。

- 米国の電話：9.1!（ドットの前の番号を削除して、先頭に + を付加します）
- 英国の電話：900.!（ドットの前の番号を削除して、先頭に + を付加します）
- フランスの電話：000.!（ドットの前の番号を削除して、先頭に + を付加します）

いずれの場合でも、地域で有効なダイヤルされたストリングは、グローバル化された形式の + 1 408 526 4000 に変換されます。

同一サイト内の 2 人のユーザ間のコール、または異なるサイト間にいるユーザ間のコールなどのオンネットの宛先の場合、トランスレーション パターンを使用して宛先番号のグローバル化されたオンネット形式を生成する必要があります。サイト コードを使用してオンネット ダイヤリングを行ったり、電話の完全修飾公衆網アドレスをオンネット番号として使用したりしている場合に、該当します。

たとえば、San Jose サイトにいる 2 人のユーザがお互いにコールするために 5 桁の短縮ダイヤリングを使用するとします。ユーザ A は、51234 とダイヤルしてユーザ B にコールします。このサイトで固有のトランスレーション パターンが設定され、5 で始まる 5 桁の任意のストリングが認識されます。そして着信番号はグローバル化されたオンネット形式の 800151234 に変換されます。トランスレーション パターンは、「5XXXX、先頭に 8001 を付加」として設定されます。

システム内の他のサイトにある内線 51234 との混同を避けるため、トランスレーション パターンはサイト固有（San Jose サイトの電話機のみにある CSS に含まれる）である必要があります。上の例では、オンネットのグローバル形式は、サイト間アクセス コード（8）とサイト コード（001）を使用して実装されます。システムがオンネット番号として、電話機の完全修飾公衆網アドレスを使用していた場合、トランスレーション パターンでは先頭に +140855 を付加するのではなく、グローバル化されたオンネット番号の +1 408 555 1234 を生成します。

（注）　設定が簡単になるため、可能な場合は、フラット アドレッシングを使用する Variable Length On-net Dialing（VLOD; 可変長のオンネット ダイヤリング）を推奨します。分割アドレッシングを使用する VLOD がサポートされていますが、この設定は複雑です。

グローバル形式を使用した着信コールの許可

電話機でも、グローバル形式のダイヤル番号でダイヤルされたストリングを提供します。Cisco Unified Personal Communicator などのソフトウェア エンドポイントの場合、電話機の Telephony User Interface（TUI; テレフォニー ユーザ インターフェイス）から直接 + ダイヤリングを実行できます。また、ユーザによるクリックダイヤル アクションから実行することもできます。タイプ B の IP Phone で、TUI でキーパッドから + をダイヤルできなくても、Missed Calls および Received Calls ディレクトリには + が含まれる番号のエントリが含まれます。ユーザがそれらのディレクトリからダイヤルするとき、Unified CM に入るコールには、+ で始まる着信番号になります。

（注）　タイプ A およびタイプ B 電話機の定義については、「ダイヤル プランの要素」（P.9-73）を参照してください。

電話機のダイヤル プランによってこれらのコールが正しく処理されるようにするには、ローカル化された形式のダイヤル番号だけではなく、グローバル化された形式も許可されるようにする必要があります。図 9-2 に、どのようにこれを実現するかを示します。

図 9-2　ローカル化およびグローバル化された TUI の許可

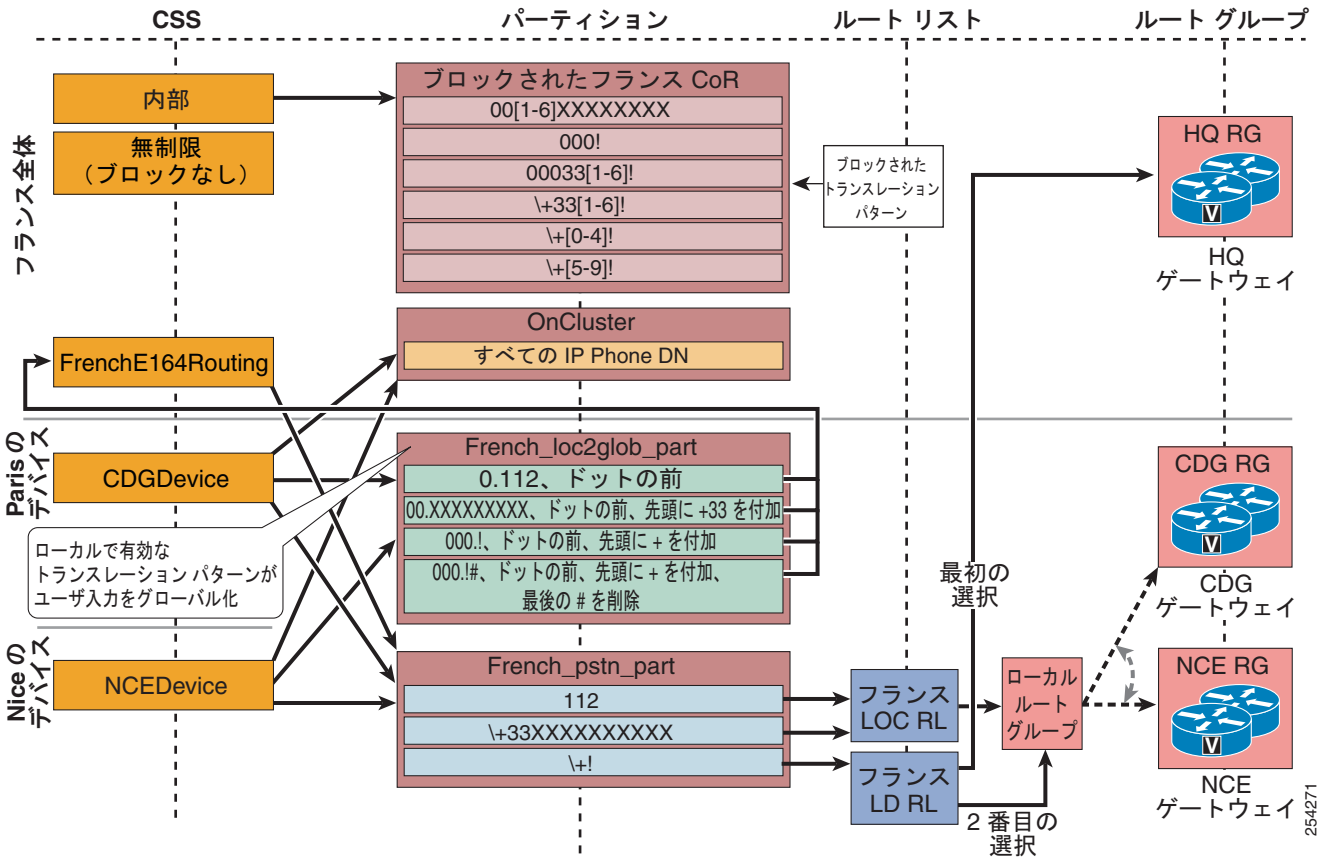


図 9-2 では、フランスの IP Phone ユーザは 0 00 1 408 555 1234 とダイヤルして宛先に接続してから、コールを解除します。着信側はフランスのユーザにコール バックし、接続してから、コールを解除します。その後フランスのユーザは Received コール ディレクトリに移り、最後の受信コールのエントリ（+1 408 555 1234）を選択し、Dial を押します。この例では、フランスのユーザは別々の 2 つのコールを同じ宛先に向けて開始します。最初のコールの場合、フランスのダイヤリング手順に合せてローカル化された宛先番号の形式が使用されます。対応するトランスレーション パターン 000.! に対してユーザ入力がマッチングされます。いったん変換されると、ルーティング パターン +! がコールのルーティングに使用されます。2 つめのコールの場合、宛先番号のグローバル化された形式が使用され、ルーティング パターン +! が直接使用されます。

サイトごとに設定されているコーリング サーチ スペースでは通常、次のことができます。

- サイトの、ローカル化されたサイト内のダイヤリング手順
- サイトにいるユーザの、ローカル化されたオフネットのダイヤリング手順
- 緊急コールなどの適用できるローカル テレフォニー サービス、ディレクトリおよびオペレータ サービス
- オンネットおよびオフネット番号のグローバル化された形式

上記リストの最初の項目を除いて、コール ルーティングを行うために使用されるローカル化されたパターンは、通常、同一のダイヤリング ドメイン内のサイト間で再利用できます（フランスのすべてのサイトは、オフネットの番号を同じようにダイヤルします。英国のすべてのサイト、米国のサイトなども同じ）。ただし、それぞれのサイトには、独自のサイト内の短縮ダイヤル トランスレーション パターンを設定する必要があります。それは、San Jose にいるユーザが、たとえば 51234 とダイヤルしたと

きに（New York にいるユーザが 51234 とダイヤルした場合と比べて）、混同しないようにするためです。サイト内形式の短縮番号から宛先が同じのグローバル化されたオンネット形式への変換は、サイト固有のトランスレーション パターンを使用して行われる必要があります。このパターンでは、各サイトに、サイト固有のコーリング サーチ スペースが設定されている必要があります。

ローカル化されたコールのゲートウェイへの着信

外部ネットワーク（たとえば、公衆網）による Unified Communications システムに送信される着信番号と発信番号は通常、ローカル化されます。番号の形式は、トランク グループのサービス プロバイダーの設定によって異なります。ゲートウェイが公衆網トランク グループに接続されると、システム管理者は公衆網サービス プロバイダーに問い合せて、この特定のトランク グループで使用される、適切なシグナリング ルールを決定します。トランク グループからシステムにコールが送信されると、発信番号と着信番号についての情報の一部は明示的に、一部の情報は暗黙的に示されます。この情報を使用して、システムはコールのグローバル化された発番号および着番号を生成する必要があります。

着番号のグローバル化は、次の方法のいずれかによって実行できます。

- ゲートウェイ設定で、[Call Routing Information] > [Inbound Calls] の設定を行います。ここで有効桁数を元の着信番号から取得し、プレフィックスをストリング（着信番号のグローバル化に使用する）に追加します。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。
- ゲートウェイのコーリング サーチ スペースによって参照される、トランスレーション パターンをパーティションに配置します。トランスレーション パターンは、ゲートウェイに接続されているトランクで使用する着番号の形式に一致するよう設定する必要があります。また、グローバル形式に変換する必要があります。プレフィックスの数字は、適用可能な + 記号および国コード、エリア コード、シティ コードの追加に使用されます。

発番号のグローバル化は、着信側の設定を使用して行う必要があります。この設定は、直接ゲートウェイ上で、またはゲートウェイを制御するデバイス プールのいずれかで設定します。

（注） 管理者がプレフィックスを **Default** に設定した場合、コール処理で次のレベル設定（デバイス プールまたはサービス パラメータ）を使用することを示します。それ以外の場合、フィールドが空白でなければ、設定された値がプレフィックスとして使用されます。フィールドが空白の場合、プレフィックスは何も割り当てられません。

たとえば、シスコの米国本社（+1 408 526 4000）に対して、米国の番号からコールが発信されるとします。そうするとコールはカリフォルニア州 San Jose にあるゲートウェイに送信されます。ゲートウェイに送信された着信番号は 526 4000 です。この情報は、Cisco Unified Communications システムがコールの完全な宛先番号を生成するのに十分です。この特定のトランク グループのサービス プロバイダーによって送信されたコールは、ゲートウェイに接続されたトランク グループの特性に基づいて暗示される国コードとエリア コードを継承します。これは、トランク グループによって処理されたすべての宛先 DID 番号が北米番号計画の国コード（1）、エリア コード 408 を継承していることを前提とします。そのため、この番号の生成されたグローバル形式は +1 408 526 4000 です。ゲートウェイに送信された発信番号は 555 1234 で、番号タイプは Subscriber に設定されています。この番号タイプは、国コードとエリア コードが、トランク グループで設定済みの特性から継承されたものであることを示します。このようにして、システムは発信番号が +1 408 555 1234 であると認識します。

別のコールで、発信番号が 33158405858、番号タイプが International の場合、これは発信番号のグローバル形式が +33158405858 と表現されるということを示します。

グローバル化されたコールのルーティング

すべてのケースに共通のグローバル形式で表現される宛先の場合、すべてのローカル形式を生成できる宛先番号のグローバル形式を採用する必要があります。+ 記号は ITU の E.164 勧告で使用されるメカニズムで、すべての公衆網番号をグローバル一意形式で表現できます。この形式は、完全修飾公衆網番号と呼ばれることもあります。

システムはルーティング パターン（+ 記号を含むグローバル化された着信番号とマッチングする）を使用して設定できます。このような同一のルーティング パターンは、Standard Local Route Group を示すルーティング リストとルーティング グループを指します。このため、発信エンドポイントのデバイス プールから出口ゲートウェイを特定できるため、グローバルのルーティング パターンを作成できます。宛先が選択されると、地域設定と要件にコールを適合させるのに必要なすべてのタスク（発番号と着番号）が実行されます。

ローカル化されたコールの発信

着信番号および発信番号のグローバル形式を使用して、コールが宛先にルーティングされる場合、コールが宛先に送信されるときに次のローカル化の操作について考慮する必要がある場合があります。

電話機の発番号のローカル化

コールが電話機に送信されると、発信番号はグローバル形式に変換されます。これは着信側からは認識できません。ユーザは通常、国内の発信者からのコールでは、発信者の番号が短縮形式で表示されることを望みます。

たとえば、米国にいるユーザは、米国の発信者からの着信コールが、10 桁の国番号で表示され、+ 記号または国コード（1）がないものを好みます。グローバル電話番号が +1 408 555 1234 のユーザは、+1 408 526 4000 とコールすると、着信番号は、電話が鳴っている間、発番号として 408 555 1234 と表示されます。これを実現するために、システム管理者は発信側トランスフォーメーション パターンを +1.!（ドットの前の番号を削除）と設定する必要があります。発信側トランスフォーメーション パターンは、宛先電話機の発信側トランスフォーメーション パターン CSS（デバイス プール レベルで設定）に含まれるパーティションに配置されます。+1 408 555 1234 からのコールが電話機に送信されると、設定済みの発信側トランスフォーメーション パターンとマッチングされます。これにより +1 が削除され、電話が鳴っているときに発番号が 408 555 1234 と表示されます。

（注）　Missed Calls と Received Calls ディレクトリに格納されている発番号は、グローバル化された形式のままのため、ディレクトリに格納された番号ストリングを手動で編集せずに、ワンタッチでダイヤルできます。

（注）　多くの電話機ユーザは公衆網番号のグローバル化形式に慣れつつあります。それは主に、国境を越える携帯電話が一般に使われているためです。システム管理者は、着信番号をグローバル形式で表示させたい場合は、電話機の発信側トランスフォーメーション パターンの設定を行うことができます。

ゲートウェイの発番号のローカル化

コールがゲートウェイに送信されると、発番号は、トランク グループを提供する公衆網サービス プロバイダーの要件に合せる必要があります（このトランク グループにはゲートウェイが接続されています)。発番号トランスフォーメーション パターンは、発信側番号の番号ストリングと番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す発番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、発番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、

シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合せは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザからのコール（+1 415 555 1234）が、最初の選択肢として San Francisco のゲートウェイ、別の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- +1415.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが San Francisco のゲートウェイに送信されると、発番号は両方の発信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、発番号の処理にはこちらが選択されます。このようにして、変換された番号は 5551234、発信側タイプは Subscriber に設定されます。

ゲートウェイがコールを処理できなかった場合（たとえば、すべてのポートがビジーだった、など）、コールは公衆網に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの発信側トランスフォーメーション パターンを使用して設定されます。

- +1708.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが Chicago のゲートウェイに送信されると、発番号は 2 番めの発信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される発番号は 4155551234 となり、発番号タイプは National に設定されます。

ゲートウェイの着番号のローカル化

コールがゲートウェイに送信されると、着番号は、ゲートウェイが接続されているトランク グループを提供する公衆網サービス プロバイダーの要件に合せる必要があります。着番号トランスフォーメーション パターンは、着番号と着番号タイプの変更に使用できます。通常、ゲートウェイの国コードを示す着番号では、+ 記号を削除し、国コードを明示するように変更する必要があります。また、それらを国のプレフィックスに置き換える必要があります。また、着番号の番号タイプを National に変更する必要があります。ゲートウェイが特定のエリア、シティ コードを示すトランク グループに接続されている場合、+ 記号、国コード、ローカル エリア コードの特定の組み合せは通常、適切なローカル プレフィックスに置き換える必要があります。また、番号タイプは Subscriber にする必要があります。

たとえば、San Francisco のユーザへのコール（+1 415 555 2222）が、最初の選択肢として San Francisco のゲートウェイ、別の選択肢として Chicago のゲートウェイを指定したルーティング リストを介してルーティングされるとします。San Francisco のゲートウェイは 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- +1415.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが San Francisco のゲートウェイに送信されると、着番号は両方の着信側トランスフォーメーション パターンとマッチングされます。ただし、最初のパターンの方がより正確に一致しているため、着番号の処理にはこちらが選択されます。このようにして、変換された番号は 5552222、着信側タイプは Subscriber となります。

ゲートウェイがコールを処理できなかった場合（たとえば、すべてのポートがビジーだった、など）、コールは公衆網に発信するために Chicago のゲートウェイに送信されます。Chicago ゲートウェイは次の 2 つの着信側トランスフォーメーション パターンを使用して設定されます。

- +1708.XXXXXXX（ドットの前の番号を削除）、番号タイプ：subscriber
- +1.!（ドットの前の番号を削除）、番号タイプ：national

コールが Chicago のゲートウェイに送信されると、着番号は 2 番めの着信側トランスフォーメーション パターンのみとマッチングされます。そのため、ゲートウェイに送信される着番号は 4155552222 となり、着番号タイプは National に設定されます。

（注） コールがゲートウェイに発信されると、発信側および着信側トランスフォーメーション パターンが、発信および着信番号にそれぞれ適用されます。

（注） SIP では番号タイプが示されません。そのため、SIP ゲートウェイでは、Unified CM によって設定された着信側または発信側の番号タイプの表示を受信できません。

新しいデザイン アプローチの利点

Unified CM 7.*x* の新しいグローバル化機能により有効になったダイヤル プラン デザイン アプローチの利点は、次のとおりです。

- コールのルーティング、特にローカルから公衆網に発信する場合の簡素化された設定。
- システム機能の簡素化された設定と拡張機能。次のものがあります。
  - Automated Alternate Routing（AAR）
  - Emergency Responder（ER）サイト固有のフェールオーバー
  - Call Forward Unregistered（CFUR）
  - テールエンド ホップオフ（TEHO）
  - Cisco Unified Personal Communicator などのソフト クライアントからの E.164 番号のクリックダイヤル（+ 記号を含む）
  - ローミング中のエクステンション モビリティ ユーザまたはローミング デバイスから発信されたスピード ダイヤルの適合コール ルーティング
  - 電話機ディレクトリ エントリ（デュアルモードの電話機を含む）からのワンタッチ ダイヤリング
  - IP Phone ディレクトリの Missed Calls および Received Calls リストからのワンタッチ ダイヤリング

Automated Alternate Routing（AAR）

AAR 宛先マスクがグローバル化された形式に入力されている場合、およびすべての AAR CSS がグローバル化された形式で宛先にコールをルーティングできる場合、システム管理者は AAR グループを設定できます。それは、この機能が、特定の宛先に到達するために、発信電話機の公衆網アクセスの地域要件に基づいてどの数字をプレフィックスとして付加するかを決定する唯一の機能であるためです。

さらに、ほとんどの場合、この AAR CSS の唯一の機能では、コールを発信電話機と同じ場所にあるゲートウェイにルーティングします。そのため、Standard Local Route Group を含むルーティング リストを指す 1 つだけのルート パターン（+!）を使用して設定できます。この 1 つのルーティング パター

ンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられた ローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話でこの 1 つの AAR CSS を使用できます。

Cisco Emergency Responder

Cisco Emergency Responder（ER）へのコールのルーティングは通常、911 CTI ルート ポイントを、プライマリ ER サーバに接続、また 912 CTI ルート ポイントはバックアップ ER サーバに接続するように設定することによって行われます。

どちらの ER サーバも利用できない場合、911 コールは、公衆網が発信側電話機と同じ場所にあるゲートウェイに発信されるように指示できます。設定は次のようにします。

- Call Forward No Answer（CFNA）への 911 CTI ルート ポイントおよび 912 への Call Forward Busy（CFB）、912 CTI ルート ポイントのパーティションを含むコーリング サーチ スペースを介して。
- CFNA への 912 CTI ルート ポイントおよび 911 への CFB、グローバル パーティションを含むコーリング サーチ スペースを介して。グローバル パーティションは Standard Local Route Group を含むルート リストを指す ルート パターン 911 を含む。

どちらの CTI ルート ポイントも登録解除された場合、911 へのコールは、発信電話機のデバイス プールで決定されたとおりにローカル ルート グループに転送されます。デバイス モビリティが設定されている場合、ローミング電話機は訪問したサイトのデバイス プールと関連付けられます。このため訪問したサイトの Local Route Group と関連付けられます。

Call Forward Unregistered（CFUR）

Call Forward Unregistered 機能によって処理されるコールが、発信側電話機と同じ場所にあるゲートウェイを使用するようにするには、電話機の CFUR 宛先を、公衆網番号のグローバル化された + 形式を使用して設定します。CFUR CSS は、標準ローカル ルート グループを指す 1 つのルート パターン（+!）のみを使用して設定できます。この 1 つのルーティング パターンを使用してルーティングされるコールは常に発信エンドポイントに関連付けられたローカル ルート グループを介してルーティングされるため、どのリージョン、どの国にいるとしても、すべてのサイトのすべての電話で同じ CSS を使用できます。

テールエンド ホップオフ（TEHO）

公衆網接続料金を低くするため、システム管理者は、IP ネットワークを使用してオフネットの宛先にコールをルーティングし、公衆網への出口点を着信番号のできるだけ近くにします。同時に、コールの優先 TEHO ルートが使用できない場合、発信電話のローカル ゲートウェイを使用してコールを公衆網に送信する必要がある場合もあります。これは、特定の番号タイプの TEHO ルーティングに参加しているすべての電話で、特定の宛先番号に一致するルート パターンと一致するように設定し、その番号が最初のエントリとして、選択した TEHO 出口ゲートウェイを含むルート リストを、2 番めのエントリとして標準ローカル ルート グループを指すように設定することによって実現できます。

コール制御ディスカバリ

複数のコール クラスタが配置されている環境におけるダイヤル プランは、可能な場合には IP ネットワーク経由でクラスタ間でコールをルーティングし、必要な場合にはバックアップ ルートとしての公衆網を使用するように設計する必要があります。

クラスタを設定してクラスタ間コール ルーティングを可能にするには、リモート クラスタでホストされている DN 範囲を記述したパターンのセットを追加する必要があります。各リモート DN 範囲に対して、ローカル クラスタにおいて次の内容を設定する必要があります。

- リモート クラスタにホストされていると認識させる番号範囲パターン
- それぞれのリモート クラスタの宛先番号範囲に到達するためのプライマリ ルート、および関連するトランクとプロトコル
- 宛先番号範囲へのセカンダリ ルート、および宛先番号を公衆網キャリアで受け入れられる形式に変換するための関連する番号操作

この設定は、ルート パターンなどの静的なダイヤル プラン エントリを使用して、手動で行うことができます。手動で設定する場合、ルーティングするリモート範囲の量が増えるに従って、設定作業量も増えます。すべてのクラスタがゲートキーパー、SIP プロキシ、Cisco Unified CM Session Management Edition などの集中型ダイヤル プラン解決プラットフォームをポイントしている場合、作業量の増加は線形的です。ただし、この場合は、中心となるコントロール ポイントに依存することになります。

これ以外に、フル メッシュを作成する方法もあります。この方法では、各クラスタ ペアにクラスタ間トランクを設定し、他方のクラスタのリモート DN 範囲を定義するルート パターンからこれらのクラスタを参照します。このモードでは、クラスタ間のダイヤル プラン解決を制御する中心的なポイントは存在しませんが、トランクおよび関連する DN 範囲のフル メッシュではすべてのクラスタ ペアをリンクする必要があるため、クラスタの数が増えるに従って設定作業量は指数関数的に増加します。

Cisco Unified Communications Manager では、ネットワークベースの Service Advertisement Framework（SAF）Call Control Discovery（CCD; コール制御ディスカバリ）サービスにサブスクライブすることによって、クラスタがホストする DN 範囲を自動的に交換できる機能が用意されています。SAF CCD によって、クラスタは、それぞれにホストされた DN 範囲をネットワークにアドバタイズし、ネットワーク内の他のコール エージェントによって生成されたアドバタイズメントにサブスクライブできます。SAF CCD を使用することの主な利点は次のとおりです。

- 同じ SAF CCD ネットワークに参加するコール エージェント間でコール ルーティング情報を自動的に配布でき、したがって新しいコール エージェントが追加されたり、コール エージェントに新しい DN 範囲が追加されたりした場合に設定作業が徐々に増大することがなくなります。
- 集中型ダイヤル プラン解決コントロール ポイントに依存しなくなります。
- 複数の Unified CM クラスタが組み合せられた場合を含め、ルーティングが変更された場合に、コール エージェント間のコール ルーティング情報が自動的に回復されます。

「ダイヤル プランの要素」（P.9-73）の項では、SAF CCD の基本的かつシステム的な機能の側面について説明しています。この内容は、次の URL にある最新バージョンの『*Cisco Unified Communications Manager Administration Guide*』に記載されている製品情報を補足するものです。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Service Advertisement Framework およびコール制御ディスカバリの詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）を参照してください。

本章のこの項は、SAF CCD サービスに参加するための Unified CM の製品設定を網羅的に説明することを目的としていません。SAF CCD サービスを提供するネットワーク内のコール エージェントとして Unified CM を使用する場合の、システム上の基本的な注意事項について説明します。次の項では、SAF CCD サービスのダイヤル プランに関する設計上の考慮事項について説明します。

SAF CCD の設計上の考慮事項

SAF CCD では、Cisco IOS ゲートウェイ、Unified CME、Unified CM などのコール エージェント間で Directory Number（DN; ディレクトリ番号）情報を交換できます。最適なパフォーマンスを実現するには、次の基準に注意してシステムを設計する必要があります。

- 「グローバル化された番号のアドバタイズ」（P.9-25）
- 「SAF CCD 要求サービスを通したリモート DN 範囲の取得」（P.9-30）
- 「SAF CCD から取得された DN 範囲へのコールの発信」（P.9-32）

グローバル化された番号のアドバタイズ

SAF CCD サービスに参加するコール エージェント間で交換される DN 範囲は、サイト固有のダイヤリング手順に関係なくすべてのコール エージェントに送信されるため、SAF CCD サービスを通して交換される DN の形式はグローバル形式である必要があります。グローバル形式とは、すべてのコール エージェントの間で一意な形式を指します。この形式は、任意のデバイスやコール エージェントで使用でき、ネットワーク内の任意の場所で使用できます。SAF CCD サービスにアドバタイズされるすべてのパターンは、企業内でグローバルに一意にすることを推奨します。

たとえば、次の番号をコールして、英国の Liverpool にいるユーザ Paul を呼び出すことができるとします。

- 同じく英国の Liverpool にいる同僚 John からコールする場合は 1234
- オーストリアの Vienna にいる同僚 Wolfgang からコールする場合、または電話機を制御するコール エージェントに関係なく、世界中のオンネットの社内オフィス ロケーションにいる他のすべての同僚からコールする場合は 85551234

カリフォルニア州の Hawthorne にいるユーザ Brian は次の番号をコールして呼び出すことができます。

- 同じくカリフォルニア州の Hawthorne にいる同僚 Carl からコールする場合は 1234
- アイルランドの Dublin にいる同僚 Bono からコールする場合、または電話機を制御するコール エージェントに関係なく、世界中のオンネットの社内オフィス ロケーションにいる他のすべての同僚からコールする場合は 84441234

この例では、Paul に関連付けられているローカル化された 4 桁の短縮形サイト内形式の番号は、ユーザ Brian の番号と競合するため、すべてのコール エージェントに送信するグローバルな識別情報としては使用できません。Paul のコール エージェントがネットワークに DN 1234 のアドバタイズメントを送信すると、同じ SAF CCD ネットワーク内の Brian のコール エージェントからアドバタイズされた DN と競合します。このような状態で Carl が 1234 にダイヤルすると、Paul または Brian のどちらを呼び出すかについて競合が発生します。

このような競合を回避するために、コール エージェントでは、常に、サイトやクラスタに固有のコンテキストに依存しないグローバル形式の番号をアドバタイズする必要があります。グローバル形式の番号は、ネットワーク上の任意の電話機からダイヤルでき、ネットワーク全体の中で宛先 DN を一意に識別するものである必要があります。このためには、主に次の 2 つの形式のグローバル DN を使用できます。

- 「サイト コード ベースのオンネット形式」（P.9-25）
- 「+E.164 ベースのオンネット形式」（P.9-26）

サイト コード ベースのオンネット形式

サイト間コールのほとんどがサイト コードに基づくオンネット方式を使用してダイヤルされるシステムでは、サイト コード形式の DN およびそれらを公衆網にフェールオーバーできるルールのセットをアドバタイズすることを推奨します。

サイト間アクセス コード、サイト コード、内線番号の順にダイヤルすることによって、システム内で各 DN にグローバルに到達できます。たとえば、サイト間アクセス コード 8、サイト コード 555（英国、Liverpool）、内線番号 1234 の順にダイヤルすると、企業ネットワーク内の任意の場所から Liverpool のユーザ Paul を呼び出すことができます。これらの構成要素を組み合せることによって、ネットワーク内でグローバルに一意な DN 85551234 が生成されます。

フラット アドレッシングの Variable Length On-Net Dialing（VLOD; 可変長のオンネット ダイヤリング）を使用して実装されたサイト コードが使用されているシステムでは、クラスタによってネットワーク内の他のクラスタにアドバタイズされる DN 範囲は、回線に設定された DN 形式と直接一致します。これにより、コールが他のコール エージェントから SAF CCD トランクに受信された場合でも、着信番号を回線内部で使用されている形式に適合させるための番号操作が不要になります。たとえば、クラスタが 855512XX をアドバタイズし、SAF CCD トランクで 85551234 へのコールを受信した場合、電話機を含む単一のパーティションで直接照合できます。

分割アドレッシングの Variable Length On-Net Dialing（VLOD; 可変長のオンネット ダイヤリング）を使用して実装されたサイト コードが使用されているシステムでは、クラスタによってネットワーク内の他のクラスタにアドバタイズされる DN 範囲は、回線に設定された DN 形式と直接一致しません。このため、コールが他のコール エージェントから SAF CCD トランクに受信された場合、着信番号を、グローバル化された形式から回線内部で使用されているサイト固有の短縮形式に変換する必要があります。たとえば、クラスタが 855512XX をアドバタイズし、SAF CCD トランクで 85551234 へのコールを受信した場合、最初に、着信番号をグローバル形式から宛先電話機のサイト固有のパーティションで使用されているローカル形式 1234 に適合できる一連のトランスレーション パターンが含まれた単一のパーティションで照合する必要があります。

+E.164 ベースのオンネット形式

サイト間コールのほとんどが公衆網形式の DN を使用してダイヤルされるシステムでは、関連する +E.164 形式で DN をアドバタイズすることを推奨します。+E.164 形式には、（オンネットかオフネットかにかかわらず）任意のシステムの任意のユーザが、任意のネットワークを経由して宛先 DN に到達するためのすべての情報が含まれています。SAF CCD サービスから取得される DN 範囲は +E.164 形式のままで保存し、ローカル ユーザ入力をその形式に一致するようにグローバル化することを推奨します。

たとえば、Liverpool のユーザ Paul が、英国クラスタの Liverpool パーティション内の 1234 として定義されている回線 DN を持つ電話機を使用しています。ただし、他のサイトのいずれかの同僚が Paul を呼び出す場合は、Paul の +E.164 形式 DID（+44 15 4555 1234）を地域で有効な形式にした番号をダイヤルします。たとえば、オーストリアの Wolfgang は 0 00 44 15 4555 1234 を、テネシー州 Memphis の Elvis は 9 011 44 15 4555 1234 をダイヤルします。Liverpool の他のサイトからコールする Ringo は、9 0154 555 1234 をダイヤルして Paul を呼び出します。世界のいずれかの地域に出張中のユーザ Edge は、ラップトップからのクリックコール アクションの形式で +44 15 4555 1234 にダイヤルして Paul を呼び出します。

Paul の +E.164 がアドバタイズされる形式が、必ずしもネットワーク上の他のクラスタのユーザによってそのまま文字どおり使用されるわけではありません。上記の例でも、Edge 以外のすべてのユーザは、Paul のローカル化された形式の番号を使用しています。ただし、いずれの場合でも、ダイヤルされたローカル形式をグローバル化することによって、Paul のクラスタからアドバタイズされるグローバル形式に変換できます。

各クラスタでは、ユーザ入力をローカル手順形式で受け付ける必要があります。たとえば、米国のユーザ Elvis が他の国のユーザを呼び出す場合の手動の社内ユーザ入力手順では、オフネット アクセス コード（9）、国際ルーティング コード（011）、宛先の E.164 番号（44 15 4555 1234）の順にダイヤルします。この場合、ユーザ入力のグローバル化においては、9011.!（ドットの前の番号を削除して、先頭に + を付加）などのパターンとの照合が必要です。この 1 つのトランスレーション パターンを、米国の任意のユーザから NANP 国コード 1 外部の任意の宛先へのすべてのコールに使用できます。

すべてのクラスタのすべてのユーザにとって、ユーザ入力手順を +E.164 形式にグローバル化するために必要な、地域で有効なグローバル化ルールの数はわずかです。グローバル化ルールでは、ローカルの公衆網コール、国内コール、および国際コールのグローバル化をカバーする必要があります。多くの国では、すべての国内コールに 1 つの形式だけが存在します。

（注）　+E.164 形式で DN 範囲をアドバタイズする場合、DN 自体がホスト クラスタで +E.164 番号として定義されている必要はありません。

フラット アドレッシングの Variable Length On-Net Dialing（VLOD; 可変長のオンネット ダイヤリング）を使用して実装された +E.164 形式が使用されているシステムでは、クラスタによってネットワーク内の他のクラスタにアドバタイズされる DN 範囲は、回線に設定された DN 形式と直接一致します。これにより、コールが他のコール エージェントから SAF CCD トランクに受信された場合でも、着信番号を回線内部で使用されている形式に適合させるための番号操作が不要になります。たとえば、クラスタが +4415455512XX をアドバタイズし、SAF CCD トランクで +441545551234 へのコールを受信した場合、電話機を含む単一のパーティションで直接照合できます。

分割アドレッシングの Variable Length On-Net Dialing（VLOD; 可変長のオンネット ダイヤリング）を使用して実装された +E.164 形式が使用されているシステムでは、クラスタによってネットワーク内の他のクラスタにアドバタイズされる DN 範囲は、回線に設定された DN 形式と直接一致しません。このため、コールが他のコール エージェントから SAF CCD トランクに受信された場合、着信番号を、グローバル化された形式から回線内部で使用されているサイト固有の短縮形式に変換する必要があります。たとえば、クラスタが +4415455512XX をアドバタイズし、SAF CCD トランクで +441545551234 へのコールを受信した場合、最初に、着信番号をグローバル形式から宛先電話機のサイト固有のパーティションで使用されているローカル形式 1234 に適合できる一連のトランスレーション パターンが含まれた単一のパーティションで照合する必要があります。

両方の形式が必要な場合

一部のシステムでは、ユーザは、上記の両方のアプローチを使用して相互に呼び出しを行います。このような状況においては、ホスト クラスタは、サイト コード形式および +E.164 形式の両方の DN 範囲をアドバタイズする必要があります。これら 2 つの形式は、+ 記号を使用するかどうかによって区別できるため、電話機の特定のグループに対してアドバタイズされる 2 つの DN 範囲の間で重複は発生しません。

DID 以外の番号に関する特別な考慮事項

システムにおいて、DID 以外の番号をクラスタ間で到達可能にする必要がある場合には、SAF CCD を使用するように DID 以外の DN 範囲を設定できます。ただし、公衆網フェールオーバー機能は、DID に関連付けられた DN の場合のようには動作しません。たとえば、800033XX などの DID 以外の DN 範囲がアドバタイズされ、公衆網を経由してホスト クラスタの回線にコールをルーティングする DID 範囲が関連付けられていない場合は、次のいずれかを実行できます。

- ネットワークの輻輳が発生しているため、後でコールを再試行する必要があるという内容を示す、発信側クラスタ内の Annunciator メッセージへのコールを行う公衆網フェールオーバー番号を設定します。
- IVR や受付電話機などのデバイスへのコールを行う公衆網フェールオーバー番号を設定します。

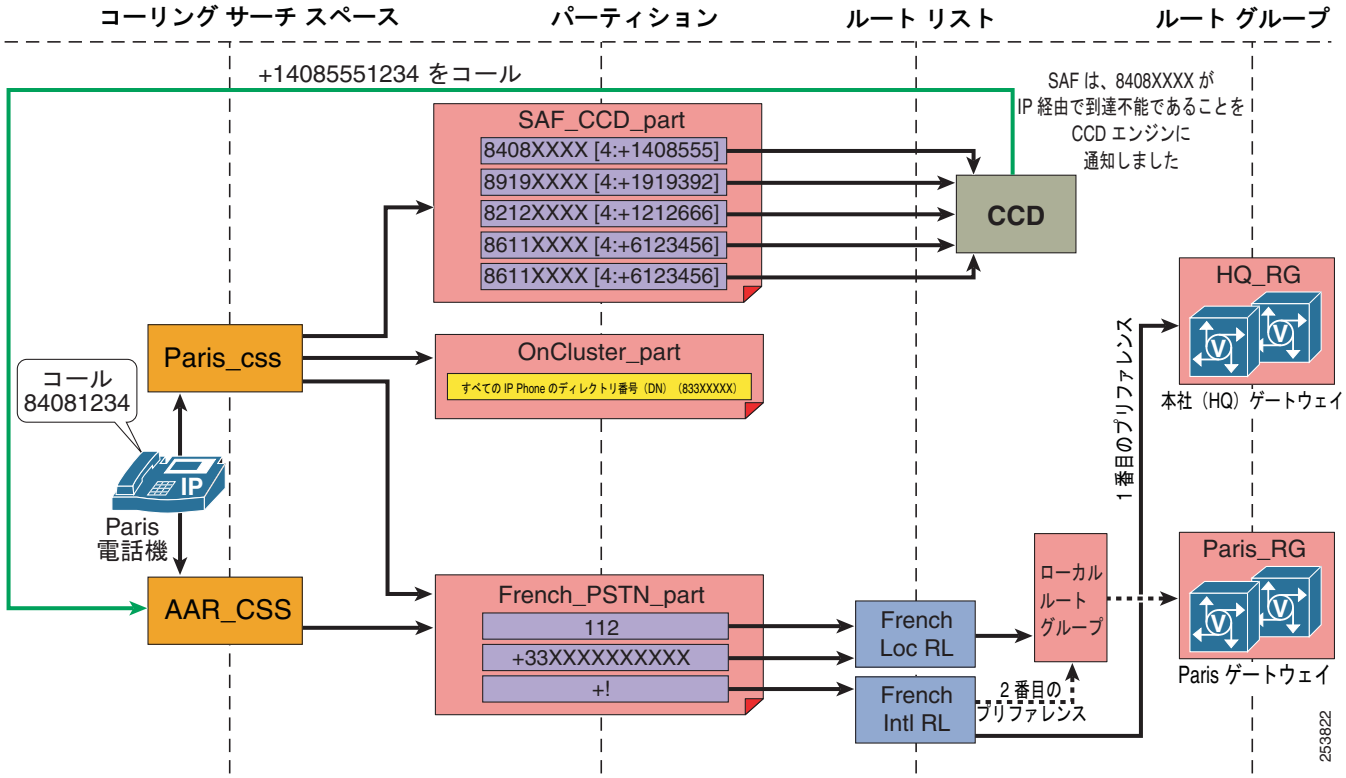
（注）　+E.164 形式では、+0 範囲を使用して、DID 以外の番号を指定できます。したがって、+0 範囲はオンネットで +E.164 形式のコールをルーティングする場合にだけ使用できます。公衆網では、コールは国コード 0 にルーティングされません。

ヒント　DID 以外の範囲を設定する場合は、+0 の範囲を、DN がホストされている実際の国コード、エリア コード、およびシティ コードに分割してください。たとえば、イリノイ州 Chicago の DID 以外の範囲を +01708XXXXXXX で始まるように設定し、DID 以外の 1000 万件の番号を指定できるようにします。同様にして、ドイツの Frankfurt の範囲を +04969XXXXXXX で始まるように設定するなどします。

SAF CCD 発信コールの公衆網フェールオーバーの考慮事項

SAF CCD で検出された番号にコールが発信されると、コールは、Unified CM の [Call Control] > [Call Control Discovery] > [Requesting Service] での設定に従って、要求サービスに関連付けられた SAF CCD トランクのいずれかを経由してルーティングされます（図 9-3 を参照）。トランクでコールを受け付けることができない場合（たとえばコール アドミッション制御によってコールが拒否された場合や、トランクがダウンしている場合）、コールは、発信側デバイスの AAR Calling Search Space（CSS; コーリング サーチ スペース）経由で公衆網に送信されます。宛先番号は、公衆網と直接互換性がない形式である可能性があるため、最初に宛先番号を適合させる必要があります。

図 9-3　SAF CCD および公衆網フェールオーバー



各コール エージェントによって SAF CCD サービスに挿入される DN 範囲レコードには、オンネット形式の番号を公衆網で受け入れられる形式に適合させるために必要なルールが含まれている必要があります。ルールには、範囲の左端から削除する桁数（[PSTN Failover Strip Digits]）、削除後の着信番号の先頭に付加する番号（[PSTN Failover Prepend Digits]）、およびコールを公衆網に再ルーティングする場合に DN 範囲をそのまま使用するかどうか（[Use HostedDN as PSTN Failover] チェックボックス）が含まれます。

たとえば、図 9-3 では、Unified CM クラスタで他のクラスタへのルートが検出されます。検出されたルートは、SAF_CCD_part という名前のパーティションに設定されます。Paris のユーザが 84081234 にダイヤルすると、最適ルーティング ロジックによって、SAF CCD で検出されたパターン 8408XXXX を使用してコールがルーティングされます。この IP ルートが使用できない場合、ダイヤル番号は ToDID 情報と組み合せられます。この情報は、左端から 4 桁（この場合は 8408）を削除し、先頭に +1408555 を付加するように Unified CM に対して指示します。これにより、+14085551234 という番号が生成されます。この番号は、発信側電話機の AAR コーリング サーチ スペースを通して一致を検出するために使用されます。これにより、コールは +! ルート パターンに一致し、French INtl RL ルート リストを経由してルーティングされます。最初に HQ_RG ルート グループ経由でのコールのルーティングが試みられ、失敗した場合は発信側電話機のローカル ルート グループ（この場合は Paris_RG）を使用してルーティングが試みられます。

これらのルールは、Unified CM の [Call Routing] > [Call Control Discovery] > [Hosted DN pattern] で、アドバタイズされる各 DN 範囲に対して設定されます。また、Unified CM の [Call Routing] > [Call Control Discovery] > [Hosted DN group] で、DN 範囲のグループに対して設定することもできます。

それぞれの範囲に対してより詳細にフェールオーバー番号を制御でき、[Hosted DN group] レベルで別途設定する必要もないため、[Hosted DN pattern] レベルで公衆網フェールオーバー番号を設定することを推奨します。

サイト コードを使用して DN 範囲をアドバタイズする場合

たとえば、Liverpool にいるユーザは、855512XX 範囲の番号をダイヤルすることによってオンネットで呼び出すことができます。この形式には、コールを公衆網経由でこの宛先にルーティングするために必要な関連する DID 番号が定義されていません。このサイト コード形式を公衆網で必要な +E.164 形式（+44 15 4555 12XX）に変換するには、アドバタイズされた DN 範囲の左端の 1 桁を削除して、先頭に +44154 を付加する必要があります。この操作は S:PP と表されることもあります。S は、左端から削除する桁数を表し、PP は削除後の着信番号に付加する番号そのものを表します。この例では、変換操作は 1:+44154 と表されます。

（注）　DN 範囲をアドバタイズするクラスタは、公衆網にフェールオーバーするための適切な情報を含む SAF CCD レコードを提供する必要があります。ルートが SAF CCD サービスに挿入されるときにこの情報が提供されない場合、各 CCD クライアント クラスタでは、取得したルートの公衆網フェールオーバー特性の適合用の設定を行う必要があります。これにより、追加の設定作業が発生し、変更が必要な場合には複数のクラスタを変更する必要があります。

着信番号の形式が +E.164 形式に変更されると、コールは、発信側デバイスの AAR CSS を経由してルーティングされます。この場合、+E.164 形式の番号に対して照合が行われる必要があります。ルート パターンが一致すると、コールはルート リスト、ルート グループ、そして最終的にはトランクやゲートウェイを経由してルーティングされます。トランクやゲートウェイでは、+E.164 から公衆網キャリアが必要とするローカル化された形式に番号を適合させるために着信側トランスフォーメーション パターンが使用されます。

+E.164 形式を使用して DN 範囲をアドバタイズする場合

この場合、DN 範囲は直接 +E.164 形式でアドバタイズされるため、公衆網フェールオーバー番号設定は必要ありません。[Hosted DN Range] 設定の下の [Use HostedDN as PSTN Failover] チェックボックスをオンにして、[Hosted DN group] のレベルで設定された公衆網フェールオーバー番号が優先されないようにすることを推奨します。この設定は、同じホストされた DN グループを通してサイト コード形式と +E.164 形式の両方の番号範囲をアドバタイズして、両方のダイヤリング形式をクラスタ間でサポートする必要がある場合に便利です。このような場合、ホストされた DN グループの公衆網フェールオーバー設定は、サイト コード形式の DN 範囲に対して適用され、+E.164 形式の DN 範囲では無視されます。

（注） SAF CCD の公衆網フェールオーバー番号設定では、+ 記号は 2 つの主要な役割を果たします。1 つめは、適合された公衆網フェールオーバー番号が、他のすべてのクラスタにおける他のすべてのサイト内有効範囲と重複しないようにする役割です。たとえば、4415 が有効なサイト内内線番号であるクラスタの番号は、+441545551234 と重複しません。2 つめは、ローカル コールが一部の国コードと重複する状況（たとえば、インドの国コード 91 がノースカロライナ州 Raleigh におけるローカルの 10 桁のダイヤリングと重複したり、モロッコの国コード 212 がニューヨーク州 New York のローカルの 10 桁のダイヤリングと重複したりする場合）において、着信側トランスフォーメーション パターンの照合で + を使用して区別する役割です。

複数のアドバタイジング サービスの設定

ホストされた DN グループは、ホストされた DN パターンの集合であり、Cisco Unified Communications Manager の管理ページでグループ化します。Unified CM Administration でホストされた DN グループを CCD アドバタイジング サービスに割り当てると、CCD アドバタイジング サービスによって、ホストされた DN グループに含まれているすべてのホストされた DN パターンがパブリッシュされます。

Unified CM では、複数のアドバタイジング サービスを設定できます。各アドバタイジング サービスで、ホストされた DN 範囲と、それらの範囲内の DN へのコールの受付を担当するノードとして自身をアドバタイズするコール処理ノードのグループとの間の一意な関係が確立されます。

アドバタイジング サービスは、ホストされた DN グループの 1 つと関連付けられます。このグループは、一連のホストされた DN 範囲に共通です。また、アドバタイジング サービスは、1 つの SIP SAF トランクまたは H.323 SAF トランクにも関連付けられます。これらの各トランクは、デバイス プールに関連付けられます。このデバイス プールは、Unified CM サーバ グループに関連付けられます。Unified CM サーバ グループの構成メンバーは、ホストされた DN グループ内の任意の DN 範囲のコールを担当するとしてアドバタイズされます。コール処理サーバが WAN 経由のクラスタとして配置されているシステムでは（WAN を介したクラスタリング）、電話機を処理するために使用される Unified CM サーバ グループを、電話機に設定された回線に対応する DN 範囲のアドバタイズにも使用することを推奨します。これにより、リモート SAF CCD クライアントからこれらの電話機へのコールが、電話機の制御サーバと同じ場所にある Unified CM サーバに送信されることが保証されます。

SAF CCD 要求サービスを通したリモート DN 範囲の取得

SAF CCD 要求サービスは、SAF CCD サービスに参加する他のコール エージェントにホストされた DN 範囲の取得に使用されます。要求サービスは SAF CCD トランクに関連付けられており、SAF CCD から取得された DN 範囲にコールが発信される場合に要求サービスと関連付けられたトランクを選択するために使用されます。

各 DN 範囲は、複数の属性に関連付けられています。

- DN 範囲：8555XXXX や +1408555XXXX などです。
- ToDID 情報：コール エージェントからのアドバタイズによって提供される公衆網フェールオーバー情報を表します。1:+1408 などです。
- IP アドレス：アドバタイズされた DN 範囲をホストするコール エージェントのシグナリング用の宛先を表します。このフィールドには、アドバタイズを行うクラスタが SAF CCD サービスに DN 範囲を挿入するために使用するトランクのアドレスが設定されます。10.0.0.1 などです。
- プロトコル：ホストされた DN 範囲を担当するコール エージェントと通信するために必要なシグナリング用プロトコルを表します。SIP や H.323 などです。

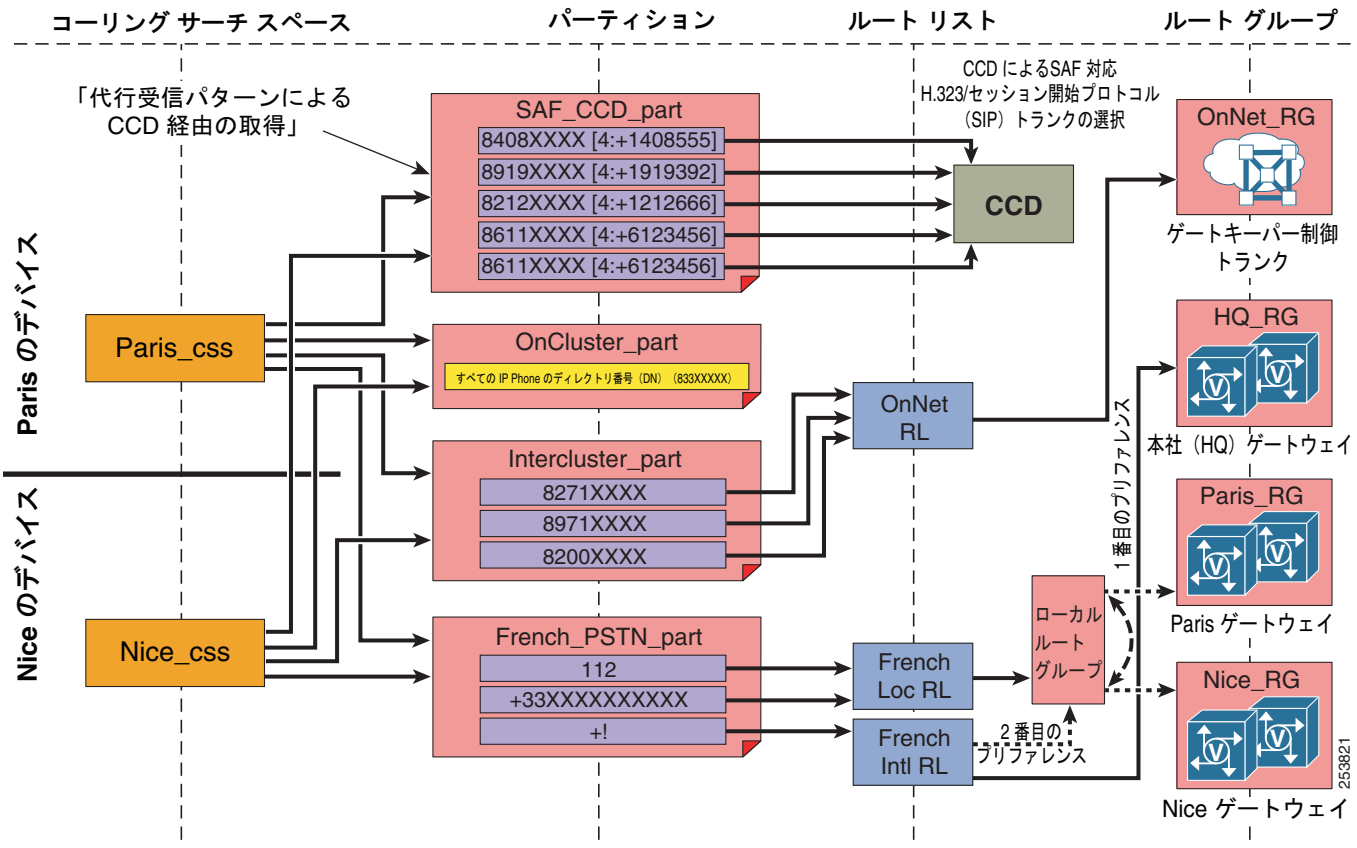
（注）　アドバタイジング サービスが、2 つ以上のメンバーを持つ Cisco Unified Communications Manager グループに関連付けられたデバイス プールのトランクに関連付けられている場合、メンバーごとに 1 つの SAF CCD レコードがアドバタイズされます。つまり、3 つの Unified CM グループ メンバーを持つトランクを通して 1 つのホストされた DN 範囲をアドバタイズすると、3 つの SAF CCD レコードがアドバタイズされます。発信側クラスタによって、同じホストされた DN 範囲をアドバタイズするすべてのレコード間でロード バランシングが使用されます。

SAF CCD パーティション

クラスタでは、SAF CCD パーティションが 1 つ設定され、アドバタイズされた DN 範囲のソース、必要なプロトコル、アドバタイズで使用される DN 範囲形式（サイト コードまたは +E.164）にかかわらずすべての取得されたパターンの格納に使用されます（図 9-4 を参照）。

（注）　SAF CCD パーティションは、[Call Routing] > [Class of Control] > *パーティション*の検索では表示されません。

図 9-4　SAF コール制御ディスカバリと静的ルーティングの統合



取得されたすべてのパターンが 1 つの Call Control Discovery パーティションに配置されるということは、取得されたパターンのサブセットにだけ電話機からアクセスすることはできないことを意味しています。電話機によって使用される CSS、またはダイヤルされたローカル形式の番号を SAF CCD サービスにアドバタイズするグローバル形式に適合させるために使用されるトランスレーション パターンの CSS に Call Control Discovery パーティションを含めることによって、すべてのパターンへのアクセスが実現されます。

たとえば、図 9-4 で、Paris のユーザが 84081234 にダイヤルするとします。静的に設定されたパターンのうち、ダイヤルされたストリングに一致するものはありません。ただし、SAF_CCD_Part パーティションには、SAF CCD 要求サービスから取得された DN 範囲が設定されています。パターン 8408XXXX はダイヤルされたストリングに直接一致するため、ユーザのコールを SAF CCD 対応 IP トランク経由で発信できます。この例で、Paris のユーザも Nice のユーザも SAF_CCD_part パーティションのすべてのパターンにアクセスできることに注意してください。

SAF CCD から取得された DN 範囲へのコールの発信

通常、SAF CCD から取得された DN 範囲に発信されるコールは、アドバタイズされたグローバル形式の番号をユーザがダイヤルした場合は範囲に直接一致する必要があります。ユーザがローカル形式の番号をダイヤルした場合は、グローバル化トランスレーション パターンを通して範囲に一致する必要があります。

発信者の DN がすでにグローバル形式（サイト コードまたは +E.164）である場合、発番号はそのまま送信される必要があります。発番号がローカル形式である場合、発番号はローカル クラスタを出る前にグローバル化される必要があります。グローバル化を行う最良の方法は、コールの発信に使用される SAF CCD トランクの発信側トランスフォーメーション パターンを使用することです。

ユーザが、リモート コール エージェントからアドバタイズされた DN 範囲に対応する番号にダイヤルすると、次のイベントが発生します。

1. ダイヤルされたストリングは、発信側電話機の有効な CSS を通して処理されます。通常どおり、最適ルーティング プロセスが使用されます。つまり、SAF CCD から取得されたルート、またはクラスタ内にローカルに設定されたパターンの複数に一致する宛先にコールが発信された場合、コールでは、最も正確に一致するルートまたはパターンが選択されます。一致精度が等しい複数のルートまたはパターンが検出された場合は、有効な CSS で関連するパーティションが指定されている順序で使用されます。同じクラスタに属する複数の Unified CM ノードが同じルートをアドバタイズするような特殊なケースにおいては、SAF CCD サービスに参加するすべてのクラスタの SAF CCD パーティションにおいて、一致精度が等しい複数のパターンが検出されます。この場合、このパターンへのコールは、一致精度が等しいすべてのパターン間でロードバランスされます。
2. ダイヤルされたパターンへの直接一致が検出されるか（たとえば、ユーザが 84081234 をダイヤルし、これが電話機の CSS に含まれる SAF CCD パーティションのパターンと一致する場合）、またはローカル形式を SAF CCD パーティションにアドバタイズされたグローバル形式に適合させるために使用されるトランスレーション パターンを使用して照合が行われます（たとえば、テネシー州 Memphis のユーザが 9011441545551234 をダイヤルし、その番号が着信番号を +441545551234 に適合させるトランスレーション パターンに一致した場合に、トランスレーション パターンの CSS に位置する SAF CCD パーティションに +441545551234 に一致するものが検出された場合）。
3. コールは、ローカル クラスタでパターンの取得に使用された IP トランクを経由して、リモート クラスタでパターンのアドバタイズに使用されたトランクに発信されます。
4. 発信側クラスタを出るときの着信番号の形式は、リモート クラスタからアドバタイズされた形式です。
5. 発信側クラスタを出るとき、発信番号は、グローバル形式で提供される必要があります。ローカル クラスタの DN がグローバル形式でプロビジョニングされていない場合は、発信側トランスフォーメーション パターンを使用して、ローカル形式を、リモート クラスタに送信するグローバル形式に適合させる必要があります。このことは、特に、リモート ユーザが Missed および Received コール リストからダイヤル機能を使用する場合に重要となります。また、設定を簡易化するために、発番号のグローバル化は、発信側クラスタで実行する必要があります。発信側クラスタで実行しない場合には、他のクラスタから着信するコールを認識して発番号をグローバル化するために必要なルールをすべてのリモート クラスタに設定する必要があります。

6. 発信側クラスタと着信側クラスタとの間で IP ルートが使用できる場合、コールは、リモート クラスタにおいて、SAF CCD サービスに DN 範囲を挿入するために使用されるアドバタイジング サービスに関連付けられたトランクで受信されます。
7. コールを受信するリモート クラスタの SAF CCD トランクでは、トランクの着信コール CSS で一致が検索されます。
8. クラスタに設定されている DN が SAF CCD サービスにアドバタイズされるグローバル形式と同じ形式である場合は、SAF CCD トランクの着信コール CSS に DN パーティションが組み込まれて、一致が検索されます。コールが着信回線に提供されます。
9. クラスタに設定されている DN が SAF CCD サービスにアドバタイズされるグローバル形式とは異なる形式である場合は、SAF CCD トランクの着信コール CSS に、グローバル形式を回線の DN に設定されたローカル形式と照合するためのトランスレーション パターンが含まれたパーティションが組み込まれて、一致が検索されます。コールが着信回線に提供されます。
10. ステップ 6. で、2 つのクラスタ間で IP ルートが使用できない場合は、着信番号に公衆網フェールオーバー番号トランスフォーメーション ルール（ToDID ルール）が適用されて、その結果生成された宛先番号が発信側デバイスの AAR CSS での一致の検索に使用されます。
11. この時点で、着信番号は +E.164 形式になっており、ルート リスト、ルート グループ、およびゲートウェイ（またはトランク）の組み合せを指すルート パターンとの照合に使用されます。
12. コールがゲートウェイまたはトランクから出るときには、トランスフォーメーション パターンを使用して、発番号および着番号の両方を、公衆網キャリアが必要とする形式に適合させる必要があります。この段階で、コールは公衆網に送信されます。
13. コールがリモート クラスタに到達すると、コールは通常の着信公衆網コールと同様に処理されます。

（注） VoPSTN アプローチを配置する場合などのように、設計においてすべてのコールを公衆網を経由して SAF CCD から取得されたルートにルーティングすることを意図している場合は、単純に 1 kbps の帯域幅に設定されたコール アドミッション制御の静的ロケーションに SAF 要求サービスの関連トランクを配置します。これにより、すべてのコールが、強制的に発信側デバイスの AAR CSS を経由してルーティングされます。

Intercompany Media Engine のダイヤル プランに関する考慮事項

Cisco Intercompany Media Engine（IME）を使用すると、参加企業間でインターネット経由でコールをルーティングできます。電話機が IME に参加し、[PSTN Access] としてマークされているトランクまたはゲートウェイ経由でコールを発信した場合、発信番号や着信番号を含むコールのレコードが企業の IME サーバに送信されます。このレコードは、以降にインターネット経由で行われるコール ルーティングにおいて、IME に参加している 2 つの異なる企業の番号のペアにフラグを設定するために使用されます。IME サーバは、同じ 2 つの番号間のコールを再度検出すると、Cisco Unified Communications Manager（Unified CM）に対してこのコールをインターネット経由でルーティングするように指示します。

このように番号のペアを保持する場合、参加しているすべての IME 対応の Unified CM クラスタにおける番号を一貫性を維持しつつ正規化することが課題となります。コールは、最初は公衆網経由で発信され、これらのコールは異なる都市、地域、州、国などの境界を横断することがあるため、ユーザがダイヤルする番号の形式は大きく異なります。同様に、会社によって、DN を回線に割り当てるときのアプローチが異なることがあります。

IME サービスに参加するコールの発信番号および着信番号は、+E.164 形式を使用して識別することを推奨します。+E.164 形式では、一貫性のある結果を保証するために必要な正規化（すべての番号を + で始め、その次に関連する DID 番号の国コードを付加するなど）およびグローバル化が可能です。

[PSTN Access] としてマークされたトランクまたはゲートウェイに対してコールを発信すると、トランクまたはゲートウェイに関連付けられた IME E.164 トランスフォーメーション プロファイルが適用されます。これにより、発番号および着番号に一連のトランスフォーメーション パターンが適用されます。発信コールでは、IME サーバに送信されるレコードで、変換後の番号が使用されます。

（注）　IME E.164 トランスフォーメーション プロファイルは、Unified CM の [Advanced Features] > [Intercompany Media Services] > [E.164 Transformation] で設定されます。

[Intercompany Media Services] > [E.164 Transformation] の設定によって、発信コールに対するトランスフォーメーション パターンの適用が可能になります。設定は、発信側と着信側で分かれています。それぞれに対して、発信側または着信側トランスフォーメーション パターンが含まれているパーティションを含む CSS を設定できます。トランスフォーメーションは、元の番号（ルート パターンに一致したときの形式の番号）またはルーティング用に変換された番号（ルート リスト トランスフォーメーションが適用された後の形式の番号）に対して適用されます。

発番号の場合：

発信側設定を検討する場合の元の番号は、ルート パターンに一致した電話機の DN です。ルーティング用に変換された番号は、ルート リストによって発番号操作が行われた後の電話機の DN です。

たとえば、85551234 と設定された DN から、公衆網経由で 91415551000 にコールを発信します。コールは、トランスレーション パターン 91[2-9]XX[2-9]XXXXXX を使用して発信されます。トランスレーション パターンは、着番号を +14155551000 に、発番号を +14085551234 に変更するように設定されています。次に、このコールは、発番号を 408 555 1234 に、着番号を 415 555 1000 に変更するルート リストが設定されたルート パターン +! に一致します。

元の番号にトランスフォーメーションを適用するように [Outgoing Calling Party Settings] が設定されている場合は、[Outgoing Party E.164 Transformation CSS] の発信側トランスフォーメーション パターンの照合に +14085551234 が使用されます。

ルーティング用に変換された番号にトランスフォーメーションを適用するように [Outgoing Calling Party Settings] が設定されている場合は、[Outgoing Party E.164 Transformation CSS] の発信側トランスフォーメーション パターンの照合に 4085551234 が使用されます。

着番号の場合：

着信側設定を検討する場合の元の番号は、ルート パターンに一致するダイヤルされた番号です。上記の例では、元の番号は +14155551000 です。

ルーティング用に変換された番号は、ルート リストによって番号操作が行われた後の電話機の宛先です。上記の例では、4155551000 です。

変換が番号のどの形式に適用されるかにかかわらず、変換によって、IME サービスに送信される正規化されたグローバル形式の番号が生成される必要があります。

コールが [PSTN Access] としてマークされたトランクおよびゲートウェイから受信される場合、発信番号および受信番号が受信される形式は、IME サービスに送信される前に正規化およびグローバル化される必要があります。発信番号および着信番号の着信形式を IME サービスで必要とされる +E.164 形式に適合させるために、[Incoming Transformation Profile Settings] を使用できます。ここでは、[Incoming Calling Party Transformation Profile] および [Incoming Called Party Transformation Profile] の設定が可能です。それぞれに対して、発信側または着信側トランスフォーメーション パターンが含まれているパーティションを含む CSS を設定できます。

発信番号のトランスフォーメーションは、ルーティング用に変換された番号、つまりトランクまたはゲートウェイのレベルで [Incoming Calling Party Settings] によって処理された番号に適用されます。

着信番号のトランスフォーメーションは、着信コールのゲートウェイまたはトランクの CSS に提供された番号に適用されます。

マルチサイト配置用の設計ガイドライン

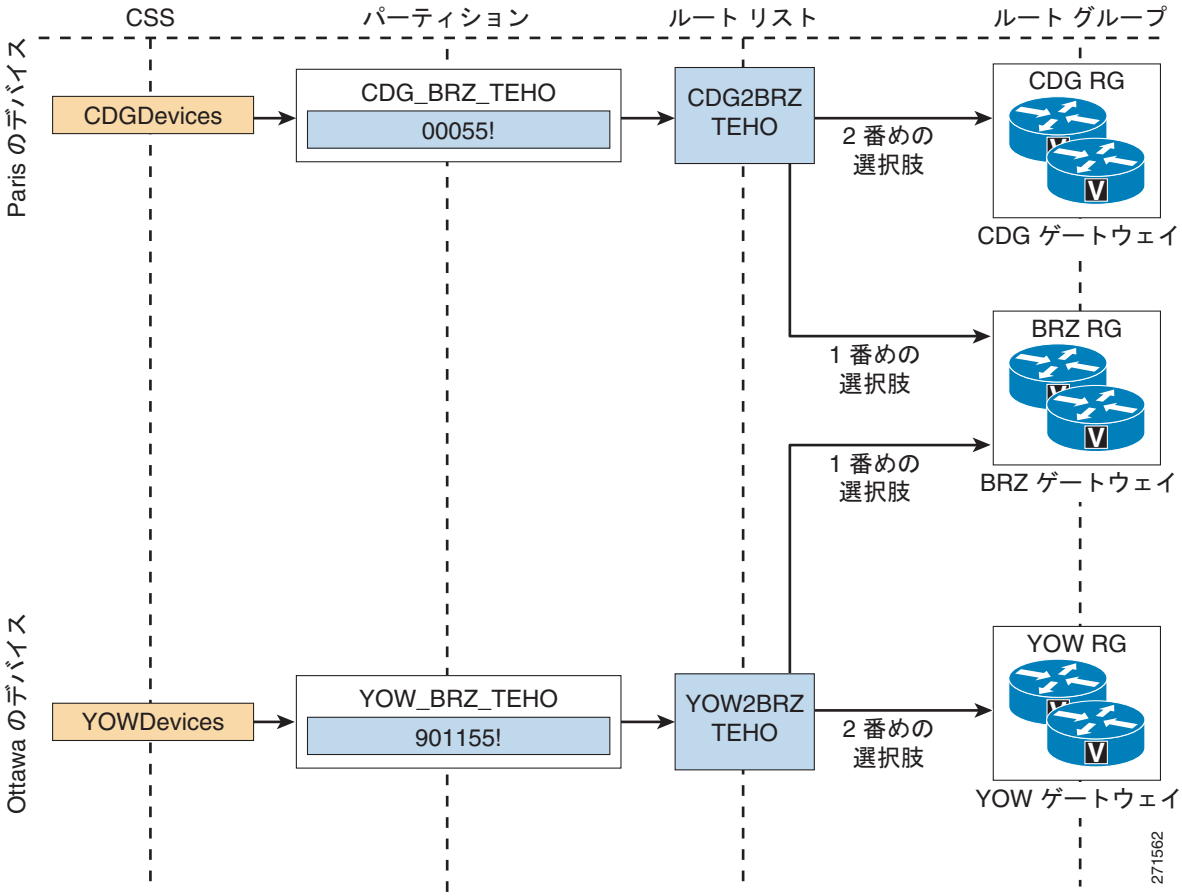
あらゆるマルチサイト IP テレフォニー配置に対して、次のガイドラインとベスト プラクティスが共通して適用されます。複数の Unified CM クラスタが関係する配置については、「マルチクラスタ システムに関する追加の考慮事項」（P.9-37）の項も参照してください。

- ルーティング ループを防ぐには、すべての公衆網ゲートウェイのコーリング サーチ スペースに、同じゲートウェイにコールを送信できるルート リストおよびルート グループに割り当てられている外部ルート パターンが含まれているパーティションを含めないでください。
- 地域通信事業者（LEC）との間で DID 範囲を取り決めるときは、サイト内で重複が発生しない DID 範囲を選択するようにしてください。たとえば、サイト内で 4 桁ダイヤリングを使用していて、1,000 個の DID ブロックが 2 つ必要な場合、ブロック (408)555-1XXX と (408)444-1XXX は 4 桁番号に短縮すると重複し、着信変換と発信変換が実行されるとさらに複雑になります。
- 緊急番号をダイヤルする方法は、複数用意します。たとえば、北米の場合には、911 と 9.911 の両方を Unified CM で緊急ルート パターンとして設定します。
- Automated Alternate Routing（AAR; 自動代替ルーティング）を配置する場合は、IP Phone 上に設定されている外部電話番号マスクまたは AAR 宛先マスクが、各種 AAR グループによって付加されるどのプレフィックスとも競合しないようにする必要があります。たとえば、複数の国にわたる配置の場合、0 などの国内アクセス コードは、それらがグローバル E.164 アドレスの一部でない限り、マスクに含めないでください。AAR を設定する最も簡単な方法は、電話機の完全な E.164 アドレス（+ 記号を含む）として AAR 宛先マスクを設定することです。
- 強制的にオンネットの宛先にダイヤルできますが、公衆網コールとしてダイヤルすると、クラスタ内のオンネットにルーティングされます。このためには、各サイトの E.164 DID 範囲に一致するトランスレーション パターンを追加し、このパターンによって、宛先内線番号に一致するように番号を操作します。たとえば、1234 とダイヤルすることによって DN にオンネットで到達可能な場合で、システム内の誰かがこの同じ宛先を 9 1 415 555 1234 とダイヤルしたとき、トランスレーション パターン 9 1 415 555.1XXX（ドットの前のすべての番号を削除し、変換後の番号にオンネットでコールをルーティングします）を作成することにより、強制的にコールをオンネットのままにできます。ただし、「オンネット強制」トランスレーション パターンを含んだパーティションを除外し、公衆網を指す標準ルート パターンを含んだパーティションを含むように、AAR コーリング サーチ スペースを設定してください。IP WAN が帯域幅外になったときに自動公衆網フェールオーバーができるようになります。
- N 個のサイトがある集中型コール処理クラスタでは、次のいずれかの方法を使用することで、テールエンド ホップオフ（TEHO）を実装できます。
  - 集中型フェールオーバーを使用する TEHO

    この方法では、N 個のルート パターンをグローバル パーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、中央サイト ルート グループを 2 番めの選択肢として保持しているルート リストを指すようにします。
  - ローカル フェールオーバーを使用する TEHO

    この方法では、N 個のルート パターンを N セット、サイト固有のパーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、ローカル サイト ルート グループを 2 番めの選択肢として保持しているルート リストを指すようにします。たとえば図 9-5 では、ブラジル、Paris（フランス）のあるサイトへのローカル フェールオーバー TEHO ルーティングには専用のルート パターン、およびブラジルの TEHO ゲートウェイを最初の選択肢、Paris のゲートウェイを別の選択肢としてコールをルーティングするためのルート リストが必要です。パターンはサイト固有のルート リストにリンクしているため、他のサイトで再利用することはできません。同様に、Ottawa（カナダ）にあるサイトで、カナダでは、Ottawa 固有のルート リストを指す専用のルート パターンで、Ottawa にあるゲートウェイへのローカル フェールオーバーを許可する必要があります。

図 9-5　ローカル ルート グループを持たない TEHO

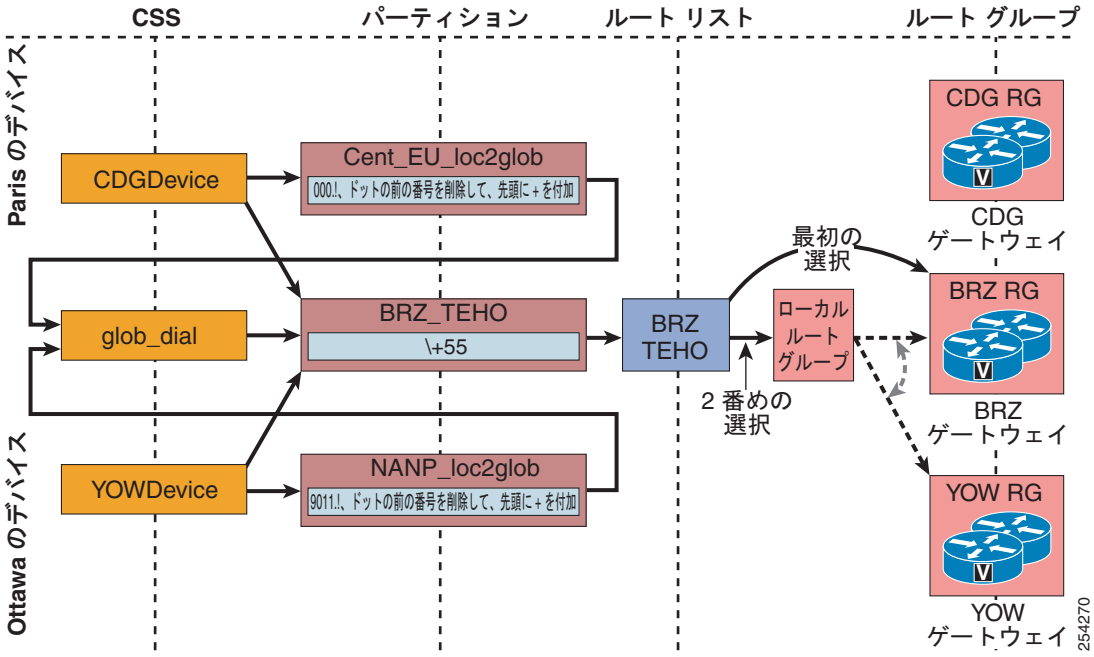


2 番めの方法では、リモート ゲートウェイや IP WAN が使用不可になった場合に、最も優れたフェールオーバー シナリオを実現できる一方で、ダイヤル プランが非常に複雑になります。最初の方法では、必要になるのは N 個のルート パターンと N 個のルート リストであるのに対して、少なくとも N^2 個のルート パターンと N^2 個のルート リストが必要になるためです。

- ローカル ルート グループを持つ TEHO のローカル フェールオーバー

  ローカル ルート グループでは TEHO ルートのローカル フェールオーバーが、サイトごとのルート パターンを作成せずに実装できるようにします。図 9-6 の例の場合、Paris と Ottawa のサイトで単一の TEHO パターンとルート リストが使用されます。これら 2 つのサイトのユーザ入力は同じではないため（フランスのユーザはブラジルの宛先をカナダのユーザとは異なる方法でダイヤルする）、設定は、ユーザ入力をグローバル化するトランスレーション パターンに依存します。最初のエントリがブラジルのルート グループ、2 番めのエントリが標準ローカル ルート グループであるルート リストを指す、単一の、クラスタ全体のルート パターンの照合に、グローバル形式が使用されます。ローカル ルート グループは、発信側デバイスが Paris のデバイス プールにある場合は Paris のルート グループに、発信側デバイスが Ottawa のデバイス プールにある場合は Ottawa のルート グループによって解決されます。

図 9-6　ローカル ルート グループを持つ TEHO



- 国内の番号計画で許容される場合は、長距離電話としてダイヤルされたローカル公衆網コールを捕捉し、適切な短縮形式に変換するための追加トランスレーション パターンを各サイトに設定することを推奨します。このトランスレーション パターンには、サイト内の電話からのみアクセスできるようにします。このように設定することで、AAR 設定も簡潔化できます（「同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項」（P.9-107）を参照）。
- Multilevel Precedence and Preemption（MLPP）機能を使用して、緊急コールに高い優先順位を割り当てないでください。緊急時のコールは、IP テレフォニー システムに緊急コールとして表示されない場合もあります。また、メインの緊急サービス ルーティング番号に新たにコールが発信された場合、既存の緊急コールが終了するおそれがあります。たとえば、緊急時に通常の 10 桁の番号へコールを発信し、医療専門家に連絡することが必要になる場合があります。このコールのプリエンプション処理により、進行中の緊急通信が中止され、緊急時の処理が遅延することがあります。また、救急隊員からの着信コールも MLPP でプリエンプション処理される危険性があります。

（注）　多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランを持つ Unified CM クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Unified CM Administration オンライン ヘルプのサービス パラメータに関する説明を参照してください。

マルチクラスタ システムに関する追加の考慮事項

複数サイトの配置（複数の Unified CM クラスタを含む）のダイヤルプランを設計する場合は、前の項で説明した考慮事項に加えて、次のベスト プラクティスに従ってください。

- DID 範囲を複数の Unified CM クラスタにわたって分割することは避けます。分割した場合、経路の集約が不可能になり、クラスタ間ルーティングが非常に困難になります。各 DID 範囲は、それぞれ単一の Unified CM クラスタに配置してください。

- 1 つのリモート サイト内にある複数のデバイスを、静的ロケーションに基づいたコール アドミッション制御を使用して複数の Unified CM クラスタに分割することは避けます。静的ロケーションベースのコール アドミッション制御が意味を持つのは、1 つのクラスタ内のみです。それぞれ別のクラスタに属している複数のデバイスを同じリモート サイトに配置すると、クラスタ間で使用可能な帯域幅を分割する必要があるため、IP WAN 帯域幅が効率よく使用されなくなります。各リモート サイトは、それぞれ単一の Unified CM クラスタに配置してください。RSVP をロケーションのコール アドミッション制御メカニズムとして使用するよう Unified CM に設定できるため、単一サイトの合計 WAN 帯域幅を、さまざまなクラスタに属する電話機間で効率よく共有できます。RSVP ベースのコール アドミッション制御を最も効率よく使用するには、RSVP を使用するよう、リモート サイト内にあるすべての電話機に設定する必要があります。
- Unified CM クラスタ間でのコール ルーティングには、ゲートキーパー制御クラスタ間トランクを使用します。このようにすると、ネットワーク内でクラスタを簡単に追加および修正できるようになり、他のクラスタをすべて再設定しなくても済みます。
- Unified CM とゲートキーパー間の接続には、冗長性を持たせます。このためには、ゲートキーパー クラスタを使用するか、複数のサーバが設定された Unified CM グループを使用しているデバイス プールに対して、クラスタ間トランクを割り当てます。
- コールをゲートキーパーに送信するときは、着信番号を完全な E.164 アドレスへと展開します。このようにすると、IP WAN が使用不可になった場合の公衆網フェールオーバーが簡単になります。これは、コールを公衆網ゲートウェイ経由で再ルーティングするための追加の番号操作が必要ないためです。また、リモート サイトごとのダイヤル長情報を使用してローカル（発信側）Unified CM を設定する必要がなくなります。
- ゲートキーパー内に、Unified CM クラスタごとにゾーンを 1 つ設定します。クラスタ（ゾーン）ごとに、そのクラスタの所有するすべての DN 範囲に一致するゾーン プレフィックス ステートメントを追加します。
- 次のガイドラインに従うと、複数の Unified CM クラスタにわたってテールエンド ホップオフ（TEHO）を実装できます。
  - 関係する E.164 範囲の個々のルート パターンを、送信元（発信元）Unified CM クラスタに追加します。これらのパターンでは、IP WAN ルート グループを最初の選択肢として保持し、Standard Local Route Group を 2 番めの選択肢として保持するルート リストを指すようにします。
  - Cisco IOS ゲートキーパー設定に、関係するすべての E.164 範囲のゾーン プレフィックス ステートメントを追加します。これらのステートメントでは、適切な Unified CM クラスタを指すようにします。
  - 宛先 Unified CM クラスタに含まれているクラスタ間トランク コーリング サーチ スペースに、ローカル公衆網番号に一致するルート パターンを備えたパーティションを含めます。また、必要に応じて、適切な着番号トランスフォーメーション パターンを使用して番号操作を適用します（たとえば、コールを公衆網に送信する前にエリア コードを除去します）。

分散型コール処理配置の Cisco IOS ゲートキーパーを設定する方法の詳細については、「ゲートキーパーの設計上の考慮事項」（P.8-46）を参照してください。

ダイヤル プラン アプローチの選択

「プランニングの考慮事項」（P.9-4）で紹介したように、IP テレフォニー システムの内部宛先用のダイヤル プランには、主に次の 2 つのアプローチがあります。

- 固定オンネット ダイヤル プラン：個々の内部宛先には、発信者が同じサイトにいるか、別のサイトにいるかにかかわらず、同じ方法でダイヤルします。
- 可変長オンネット ダイヤル プラン：内部宛先がサイト内にある場合、複数のサイトにわたっている場合とは別の方法でダイヤルします。通常、サイトの内部でやり取りされるコールの場合は 4 桁または 5 桁の短縮ダイヤルを使用し、複数サイトにわたるコールの場合は、完全な E.164 アドレスを使用するか、オンネット アクセス コード、サイト コード、内線番号をこの順序で使用します。

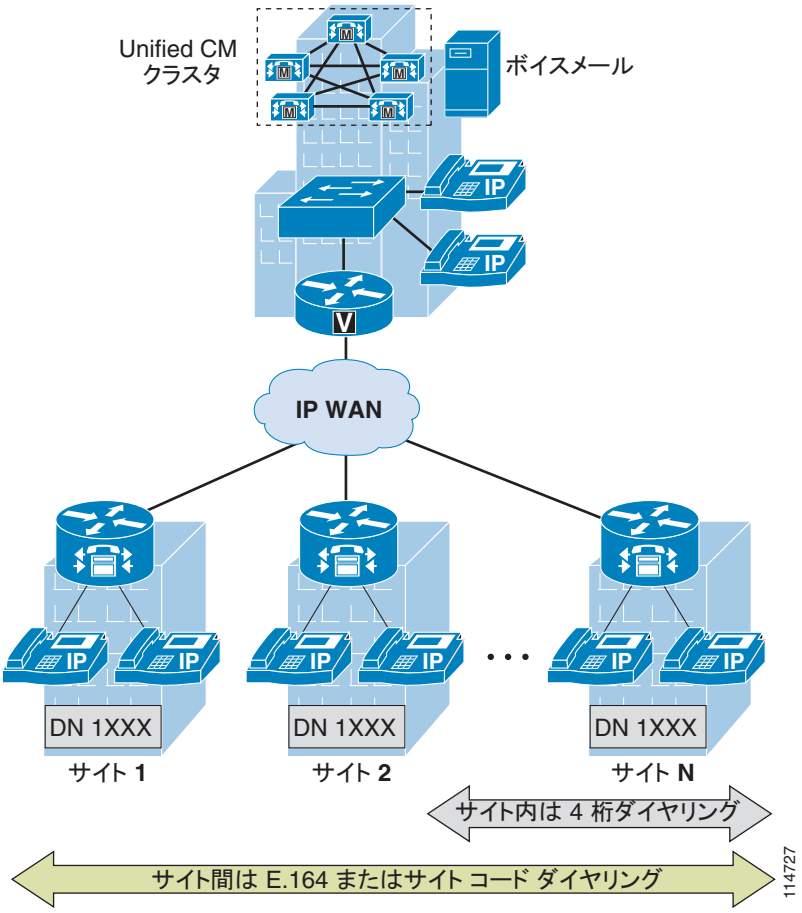
どちらのアプローチが最適かを判断するには、次の基本設計上の質問について検討すると役立ちます。

- IP テレフォニー システムによってサービスされるサイトは、最終的にいくつあるか。
- サイト間または支店間の発信パターンは何か。
- サイト内で、および別のサイトに到達するために、ユーザは何をダイヤルするか。
- オンネットサイト間コールに適用されるコール制限はあるか。
- ほとんどのサイト間コールで使用される転送ネットワークは何か（公衆網または IP WAN）。
- CTI アプリケーションが使用されている場合、それは何か。
- サイト コードを使用して、オンネット ダイヤリング構造を標準化する予定はあるか。

固定オンネット ダイヤル プランは、設計と設定が最も簡単です。ただし、このプランが最も適しているのは中小規模の配置であり、サイトおよびユーザの数が大きくなるほど、実用には適さなくなります。このプランについては、「固定オンネット ダイヤル プランの配置」（P.9-40）の項で詳しく説明および分析しています。

可変長オンネット ダイヤル プランは、スケーラビリティが優れていますが、設計と設定も複雑になります。図 9-7 では、可変長オンネット ダイヤル プラン アプローチを使用する大規模配置について、一般的な要件を示しています。

図 9-7　大規模マルチサイト配置の一般的なダイヤリング要件



Unified CM では、ダイヤル プランに可変長のオンネット ダイヤリングを実装するための主な方法は、フラット アドレッシングに依存します。内部の内線番号を、すべて同じパーティションに配置します。この方法は、通常はサイト間コールのオンネット サイト コードに基づいています。詳細については、「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.9-43）の項を参照してください。このアプローチは、サイト間コールに完全な E.164 アドレスを使用している場合でも使用できることがあります。「サイト コードを使用しない配置に関する特別な考慮事項」（P.9-50）の項を参照してください。

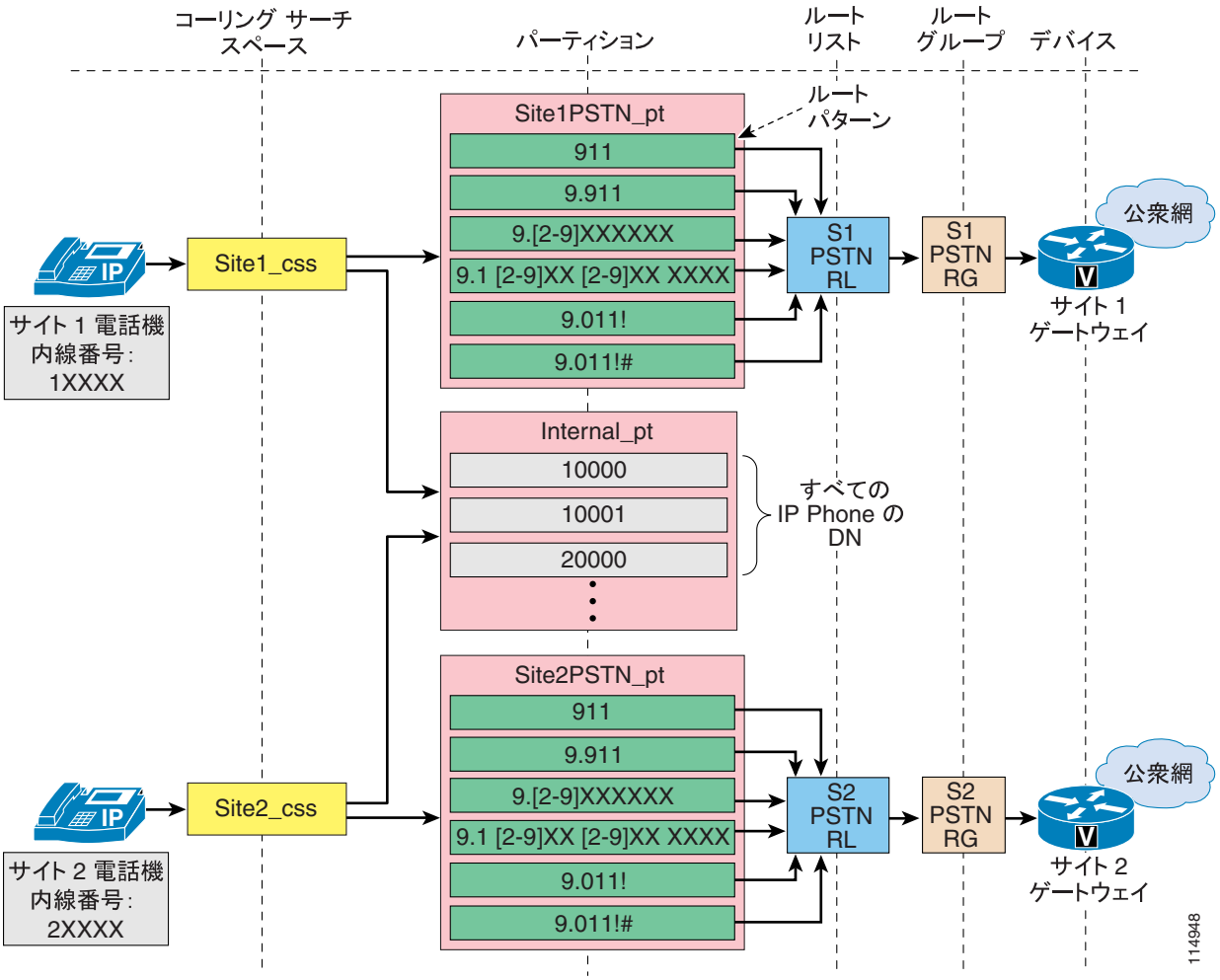
固定オンネット ダイヤル プランの配置

固定オンネット ダイヤル プランを実装するには、次のガイドラインに従います。

- 短縮内線番号を使用して、すべての電話を一意的に識別する。
- すべての電話 DN を単一のパーティションに配置する。
- 各サイトで、選択したサービス クラス アプローチに従って、公衆網ルート パターンを 1 つまたは複数のサイト固有パーティションに配置する。

図 9-8 では、単一 Unified CM クラスタ配置での実装例を示しています。

図 9-8　固定オンネット ダイヤル プランの配置の例



次の両方の条件に当てはまる場合は、このアプローチを使用します。

- 内部内線番号の識別用に選択した桁数を考慮したとき、使用可能な DID 範囲同士が重複していない。
- IP テレフォニー システムによって処理されるサイトの数は、長期的に見て大幅に増加することがない。

次の各項では、固定オンネット ダイヤル プランのフレームワークで使用される各種のコールについて、実装の詳細およびベスト プラクティスを分析します。

- 「クラスタ内でのサイト間コール」（P.9-42）
- 「発信公衆網コールと IP WAN コール」（P.9-42）
- 「着信コール」（P.9-42）
- 「ボイスメール コール」（P.9-42）

クラスタ内でのサイト間コール

すべての内部 DN に対して、あらゆるデバイスのコーリング サーチ スペースから直接到達することができるため、すべてのオンネット コール（サイト内およびサイト間）が自動的に使用可能になります。Unified CM で特に設定する必要はありません。

発信公衆網コールと IP WAN コール

公衆網コールは、サイト固有のパーティションとルート パターンを使用することで可能になります。このため、緊急コールと市内電話は、ローカルの支店ゲートウェイを通じてルーティングできます。長距離電話と国際コールは、企業のポリシーに応じて、同じ支店ゲートウェイを通じてルーティングすることも（図 9-8 を参照）、中央ゲートウェイを通じてルーティングすることもできます。この 2 番めの方法で必要になるのは、サイトごとの追加ルート リストのみです。このリストには、中央サイト ゲートウェイを指す第 1 位ルート グループ、およびローカル支店ゲートウェイを指す第 2 位ルート グループ（省略可）を含めます。サイト固有のコール ルーティングを許可しながら、公衆網コールでのサイト間のルート パターンの再利用を許可するには、Standard Local Route Group を参照するルート リストを使用できます。

別の Unified CM クラスタまたは Cisco Unified Communications Manager Express（Unified CME）への短縮ダイヤリングも、ゲートキーパーを介して可能になります。これらの IP WAN コールについては、ゲートキーパーに送信する前に、トランスレーション パターンを通じて短縮ストリングを完全な E.164 に展開することを推奨します。

緊急コール

緊急コールの処理に Cisco Emergency Responder を使用する場合は、コールを Cisco Emergency Responder へ送信するために使用される CTI ルート ポイントを含むパーティションを、図 9-8 に示したようなサイト固有の 911 パターンではなく、すべての支店内にあるすべての電話機のコーリング サーチ スペースに含める必要があります。内部パーティション内での DN の重複は許容されないので、Cisco Emergency Responder は発信側の電話機を識別できます。Cisco Emergency Responder に関する考慮事項の詳細については、「緊急サービス」（P.10-1）の章と、次の Web サイトで入手可能な Cisco Emergency Responder 製品資料を参照してください。

http://www.cisco.com

着信コール

着信公衆網コールで必要となるのは、Unified CM に設定されている内線番号の長さに合せて、余分な桁を除去することのみです。この操作は、ゲートウェイの設定によって、またはゲートウェイのコーリング サーチ スペースに含まれているトランスレーション パターンを通じて実行できます。

ボイスメール コール

各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定できます。ボイスメール システムにコールを送信するために、または Unified CM 内の Message Waiting Indicator（MWI; メッセージ待機インジケータ）をオンにするために、変換を実行する必要はありません。

ただし、ユーザが公衆網からボイスメール システムにアクセスする場合は、ユーザを訓練して、ボイスメール ボックスにアクセスするときに内線番号を入力してもらうようにする必要があります。

フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置

フラット アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、電話の DN を、オンネット アクセス コード、サイト コード、および内線番号を含んだ一意のストリング（たとえば、8-123-1000）として定義します。これらの DN を同じグローバル パーティションに配置すると、サイト コードを使用したサイト間コールを使用できるようになり、サイト固有のパーティション内にトランスレーション パターンを定義すると（サイトごとに 1 トランスレーション パターンと 1 パーティション）、サイトの内部では短縮ダイヤルを使用できるようになります。

サイト内でユーザが通常ダイヤルしている 4 桁または 5 桁の番号を使用して、[Directory Number] 設定ページの [Line Text Label] パラメータを設定すると、この内部構造をエンド ユーザから見えないようにできます。AAR を使用可能にし、ユーザが自分の DID 番号を IP Phone のディスプレイで見られるようにするには、外部電話番号マスクについても、対応する公衆網番号を使用して設定する必要があります。

表 9-4 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 9-4　フラット アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Translations_pt	サイト 1 の短縮ダイヤルのためのトランスレーション パターン
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）
…		
SiteN_css	SiteNTranslations_pt	サイト N の短縮ダイヤルのためのトランスレーション パターン
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- オンネットのサイト間コールで、ダイヤリング制限が必要ない。
- サイト コードを使用するグローバル オンネット番号計画を使用する予定がある。
- サイト間コールは、通常は IP WAN を通じてルーティングされる。
- CTI ベースのアプリケーション（Cisco Emergency Responder など）がサイト間で使用される。

（注） オンネットのサイト間コールにダイヤリング制限を適用する必要がある場合や、サイト コードを使用するオンネット番号計画を使用する予定がない場合は、それらのニーズに対応可能なこのアプローチの変型について、「サイト コードを使用しない配置に関する特別な考慮事項」（P.9-50）の項を参照してください。

このアプローチには、次の考慮事項が適用されます。

- サイト内の 4 桁コールの宛先番号は、IP Phone のディスプレイでは一意の内部 DN へと展開されます。
- Placed Calls ディレクトリでは、ユーザがダイヤルしたとおりに元の 4 桁のストリングが表示されます。
- 発信番号、および Missed Calls ディレクトリと Received Calls ディレクトリの番号は、一意の内部 DN として表示されます。
- IP WAN が使用不可になって支店の電話が SRST モードになっている場合でも、4 桁ダイヤリング機能をそのまま使用できるようにするには、SRST ルータの **call-manager-fallback** 設定に変換ルールを適用する必要があります。
- 支店の電話が SRST モードになっている場合、一意の内部 DN を IP Phone のディスプレイ上で 4 桁番号としてマスクする Line Text Label は、使用できません。代わりに、ユーザには完全な内部 DN が表示されます。

フラット アドレッシング アプローチを配置する方法をわかりやすくするために、図 9-9 に示す架空の顧客ネットワークについてもう一度考えます。この場合、可変長オンネット ダイヤル プランが必要になることは決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間のダイヤリングでは、オンネット アクセス コード（この例では 8）、3 桁のサイト コード、および 4 桁の内線番号で構成される 8 桁のストリングを使用します。3 桁のサイト コードは、米国にあるサイトの場合は NANP エリア コードから生成され、欧州にあるサイトの場合は E.164 国コードとサイト識別子から生成されます。表 9-5 では、選択されたサイト コードを示しています。

表 9-5　　図 9-9 の顧客ネットワークのサイト コード

	San Jose	New York	Dallas	London	Paris	Milan
サイト コード	408	212	972	442	331	392

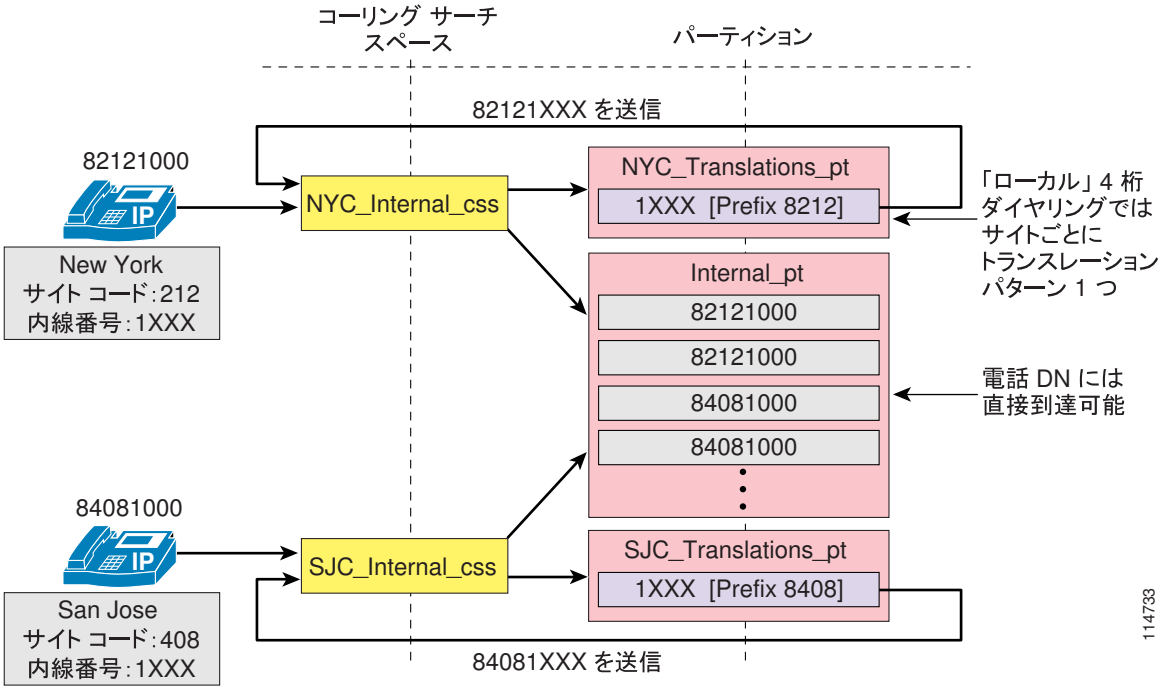
次の各項では、この例の US クラスタを使用して、フラット アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- 「クラスタ内でのサイト間コール」（P.9-45）
- 「発信公衆網コールと IP WAN コール」（P.9-46）
- 「着信コール」（P.9-49）
- 「ボイスメール コール」（P.9-49）
- 「サイト コードを使用しない配置に関する特別な考慮事項」（P.9-50）

クラスタ内でのサイト間コール

図 9-9 では、US クラスタでのサイト間コールの設定例を示しています。

図 9-9　フラット アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってください。

- オンネット アクセス コード 8 を含めて、一意の DN をすべてグローバル パーティション（この例では Internal_pt）に配置します。
- サイトごとにパーティションを 1 つ作成し、それぞれのパーティションの中に、4 桁番号をそのサイトの完全修飾 8 桁番号に展開するトランスレーション パターンを配置して、サイト内部で短縮ダイヤルを使用できるようにします。
- 各サイトで、Internal_pt パーティションとローカル トランスレーション パーティションの両方を電話のコーリング サーチ スペースに含めます。

Unified CM に設定されている DN にオンネット アクセス コードを含めると、すべての電話から直接アクセスできるパーティションの中にすべての内部内線番号を配置できるようになり、同時に、IP Phone 上のすべてのコール ディレクトリの中に、直接にリダイヤル可能な番号が確実に入力されます。

（注）　ただし、オンネット アクセス コードとサイト コードの組み合せが、どのサイトのローカル短縮ダイヤル範囲とも重複しないようにする必要があります。

発信公衆網コールと IP WAN コール

各種の公衆網コールをどのようにルーティングするかに応じて（集中型ゲートウェイと分散型ゲートウェイ）、設定が異なります。

欧州（EU）クラスタへのサイト間コールに対してオンネット接続を提供するには、次のオプションがあります。

オプション 1：8 桁番号のみ

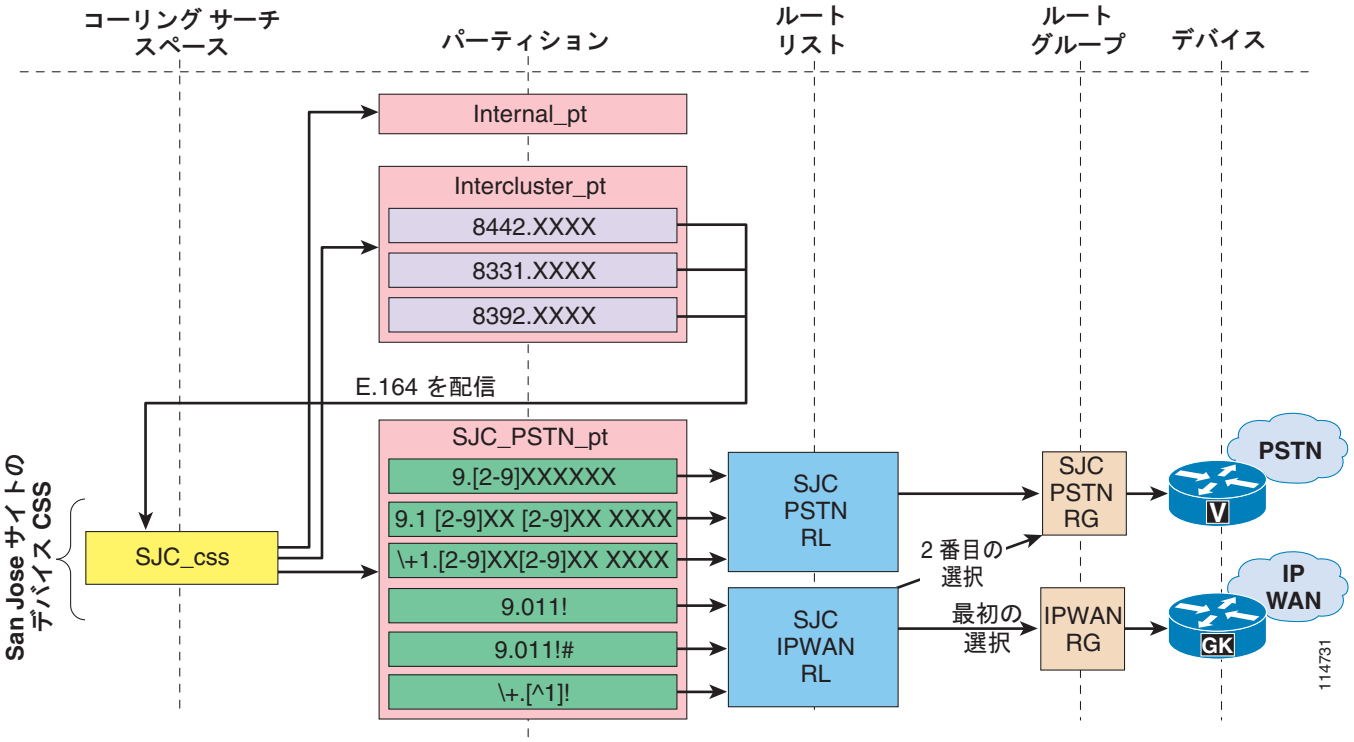
このオプションでは、単一のルート パターンを利用します。このパターンはすべての 8 桁範囲（8XXXXXXX）に一致し、ゲートキーパー制御クラスタ間トランクのみを含んだルート リストまたはルート グループを指しています。ゲートキーパーは、サイト コードをゾーン プレフィックスとして使用するように設定します。

このソリューションは、他のクラスタのサイト コードや E.164 範囲に関する情報が必要ないため、簡潔で保守が容易です。ただし、IP WAN が使用不可になった場合、自動公衆網フェールオーバーは提供されません。ユーザは、公衆網アクセス コードと宛先の E.164 アドレスを使用して、手動で再ダイヤルする必要があります。

オプション 2：8 桁番号と E.164 アドレス（集中型公衆網フェールオーバーを使用）

このオプションでは、図 9-10 に示すように、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換するグローバルな一連のトランスレーション パターンを使用します。これらのトランスレーション パターンでは、中央サイト（この場合は San Jose）のコーリング サーチ スペースを使用するので、コールは中央サイトの公衆網パーティションにある国際公衆網ルート パターンに一致します。各サイトの国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを別の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

図 9-10　IP WAN コールに集中型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



（注）　図 9-10 の設定例は、サービス クラスを構築するための回線/デバイス アプローチが使用されていることを前提としています。ただし、従来のアプローチを使用する場合も同じ考慮事項が適用されます。

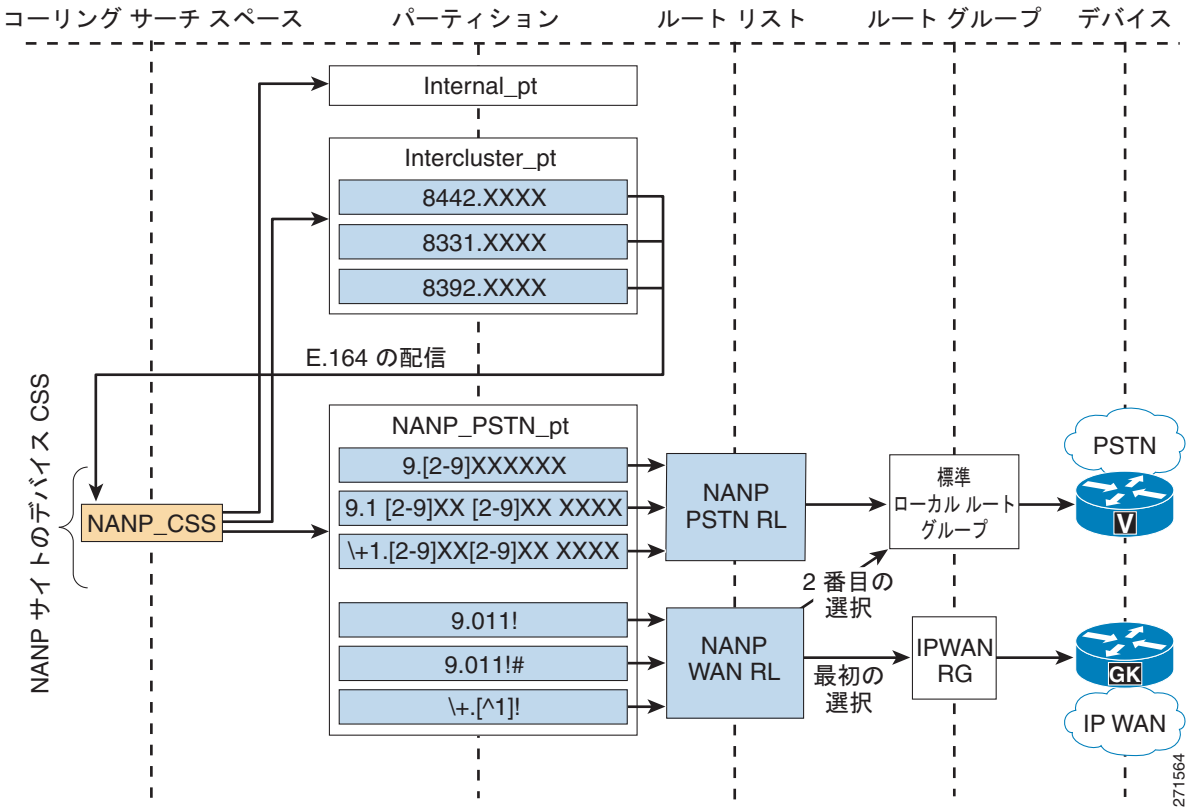
このソリューションは、オプション 1 で説明したソリューションよりもわずかに設定および保守作業が増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守する必要があるためです。その一方で、IP WAN が使用不可になった場合には、自動公衆網フェールオーバーが提供されます。公衆網フェールオーバーは、中央サイトのゲートウェイのみを使用して提供されます。このため、IP WAN 帯域幅の使用効率は最適なものにはなりません。

また、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、自動的にオンネットになります。

オプション 3：8 桁番号と E.164 アドレス（分散型公衆網フェールオーバーを使用）

このオプションでは、図 9-11 に示すように、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換するグローバルな一連のトランスレーション パターンを使用します。トランスレーション パターンでは、グローバル コーリング サーチ スペース（北米番号計画内（NANP）のすべてのサイトで使用）を使用し、コールは NANP の公衆網パーティション内の国際公衆網ルート パターンとマッチングします。国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、標準ローカル ルート グループを別の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

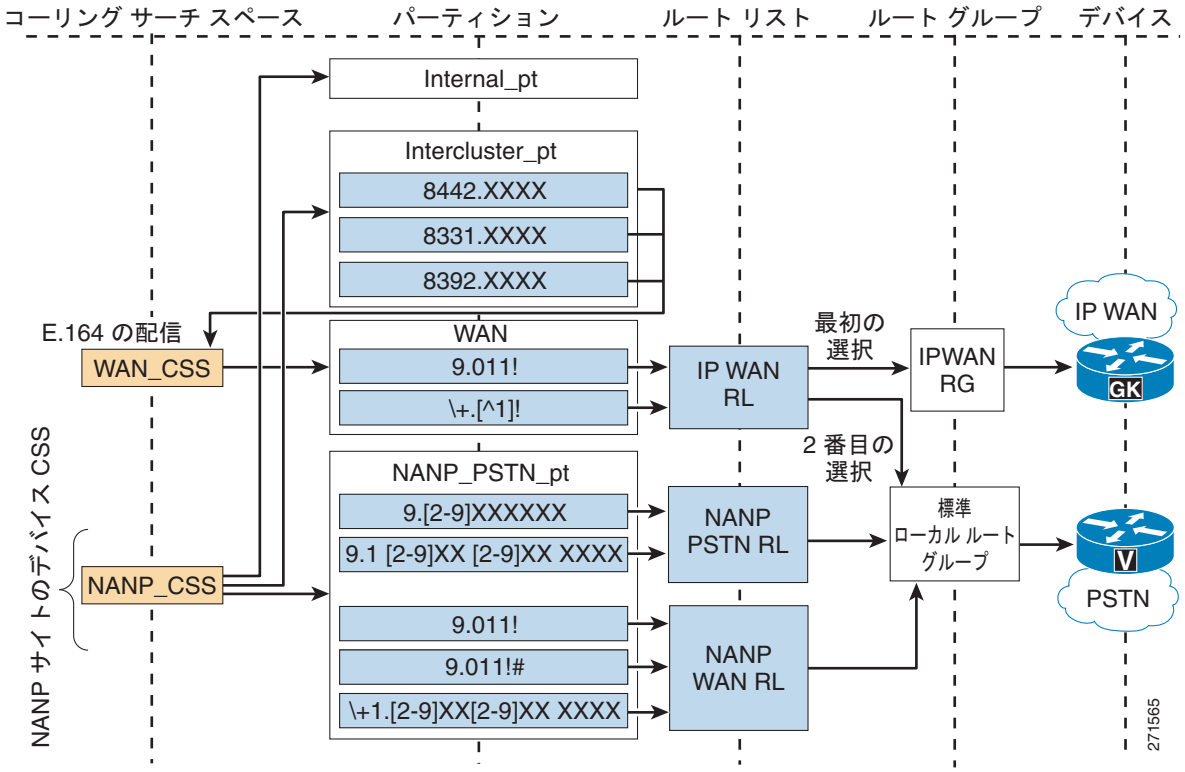
図 9-11　IP WAN コールに分散型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



IP WAN が使用不可になった場合には、このソリューションによりローカル サイトのゲートウェイを使用して自動公衆網フェールオーバーが提供されるため、IP WAN 帯域幅の使用効率は最適なものになります。ローカル ルート グループ コンストラクトの出現により、このアプローチは実質的に 2 番めの選択肢に優先します。このコンストラクトは同じレベルの設定を必要としますが、ローカル公衆網フェールオーバーを行えるためです。

このソリューションでも、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、オプション 2 と同様に自動的にオンネットになります。これは実質的に、NANP サイトから発信されたすべてのオフネットの欧州でのコールに TEHO 機能の形式を提供します。オンネットの宛先としてダイヤルされたコールのみが IP WAN に送信される場合は、発信側でオンネットのクラスタ間宛先としてダイヤルされた場合にのみ IP WAN にコールを送信するよう、アプローチを変更できます。図 9-12 に、このアプローチを示します。

図 9-12　クラスタ間コールのみの IP WAN アクセス



着信コール

着信公衆網コールでは、8 桁の内部番号を取得して宛先の電話に到達するには、E.164 番号を操作する必要があります。この要件は、次の方法のいずれかで満たすことができます。

- [Unified CM の Gateway Configuration] ページにある [Num Digits] フィールドと [Prefix Digits] フィールドを設定して、必要な番号を除去してプレフィックスを付加するようにします。
- クラスタ内でオンネット サイト間コールを強制するトランスレーション パターンを設定した場合は、公衆網アクセス コードをゲートウェイ上の着信番号にプレフィックスとして付加するだけで、それらのパターンを再利用できます。
- H.323 ゲートウェイを使用している場合は、コールを Unified CM に送信する前に、ゲートウェイ内の変換ルールを使用して番号を操作できます。

3 番めのアプローチは、支店が SRST モードになっている場合、設定済みの変換ルールを再利用して IP Phone に着信公衆網接続を提供できる利点があります。

ボイスメール コール

8 桁の各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定できます。ボイスメール システムにコールを送信するために、または Unified CM 内の Message Waiting Indicator（MWI; メッセージ待機インジケータ）をオンにするために、変換を実行する必要はありません。ユーザは、メールボックス番号の入力を求められたときに、8 桁のオンネット番号を使用する必要があることに注意してください。

サイト コードを使用しない配置に関する特別な考慮事項

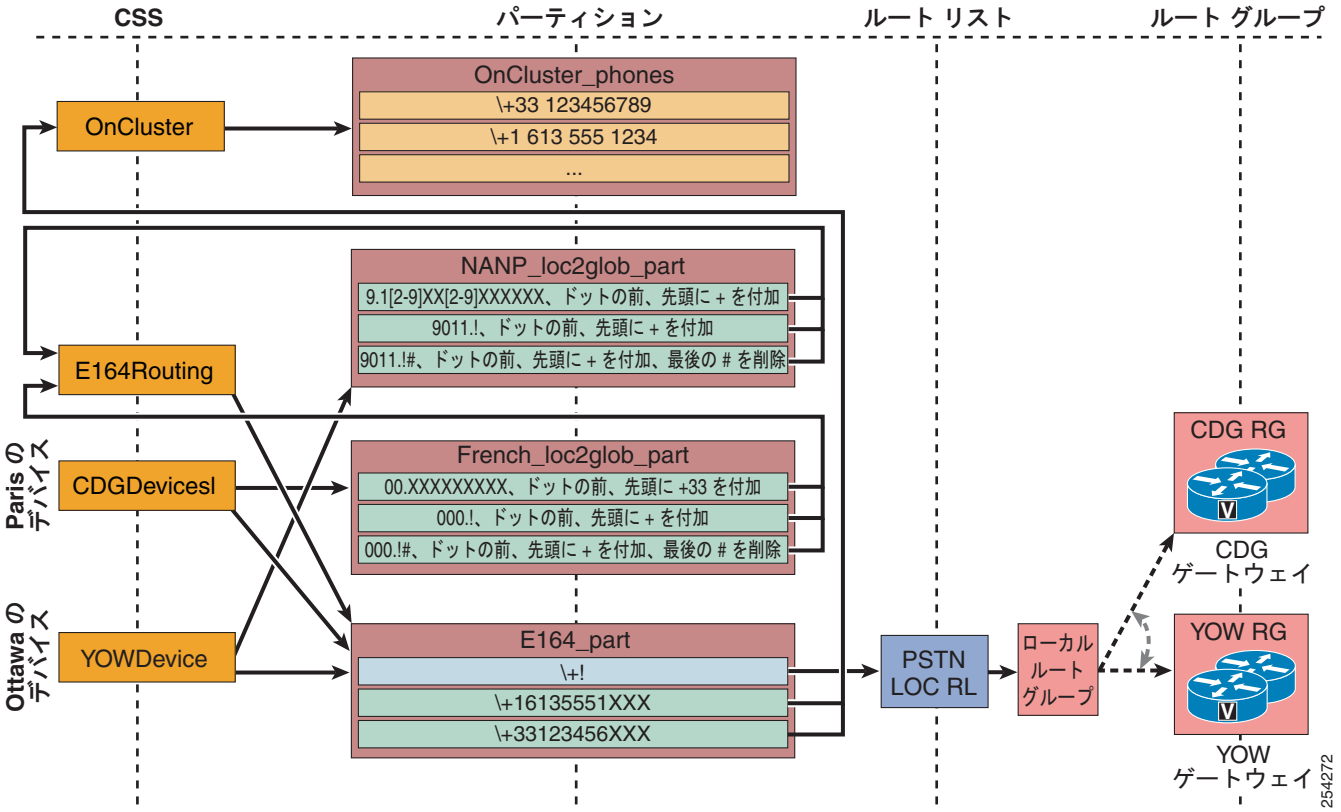
このシナリオは、フラット アドレッシング アプローチの変型であり、サイト コードに基づいてオンネット番号計画を定義することに依存しません。このシナリオでは、サイト内コールは 4 桁番号としてダイヤルします。その一方で、サイト間コールは通常の公衆網コールとしてダイヤルするため、コールは Unified CM によって代行受信され、IP WAN を通じてルーティングされます。

このメカニズムを実装するには、図 9-13 に示すように、次のガイドラインに従います。

- 電話 DN は、完全な E.164 アドレスとして定義し、すべて同じパーティション（この例では OnCluster_phones）に配置します。
- トランスレーション パターンで、ローカル化されたユーザ入力を許可し、完全な E.164 番号を取得できるようにグローバル化するよう設定します。グローバル化された番号は CSS E164Routing を介してルーティングされます。この例では、2 つのデバイスのコーリング サーチ スペースのみを必要とします。1 つは、Paris のサイトからのローカル化されたユーザ入力を受け入れますが、すべてのフランスのサイトで再利用できます。もう 1 つは Ottawa サイトからのユーザ入力を受け入れますが、すべての NANP サイトで再利用できます。
- E.164 ルーティング パーティション（この例では E164_part）を設定します。PSTN コールをルーティングするルート パターンとルート リストの適切なセットを作成します。この例では、ローカル ルート グループへのグローバル化されたすべての宛先 PSTN コールをルーティング可能な単一のクラスタ規模のルート パターン \+! を使用します。加えて、既存のオンクラスタ E.164 プレフィックスを照合し、コール バックを OnCluster_phones パーティションにルーティングするトランスレーション パターンを作成します。

Paris のユーザが番号をダイヤルすると、French_loc2glob_part パーティションにあるトランスレーション パターンを使用してグローバル化され、変換された番号は E164Routing CSS を介してルーティングされます。宛先番号がオンクラスタ DN の場合は、汎用パターンの \+! とトランスレーション パターンを、同時に、E164_part パーティション内のそれぞれに固有のサイト プレフィックスと照合します。より特殊なサイト プレフィックスが選択され、OnCluster コーリング サーチ スペースによってコールがオンクラスタ DN に拡張されます。この 2 段階のルーティングは、オンネット宛先にダイヤルする場合の T.302 桁間タイムアウトを避けるために必要です。ダイヤルした宛先がクラスタ上の電話機ではない場合は、E164Routing CSS を介してルーティングされたグローバル化された番号は E164_part パーティションの +! パターンのみと一致し、変換されたコールは PSTN にルーティングされます。

図 9-13　サイト コードを使用せずにフラット アドレッシングを使用する可変長ダイヤル プラン



この設定変数では、ダイヤリング ルールを簡素化して、使用しやすくします。宛先がサイト内にある場合、短縮ダイヤル（見やすくするために 図 9-13 では省略）を使用します。宛先がサイト外にある場合、オンネットかオフネットかにかかわらず、オフネット公衆網形式でダイヤルします。

- 実質上オンネット公衆網コールを強制することになるため、AAR を設定して、IP WAN の帯域幅が十分にない場合でも公衆網経由でコールを発信できるようにしてください。
- 「発信履歴」ディレクトリには、ユーザがダイヤルしたとおりに番号ストリングが表示されます。たとえば、ユーザが 1000 をダイヤルして電話機 +16135551000 へのコールが発信された場合、「発信履歴」のディレクトリには 1000 が表示されます。これにより、ダイヤル ストリングを編集しなくても番号を直接リダイヤルできます。
- 「不在履歴」と「発信履歴」のディレクトリには、電話機にコールが提供されたときに表示されたとおりの電話番号が表示されます。DN は + を使用して E.164 番号として設定されます。ワンタッチ ダイヤリングが可能です。図 9-13 で、電話機のデバイス CSS は、+ 記号を含むグローバル化された E.164 形式を使用して、直接 DN にコールをルーティングできます。

SIP 電話機でのダイヤルされたパターン認識の導入

SIP 電話機のダイヤルされたパターンの認識機能では、企業内のユーザから予測される一般的なダイヤリング手順の傾向を考慮する必要があります。一般に、ほとんどの企業では次のパターンの組み合せが使用されます。

- 同じサイト内でのコールのための短縮ダイヤル パターン（固定オンネット ダイヤル プランの場合、短縮ダイヤル パターンがサイト間コールに使用される場合があります）
- サイト コードとオンネット アクセス コード（たとえば 8）を使用しているときに可変オンネット ダイヤル プランで一般的に使用されるサイト間ダイヤリング パターン
- ローカル コール用のオフネット ダイヤリング パターン
- 長距離コール用のオフネット ダイヤリング パターン
- 緊急コール パターン（オフネット アクセス コードありとなし）
- 国際コール用のオフネット ダイヤリング パターン

表 9-6 と表 9-7 は、次のダイヤル プラン特性を持つ企業で採用できる SIP ダイヤル規則の例を示しています。

- 短縮ダイヤルは 4 桁（サイト間コールに短縮ダイヤルが使用されるかどうかは無関係）
- サイト間コールではオンネット アクセス コードとして 8 を使用し、その後にサイト コードと DN を表す 7 桁が続く
- 緊急ダイヤリングは 911 および 9911 として許可
- ローカルの 7 桁コールでは 9 をオフネット アクセス コードとして使用し、その後に 7 桁が続く
- ローカルの 10 桁コールでは 9 をオフネット アクセス コードとして使用し、その後に 10 桁が続く
- 長距離コールは 91 と 10 桁をダイヤル
- 国際コールは、9011 の後に不定の桁数が続き、ダイヤリングを # で終了可能

パターン認識は、桁間タイムアウトや Dial キー操作の必要なく、Unified CM に自動的に転送されるユーザ番号入力の収集の自動化だけに関係しています。サービス クラスの実施はすべて、Unified CM の中から選択された各種のコーリング サーチ スペースによって処理されます。すべての電話機を SIP ダイヤル規則を使用して設定し、たとえば、一部の電話機に無制限のサービス クラスが割り当てられていなくても国際ダイヤリングを認識できるようにするのは、その理由からです。

上記のダイヤル プラン特性は、フラット アドレッシングを使用する代表的な可変長オンネット ダイヤル プランです（「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」（P.9-43）を参照）。パターン認識の観点から見ると、このダイヤル プランは、固定オンネット ダイヤル プラン、および分割アドレッシングを使用する可変長オンネット ダイヤル プランと互換性があります（「固定オンネット ダイヤル プランの配置」（P.9-40）を参照）。

表 9-6 と表 9-7 の各パターンに対して、同等の Unified CM 表記のパターンを示してあります。これらの表は、7905_7912 と 7940_7960_OTHER の両方のケースについて、SIP ダイヤル規則を示しています。

（注）　7905_7912 の SIP ダイヤル規則は 128 文字までに制限され、7940_7060_OTHER の SIP ダイヤル規則は 8K（8,192）文字までに制限されています。

表 9-6　7940_7960_OTHER ダイヤル規則

説明	パターン	タイムアウト	効果
短縮形の 2XXX	2...	0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の短縮ダイヤル パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Unified CM に送信されます（timeout = 0）。
短縮形の 3XXX	3...	0	
短縮形の 4XXX	4...	0	
短縮形の 5XXX	5...	0	
短縮形の 6XXX	6...	0	
短縮形の 7XXX	7...	0	
サイト間ダイヤリングの 8.XXXXXXX	8、.....	0	8 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
緊急の 911	9、11	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 11 が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
緊急の 9.911	9、911	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 911 が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
ローカル公衆網の 7 桁	9、.....	3	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。ローカル公衆網の 10 桁ダイヤリングが設定されていると、ユーザは 3 秒のタイムアウトの間にダイヤリングを続行できます。
ローカル公衆網の 10 桁	9、.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
長距離	9、1.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Unified CM への転送が行われます（timeout = 0）。
6 秒の桁間タイムアウトによる国際ダイヤル	9、011*	6	9 が認識されると 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガーすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。
ダイヤリングの終わりとして # を使用した国際ダイヤル	9、011*#	0	9 が認識されるとすぐに 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集され、# によって終了します。Unified CM にすぐに転送されます（timeout = 0）。
オペレータ	0	0	0 が検出されると Unified CM にすぐに転送されます（timeout = 0）。

表 9-7　7905_7912 ダイヤル規則

説明	パターン	効果
短縮形の 2XXX	2...t0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の短縮ダイヤル パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Unified CM に送信されます（t 0）。
短縮形の 3XXX	3...t0	
短縮形の 4XXX	4...t0	
短縮形の 5XXX	5...t0	
短縮形の 6XXX	6...t0	
短縮形の 7XXX	7...t0	
サイト間ダイヤリングの 8.XXXXXXX	8.....t0	番号 8 とそれに続く 7 桁が収集された後、すぐに Unified CM に転送されます（t0）。
緊急の 911	911t0	番号 911 が収集され、すぐに Unified CM に転送されます（t0）。
緊急の 9.911	9911t0	番号 9911 が収集され、すぐに Unified CM に転送されます（t0）。
ローカルの 7 桁と LD	9.....t4>#....t1	番号 9 とそれに続く 7 桁が収集され、さらに 4 秒間に最大 4 桁までダイヤルできます。さらに 4 桁を入力した場合、それらは 1 秒後に Unified CM に送信されます。# は、9 と 7 桁が入力された後の終了文字として認識されます。
国際	9011>#t6-	番号 9 011 と、それに続く不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガーすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。# を終了文字として使用できます。
オペレータ	0	0 が検出されると Unified CM にすぐに転送されます（timeout = 0）。

Unified CM のサービス クラスの構築

Unified CM では、従来のアプローチおよび回線/デバイス アプローチという、ユーザおよびデバイスにサービス クラスを定義、適用する 2 つの主要なアプローチを用意しています。それぞれのアプローチで扱う基本的な要素には、許可するコールの種類（たとえば、local、national、または international）およびコールが取るパス（たとえば、IP ネットワーク、ローカル ゲートウェイ、または中央ゲートウェイ）が含まれます。どちらの要素もコーリング サーチ スペースを使用します。次の項では、Unified CM システムで使用される、サービス クラスを実装するための 2 つの主要なアプローチについて説明します。どちらのアプローチも回線とデバイスのコーリング サーチ スペースの基本的な機能に基づいています。

デバイスのコーリング サーチ スペースは、電話機の IP アドレスで定められているように、ネットワークのどの場所に電話機が物理的に存在しているか、デバイス モビリティが設定されているかどうかに基づいて動的に特定できます。詳細については、「デバイス モビリティ」（P.9-108）を参照してください。

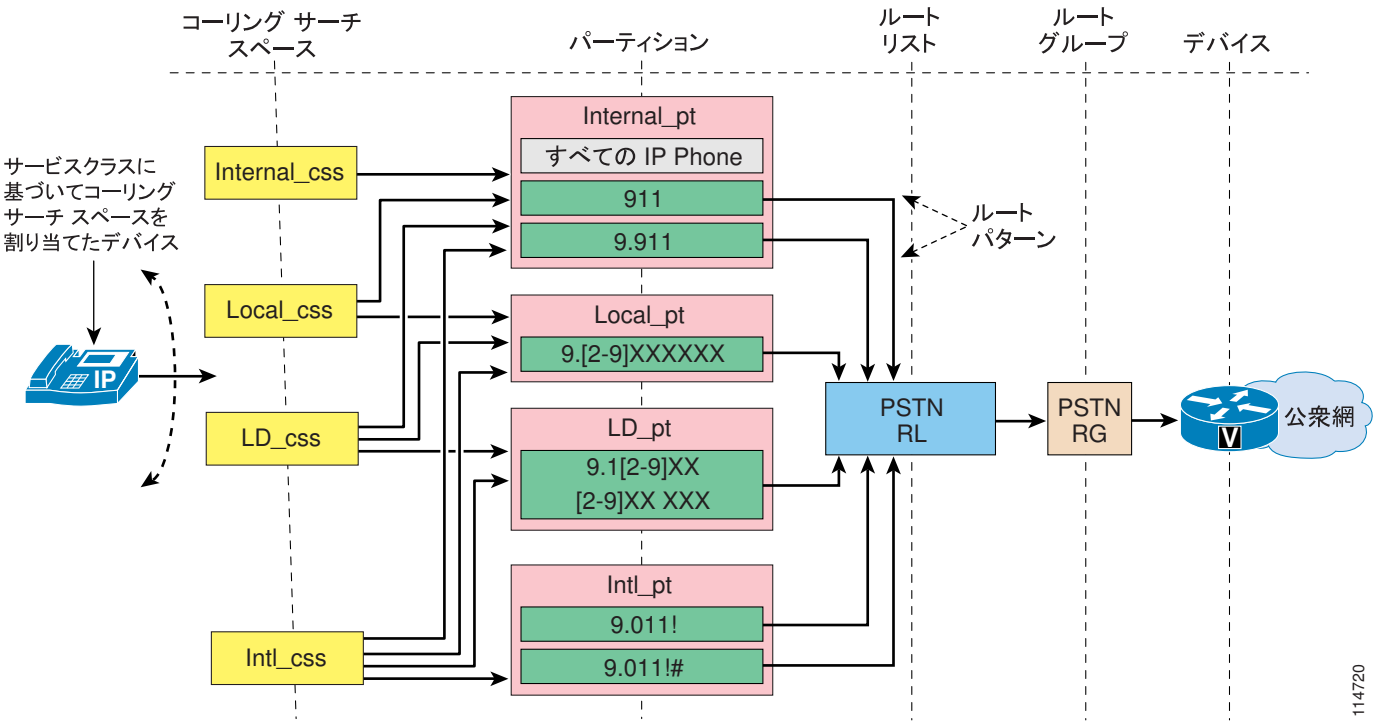
従来のアプローチによる Unified CM のサービス クラスの構築

Unified CM では、次のようにパーティションおよびデバイス コーリング サーチ スペースを外部ルート パターンと組み合せると、IP テレフォニー ユーザにサービス クラスを定義できます。

- 外部ルート パターンをコール可能な宛先に関連したパーティションに置きます。1 つのパーティションにすべてのルート パターンを含めることができますが、コール可能な宛先に応じてルート パターンをパーティションに関連付けると、より高度なコール制限ポリシーを実現できます。たとえば、同じパーティションにローカル ルート パターンと国際ルート パターンを入れる場合、すべてのユーザは、ローカルの宛先と海外の宛先の両方と通信できます。ただし、これは好ましくない場合があります。ルート パターンは、さまざまなサービス クラスの到達可能性ポリシーに従って、それぞれのパーティションに分類することを推奨します。
- 各コーリング サーチ スペースがそのコール制限ポリシーに関連したパーティションのみに到達できるように設定します。たとえば、ローカル コーリング サーチ スペースが内部パーティションとローカル パーティションを指定するように設定します。その結果、このコーリング サーチ スペースに割り当てられるユーザは、内部コールおよびローカル コールしか発信できません。
- Unified CM のデバイス ページで電話機を設定して、これらのコーリング サーチ スペースを電話機に割り当てます。このように設定すると、デバイス上に設定されているすべての回線が自動的に同じサービス クラスを受信します。

図 9-14 では、単純な単一サイト配置の例を示しています。

図 9-14　従来のアプローチを使用するサービス クラスの基本的な例



このアプローチでは、デバイス コーリング サーチ スペースが次の 2 つの論理機能を実行します。

- パスの選択

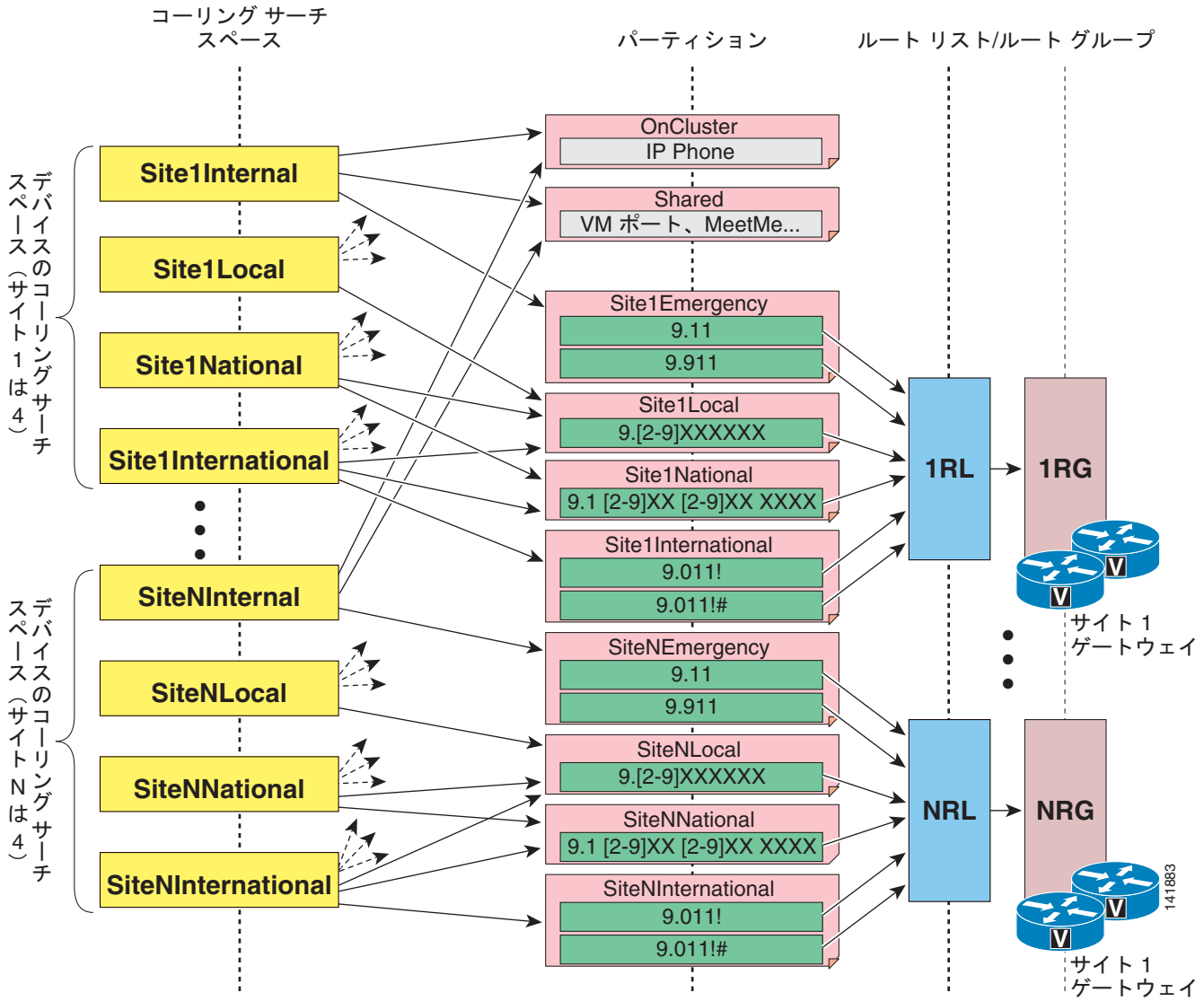
  コーリング サーチ スペースは、特定のパーティションを含んでいます。このパーティションは、ルート リストとそれに関連したルート グループを通じて、特定の公衆網ゲートウェイを指している特定のルート パターンを含んでいます。

- サービス クラス

  特定のパーティションのみをデバイス コーリング サーチ スペースに含めて、他のパーティションを含めないようにすると、特定のユーザ グループに対して実質上のコール制限が適用されます。

結果として、このアプローチを集中型コール処理のマルチサイト配置に適用する場合は、パーティションとコーリング サーチ スペースを各サイトに複製する必要があります。これは、図 9-15 に示すように、サイトごとにサービス クラスを作成し、同時に、ローカル支店ゲートウェイから発信される公衆網コールをルーティングする必要があるためです。または、Standard Local Route Group を参照するルート リストを指すルート パターンを設定できます。こうすると、実際の出口ゲートウェイが、発信電話機のデバイス プールによって決定されます。これにより、コール ルーティングのサイト特性を保持しながら、サイト間のパターンを再利用できます。

図 9-15　従来のアプローチで必要となるコーリング サーチ スペースとパーティション



集中型コール処理を行う複数サイト配置に対してこのダイヤル プラン アプローチを適用するときに、サイト間でオンネット ダイヤリングを構成するために、すべての IP Phone の DN をすべてのサイトのコーリング サーチ スペースからアクセス可能なオンクラスタまたは内部のパーティションに置きます。これは、IP Phone の DN が重複している場合は不可能であることに注意してください。

従来のアプローチにおけるエクステンション モビリティの考慮事項

エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、その電話機へのログイン（またはログアウト）中の機能の 1 つになります。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

エクステンション モビリティを使用する場合、サービス クラスを構築するための従来のアプローチでコール制限を適用するには、次のガイドラインを考慮してください。

- 各サイトで、すべての IP Phone のデバイス コーリング サーチ スペースを、公衆網緊急サービスのみを（ローカル ゲートウェイを使用して）指すように設定します。
- エクステンション モビリティに使用される IP Phone がログアウト状態になっている場合の回線コーリング サーチ スペースを、内部番号のみを指すように設定します。
- 各エクステンション モビリティ ユーザについて、デバイス プロファイル内の回線コーリング サーチ スペースを、個々のユーザのサービス クラスで許可されている内部番号と追加公衆網ルート パターンを（ここでも、企業ポリシーに従って適切なゲートウェイを使用して）指すように設定します。

通常はサイト 1 を拠点としているエクステンション モビリティ ユーザが、サイト 2 の IP Phone にログインすると、公衆網コールのパス選択が次のように変更されます。

- 緊急コールは、サイト 2 の公衆網ゲートウェイを使用して正しくルーティングされます。緊急サービスは、サイト 2 にある IP Phone のデバイス コーリング サーチ スペースによって提供されるためです。
- この他のすべての公衆網コールは、エクステンション モビリティ ユーザのプロファイル（具体的には、デバイス プロファイル内に設定されている回線コーリング サーチ スペース）に従ってルーティングされます。これは、通常、これらの公衆網コールが 2 つの WAN リンクを通過し、サイト 1 のゲートウェイを使用して公衆網にアクセスすることを意味します。

この動作を修正し、エクステンション モビリティ ユーザが別のサイトにローミングしている場合でも、公衆網コールが常にローカル公衆網ゲートウェイを通じてルーティングされるようにするには、次のいずれかの方法を使用します。

- ローカル公衆網ルート パターンは、デバイス コーリング サーチ スペースに含めて、デバイス プロファイル内の回線コーリング サーチ スペースからは削除します。この方法によって、ローカルの公衆網コールは、同じ場所にある支店ゲートウェイを通じてルーティングされるようになります。ただし、同時に、ユーザは IP Phone にログインしなくてもこれらのコールをダイヤルできるようになります。長距離電話と国際コールについては、エクステンション モビリティ ユーザのデバイス プロファイルに従ってルーティングされます。したがって、このソリューションが適しているのは、通常これらのコールが中央ゲートウェイを通じてルーティングされている場合のみです。
- 各ユーザに対して、ユーザがローミングするサイトごとに 1 つずつ、複数のデバイス プロファイルを定義します。各デバイス プロファイルの設定では、回線コーリング サーチ スペースが、そのサイトのローカル ゲートウェイを使用する公衆網ルート パターンを指すようにします。ローミングするユーザおよびローミング先となるサイトが非常に多い場合、この方法は設定と管理の負荷が大きくなります。
- 次の項（「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.9-59））で説明する回線 / デバイス アプローチを実装します。

（注）　Cisco Emergency Responder を使用する場合は、デバイスに設定するサイト固有のコーリング サーチ スペースに、Cisco Emergency Responder を指す 911 CTI ルート ポイントを含むパーティションを含める必要があります。その同じパーティションに、同じ 911 CTI ルート ポイントを指すトランスレーション パターン 9.911 も含めると、ユーザは 9911 をダイヤルして救急サービスに連絡できます。

回線/デバイス アプローチによる Unified CM のサービス クラスの構築

前の項で説明した従来のアプローチは、集中型コール処理を使用した大規模なマルチサイト配置に適用する場合、結果的にパーティションとコーリング サーチ スペースの数が非常に多くなることがあります。このような構成にする必要があるのは、デバイス コーリング サーチ スペースを使用して、パス選択（外部コールにどの公衆網ゲートウェイを使用するか）とサービス クラスの両方を決定しているためです。

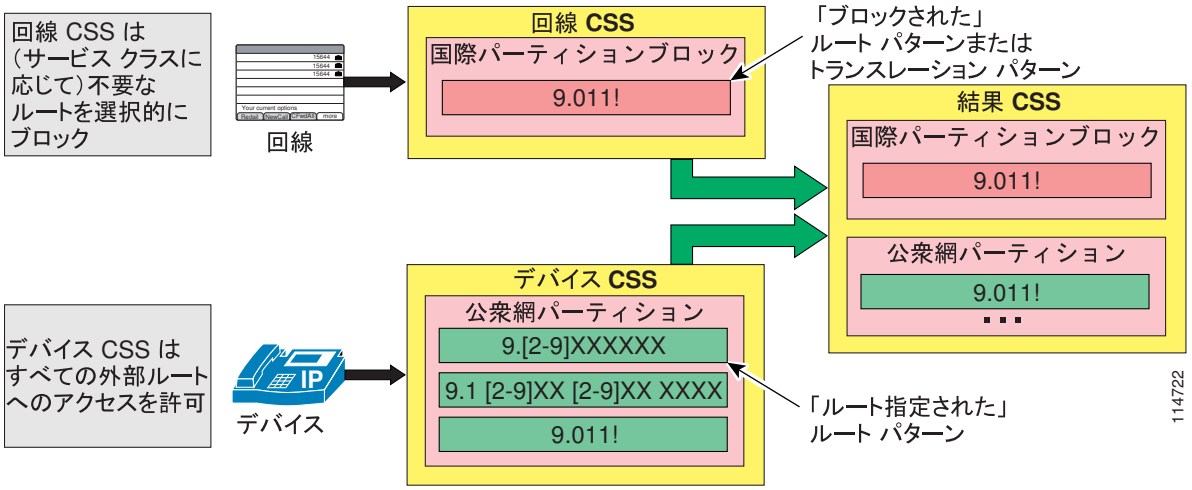
これらの 2 つの機能を回線コーリング サーチ スペースとデバイス コーリング サーチ スペースに分配すると、必要となるパーティションとコーリング サーチ スペースの総数を大幅に減らすことができます。この手法を*回線/デバイス アプローチ*と呼びます。

所定の各 IP Phone の回線コーリング サーチ スペースとデバイス コーリング サーチ スペースが Unified CM でどのように組み合されているか、および回線コーリング サーチ スペースのパーティションが、結果のコーリング サーチ スペースでどのようにして最初に表示されるのか（「Unified CM におけるコール特権」（P.9-95）を参照）に注目すると、回線/デバイス アプローチでは、一般に次の規則を適用できます。

- デバイス コーリング サーチ スペースは、コール ルーティング情報（たとえば、どのゲートウェイを公衆網コール用に選択するか）を提供するために使用します。
- 回線コーリング サーチ スペースは、サービス クラス情報（たとえば、どのコールを許可するか）を提供するために使用します。

これらの規則がどのように適用されるのかをわかりやすくするために、図 9-16 に示す例について考えます。このデバイス コーリング サーチ スペースは、国際番号を含めて、すべての公衆網番号へのルート パターンが入ったパーティションを保持しています。このルート パターンは、ルート リストおよびルート グループを通じて、公衆網ゲートウェイを指しています。

図 9-16　回線/デバイス アプローチにおける重要な概念



同時に、回線コーリング サーチ スペースは、トランスレーション パターンが 1 つのみ入ったパーティションを保持しています。このパターンは国際番号に一致し、ブロック パターンとして設定されています。

したがって、結果のコーリング サーチ スペースには、国際番号に一致する 2 つの同一パターンが保持されています。最初に表示されるのは、回線コーリング サーチ スペースに含まれているブロック パターンです。結果として、この回線からの国際通話はブロックされます。

回線コーリング サーチ スペースでは、トランスレーション パターンの代わりに、ルート パターンを使用してコールをブロックすることもできます。ブロック ルート パターンを設定するには、まず、使用されていない IP アドレスを使用して「ダミー」ゲートウェイを作成し、そのゲートウェイを「ダミー」ルート リストおよびルート グループに配置します。次に、ダミー ルート リストを指すようにルート パターンを設定します。コールをブロックするルート パターンとトランスレーション パターンの主な違いは、ブロックされている番号をエンド ユーザがダイヤルしようとしたときの対応です。次に例を示します。

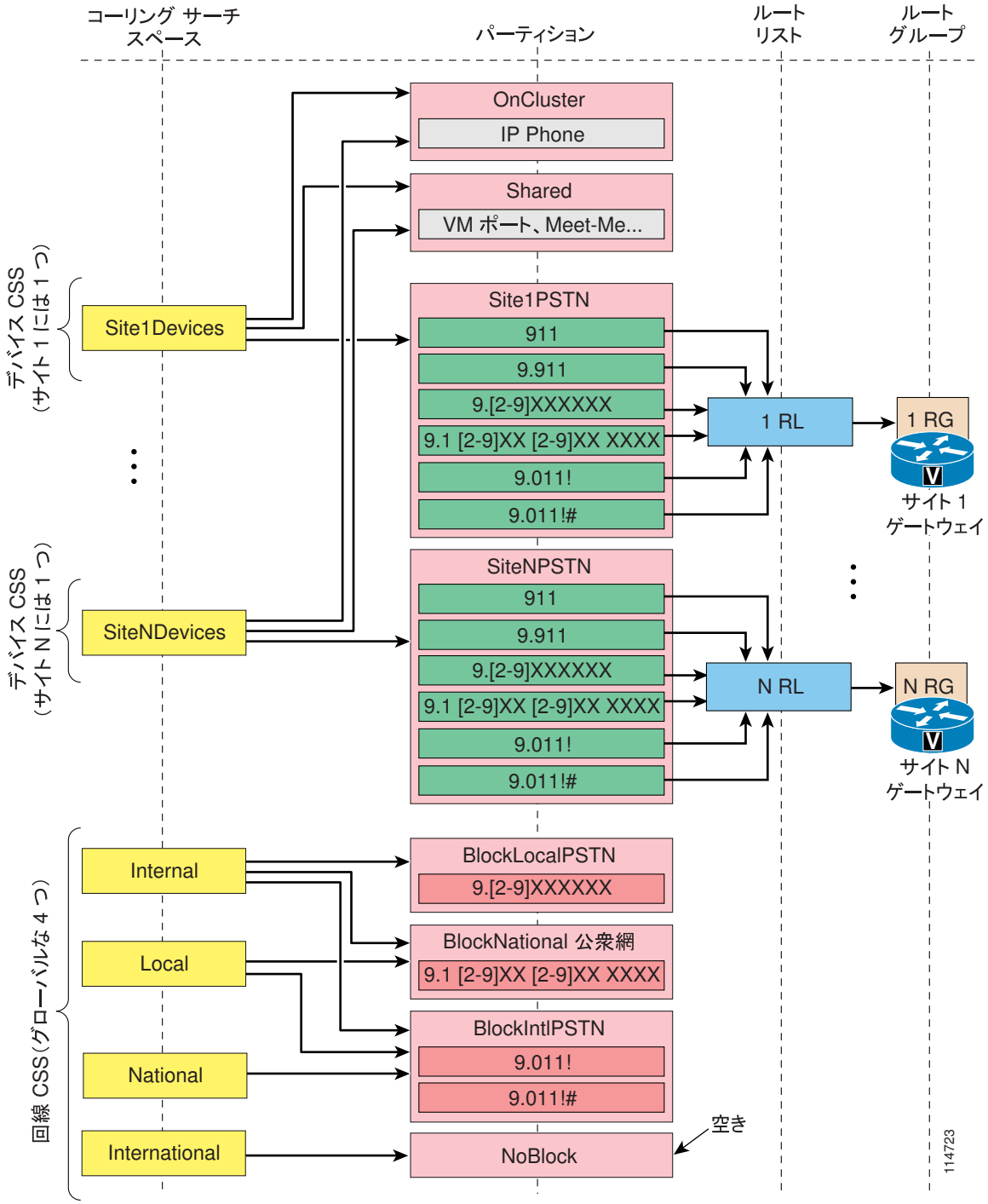
- ルート パターンを使用した場合、エンド ユーザは番号を最後までダイヤルでき、ダイヤルが完了して初めてユーザにファーストビジー トーンが再生されます。
- トランスレーション パターンを使用した場合は、エンド ユーザのダイヤルしている番号が許可パターンに一致する可能性がなくなると、その時点ですぐにファーストビジー トーンが再生されます。この動作は、SCCP を実行している IP Phone、または SIP を実行し、電話機に SIP ダイヤル規則が設定されていないタイプ B の IP Phone を前提にしています。

集中型コール処理を使用するマルチサイト配置に対して回線/デバイス アプローチを実装する場合は、さらに次のガイドラインに従ってください。

- サイトごとに無制限のコーリング サーチ スペースを作成し、電話機のデバイス コーリング サーチ スペースに割り当てます。このコーリング サーチ スペースには、電話機のロケーションに適したゲートウェイ（たとえば、同じ場所に配置されている緊急サービス用の支店ゲートウェイと、長距離電話用の中央ゲートウェイ）にコールをルーティングするルート パターンを備えたパーティションが含まれていなければなりません。
- ユーザのダイヤリング権限に含まれていないタイプのコールに対するブロック トランスレーション/ルート パターンを備えたパーティションを含むコーリング サーチ スペースを作成し、ユーザの回線に割り当てます。たとえば、ユーザが国際コール以外のすべてのタイプのコールを利用できる場合、そのユーザの回線は、9.011! ルート パターンをブロックするコーリング サーチ スペースを使用して設定する必要があります。

図 9-17 は、N 個のサイトがあるマルチサイト配置に対して、これらのガイドラインを適用する方法の例を示しています。

図 9-17　回線 / デバイス アプローチで必要となるコーリング サーチ スペースとパーティション



この方法の利点として、サイトごとに必要なサイト固有の無制限コーリング サーチ スペースが支店に 1 つのみであるという点があります。ダイヤリング権限は、ブロック ルート パターン（サイトに依存しない）の使用により実装されるので、同じセットのブロック コーリング サーチ スペースをすべての支店で使用できます。

結果として、必要なコーリング サーチ スペースの合計数とパーティションの合計数を計算するには、次の公式を使用できます。

合計パーティション数 =（サービス クラス数）+（サイト数）+（すべての IP Phone の DN 用に 1 パーティション）

合計コーリング サーチ スペース数 =（サービス クラス数）+（サイト数）

（注） これらの値は、最低限必要となるパーティション数とコーリング サーチ スペース数を表しています。特殊なデバイスやアプリケーションには、他のコール処理エージェント用のオンネット パターンと同様に、追加のパーティションやコーリング サーチ スペースが必要になることがあります。

（注） Cisco Emergency Responder を使用する場合は、911 CTI ルート パターンと 9.911 トランスレーション パターンをグローバルなオンクラスタ パーティションに含めることができます。

サイトの数が多い集中型コール処理配置に対して回線/デバイス アプローチを適用すると、必要となるパーティションとコーリング サーチ スペースの数が大幅に減少します。たとえば、100 のリモート サイトと 4 つのサービス クラスがある配置の場合、従来のアプローチでは、少なくとも 401 のパーティションと 400 のコーリング サーチ スペースが必要です。回線/デバイス アプローチでは、105 のパーティションと 104 のコーリング サーチ スペースしか必要ありません。

ただし、回線/デバイス アプローチが成立するのは、特定サービス クラスの使用を制限する必要のある公衆網コールのタイプ（たとえば、市内電話、長距離電話、国際コール）を、グローバルに識別できる場合です。使用している国の国内番号計画が原因で、コール タイプをグローバルに識別することができない場合、このアプローチの効果は、（設定の省力化に関しては）上の公式に示したものよりも小さくなります。

たとえば、フランスでは、番号計画は 5 桁のエリア コード（01 ～ 05、および携帯電話の 06 エリア コード）に基づいており、この後に 8 桁の加入者番号が続きます。ここで重要となる特徴は、各公衆網宛先に到達するとき、同じローカルエリアからコールするときも、別のエリアからコールするときも、必ず同じ番号（たとえば、Paris の番号は 01XXXXXXXX、Nice の番号は 04XXXXXXXX など）をダイヤルすることです。つまり、「長距離電話」であるかどうかは、発信者がどのエリアにいるかに応じて変化します。このため、1 つのパーティションと 1 つのルート パターンでは、長距離電話へのアクセスをブロックできません。たとえば、発信者が Paris にいる場合、014455667788 へのコールは市内電話ですが、発信者が Nice や Lyon にいる場合は長距離電話です。

このような場合は、市内電話と長距離電話が同じ方法でダイヤルされるエリアごとに 1 つずつ、一連のブロック用コーリング サーチ スペースとパーティションを追加設定する必要があります。フランスの例では、表 9-8 に示すように、各エリア コードに対して 1 つずつ、5 組のブロック用コーリング サーチ スペースとパーティションを追加で定義する必要があります。

表 9-8　フランス国内番号計画に適用される回線/デバイス アプローチ

コーリング サーチ スペース	パーティション	ブロック ルート パターン
Internal_css	BlockAllNational_pt	0.0[1-6]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#
Local01_css	BlockLD01_pt	0.0[2-6]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#
Local02_css	BlockLD02_pt	0.0[13-6]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#

表 9-8　フランス国内番号計画に適用される回線/デバイス アプローチ（続き）

コーリング サーチ スペース	パーティション	ブロック ルート パターン
Local03_css	BlockLD03_pt	0.0[124-6]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#
Local04_css	BlockLD04_pt	0.0[1-356]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#
Local05_css	BlockLD05_pt	0.0[1-46]XXXXXXXX
	BlockIntl_pt	0.00!、0.00!#
LD_css	BlockIntl_pt	0.00!、0.00!#
Intl_css	NoBlock_pt	なし

回線/デバイス アプローチのガイドライン

回線/デバイス アプローチを使用する場合は、次のガイドラインを考慮してください。

- このアプローチが機能するには、回線コーリング サーチ スペース内に設定するブロック パターンの詳細度が、デバイス コーリング サーチ スペース内に設定したルート パターンと少なくとも同等になっている必要があります。エラーが発生することを避けるために、ブロックの対象となるパターンは、可能な場合にはルーティングを許可するパターンよりも詳細に設定することを推奨します。@ ワイルドカード内に定義されるパターンは非常に詳細なものになるため、このワイルドカードの取り扱いには十分に注意してください。
- オンネット DN がダイヤルされると、AAR がトリガーされます。これらの DN へのアクセスは、上で説明したものと同じプロセスで制御できます。AAR は、再ルーティングされるコールには別のコーリング サーチ スペースを使用します。ほとんどの場合、AAR コーリング サーチ スペースは、サイト固有の無制限デバイス コーリング サーチ スペースと同じものでかまいません。このコーリング サーチ スペースは、エンド ユーザによって直接ダイヤルされることがないためです。
- Call Forward All 動作に対する回線/デバイス アプローチのガイドラインについては、「自動転送コーリング サーチ スペース」（P.9-99）の項を参照してください。

（注）　回線とデバイスの優先順位は、CTI デバイス（CTI ルート ポイントと CTI ポート）に関しては逆になります。これらのデバイスの場合、結果のコーリング サーチ スペースでは、デバイス コーリング サーチ スペースに含まれているパーティションが、回線コーリング サーチ スペースよりも前に配置されます。そのため、パターン選択を連結の順序だけに頼らず、ブロックされるパターンの精度が許可されるパターンの精度よりも、すべてのケースで確実に高くなるよう注意しなければ、回線/デバイス アプローチを Cisco IP SoftPhone などの CTI デバイスに適用できません。

グローバル化された番号とサービス クラス

コーリング サーチ スペースに対する回線/デバイス アプローチを使用しているシステム管理者は、エンドポイントの回線 CSS で使用されるブロック パターンがローカル化された形式だけではなく、グローバル化された形式のコールもブロックする可能性があることに注意してください。ローカル化された形式の番号は local、regional、national に分類されますが、グローバル化された形式は分類されません。これによりサービス クラスの不一致が生じます。直接ユーザ ダイヤリングはサービス クラスに従属するのに対して、不在履歴リストと着信履歴リストからのワンタッチ ダイヤリングは従属しません。

たとえば、カナダのオンタリオ州 Ottawa にローカル サービス クラスを作成するとします。Ottawa のすべてのローカル コールはエリア コード 613 と 819 に分類され、ローカル コーリングは 10 桁のダイヤリングを使用して実行されます。ローカル化されたユーザ入力のみが Ottawa の電話機で許可されている場合、9[2-9]XX[2-9]XXXXXX の形式で行われたコールのみを許可することにより、「ローカル」

サービス クラスを電話機に適用できます。国内の（長距離）宛先に行われたすべてのコールは、国際電話（9 の後に 011）のように、異なるダイヤリング形式（オフネットのアクセス コード 9 の後に国内振り分けコード 1、その後に番号）で始まります。コールの形式によりクラスが定義されます。

ワンタッチ ダイヤルを実行する場合、電話機のダイヤル プランでローカル番号のグローバル形式が許可されます。ルート パターン +1 613 [2-9]XX XXXX ともう 1 つのパターン +1 819 [2-9]XX XXXX を追加して、ローカル コールが不在履歴または着信履歴コール リストからワンタッチ ダイヤルできるようにします。

ただし、すべての 613 および 819 エリア コード宛先がローカル コールとなるわけではないので、さらに複雑です。ローカル化されたパターンにより、ユーザがローカル宛先に対してのみコールを開始することを許可された場合（ダイヤル ストリングの先頭で 9 819 または 9 613 とダイヤル）、グローバル化されたパターンでは、エリア コード 613 または 819 のローカル以外の番号からのコールの受信が許可され、受信コール リストに移動し、番号をワンタッチ ダイヤルで返し、グローバル化されたパターンと照合します。このような場合、ルート パターンのグローバル形式は、ローカル コーリング エリアそのものを表すように修正する必要があります。上の例では、Ottawa のローカル コーリング エリア内のエリア コード 613 および 819 の正確なサブセットの定義を含みます。

回線/デバイス アプローチにおけるエクステンション モビリティの考慮事項

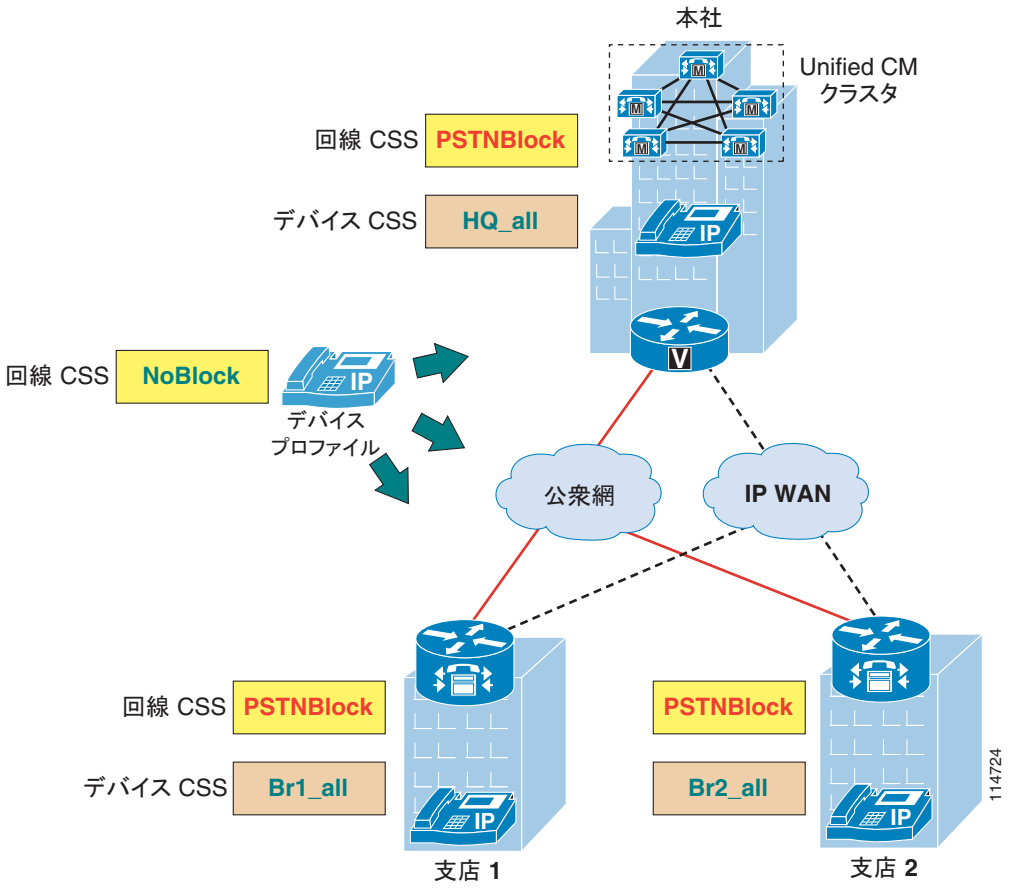
エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、回線/デバイス アプローチを使用することによって、その電話機へのログイン（またはログアウト）中の機能の 1 つとして自然な方法で実装できます。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

サービス クラスの構築に回線/デバイス アプローチを使用する場合は、前の項で説明したものと同じ規則を、エクステンション モビリティのデバイス プロファイル コンストラクトに適用するだけで済みます。エクステンション モビリティ使用時にコール制限を適用するには、次のガイドラインを考慮してください。

- 一致する可能性のあるすべての公衆網ルート パターンが入っていて、それらのパターンを適切にルーティングする（たとえば、緊急コールと市内電話にはローカル ゲートウェイを使用し、長距離電話には中央ゲートウェイを使用する）サイト固有のパーティションを指すように、各サイトのすべての IP Phone のデバイス コーリング サーチ スペースを設定します。
- ユーザがログインしていないときでも許可されるコール（たとえば、内部内線番号と緊急サービス）以外のコールをすべてブロックするブロック トランスレーション/ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、すべての IP Phone の回線コーリング サーチ デバイス（または、デフォルト ログアウト デバイス プロファイルの回線コーリング サーチ スペース）を設定します。
- エクステンション モビリティ ユーザごとに、特定のサービス クラスに対して許可しない公衆網コールを選択してブロックする（たとえば、国際コールのみをブロックする）ブロック トランスレーション/ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、回線コーリング サーチ スペースをデバイス プロファイル内に設定します。一部のユーザに無制限のコール特権を与える必要がある場合は、それらのユーザを空のパーティションを備えた回線コーリング サーチ スペースに割り当てます。

エクステンション モビリティに回線/デバイス アプローチを使用することの主な利点は、図 9-18 に示すように、集中型コール処理を使用するマルチサイト配置において、ユーザがホーム サイト以外の支店サイトにある IP Phone にログインしている場合でも、適切なコール ルーティングが保証されることです。

図 9-18　回線 / デバイス アプローチを使用したエクステンション モビリティ



この章ですでに説明したように、デバイス プロファイル内に設定した回線コーリング サーチ スペースは、ユーザがエクステンション モビリティを通じてログインすると、物理 IP Phone 上に設定されている回線コーリング サーチ スペースを置き換えます。コール ルーティングはデバイス コーリング サーチ スペースによって正しく処理されるため、ログイン操作は、単に電話のロックを解除するために使用されます。ログイン操作によって、（ブロック パターンを含んでいる）電話の回線コーリング サーチ スペースが削除され、（この単純化した例では、ブロック パターンを保持していない）デバイス プロファイルの回線コーリング サーチ スペースに置き換えられます。

コール ルーティングがすべてデバイス コーリング サーチ スペースの内部で実行されるのに対して、回線コーリング サーチ スペースは、単にブロック パターンを導入するだけです。このため、ユーザは、ホーム サイト以外のサイトにログインした場合、そのサイトのローカル ダイヤリング手順を自動的に継承します。たとえば、電話の DN は 8 桁番号として定義されているものの、各サイトの内部では、ローカル トランスレーション パターンによって 4 桁ダイヤリングが提供されているとします。この場合、別のサイトにローミングしたユーザは、ホーム サイトにいる同僚に 4 桁のみダイヤルして到達することはできなくなります。4 桁の番号は、ユーザがログインしたホスト サイトの規則に従って変換されるためです。

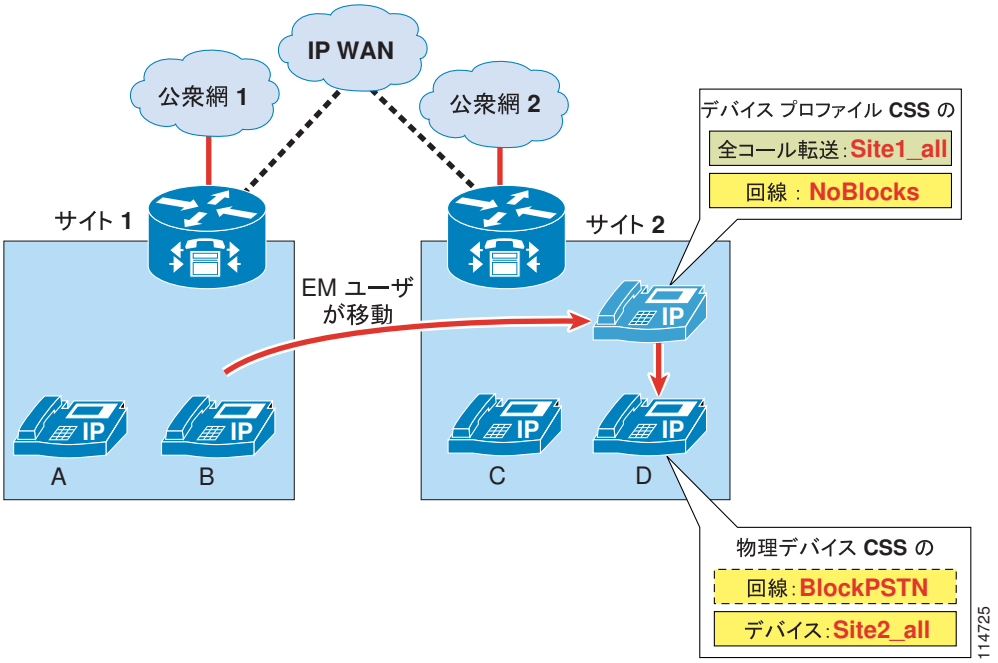
つまり、回線 / デバイス アプローチをエクステンション モビリティに使用する場合は、エンド ユーザがログイン先サイトのダイヤリング手順に従う必要があります。

自動転送の考慮事項

エクステンション モビリティを使用する集中型コール処理環境に対して回線 / デバイス コーリング サーチ スペース アプローチを適用する場合、ユーザがすべてのコールを外部公衆網番号に転送できるようにする必要があるときは、自動転送の動作に注意する必要があります。

図 9-19 では、エクステンション モビリティ ユーザが通常はサイト 1 を拠点としていて、そのデバイス プロファイルでは、無制限に公衆網コールを発信し、すべての着信コールを任意の公衆網番号に転送することが許可されています。

図 9-19　回線 / デバイス アプローチを使用したエクステンション モビリティにおける自動転送の考慮事項



「自動転送コーリング サーチ スペース」（P.9-99）の項で説明したように、Forward All コーリング サーチ スペースは、回線およびデバイスのコーリング サーチ スペースとは連結されないため、Site1_all に設定する必要があります。Site1_all は、サイト 1 のゲートウェイを使用するすべての公衆網ルートを含んでいます。

このユーザがサイト 2 に移動して電話機 D にログインすると、ユーザのデバイス プロファイルに従って、このプロファイルの回線コーリング サーチ スペースと Forward All コーリング サーチ スペースが物理デバイスに適用されます。直接公衆網コールの場合、使用されるコーリング サーチ スペースは、回線とデバイスのコーリング サーチ スペースを連結したものです。電話 D のデバイス コーリング サーチ スペース（Site2_all）は、サイト 2 のゲートウェイを正しく指しています。

このユーザが、すべてのコールを公衆網番号に転送するように電話を設定すると、転送されるすべてのコールは、Site1_all コーリング サーチ スペースを使用します。Site1_all は、サイト 1 のゲートウェイを指したままです。この状態になると、次のような動作が発生します。

- 着信公衆網コールは、サイト 1 のゲートウェイで IP ネットワークに入り、同じゲートウェイ内で公衆網にヘアピンされます。
- サイト 1 の電話（電話機 A など）から発信されるコールは、サイト 1 のゲートウェイを通じて公衆網に正しく転送されます。

- サイト 2 の電話（電話機 C など）から発信されるコールは、WAN を経由してサイト 1 に到達し、サイト 1 のゲートウェイを通じて公衆網にアクセスします。同じ Unified CM クラスタ内の他のサイトから発信されるコールに対しても、同じ動作が適用されます。

ネットワークを設計し、ユーザをトレーニングするときは、この動作に注意してください。

H.323 を使用している Cisco IOS でのサービス クラスの構築

次のシナリオでは、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを定義する必要があります。

- 集中型コール処理を使用する Cisco Unified CM マルチサイト配置
- Cisco Unified Communications Manager Express（Unified CME）配置

集中型コール処理を使用した Unified CM マルチサイト配置では、通常、Unified CM 内のパーティションとコーリング サーチ スペースを使用してサービス クラスが実装されます。ただし、支店サイトと中央サイト間の IP WAN 接続が失われた場合は、Cisco SRST が支店 IP Phone の制御を取得し、パーティションとコーリング サーチ スペースに関する設定は、IP WAN 接続が復旧するまですべて使用できなくなります。したがって、SRST モードで動作している支店ルータ内にサービス クラスを実装することが望ましくなります。

同様に、Cisco Unified CME Express 配置の場合も、ルータには IP Phone 用のサービス クラスを実装するメカニズムが必要です。

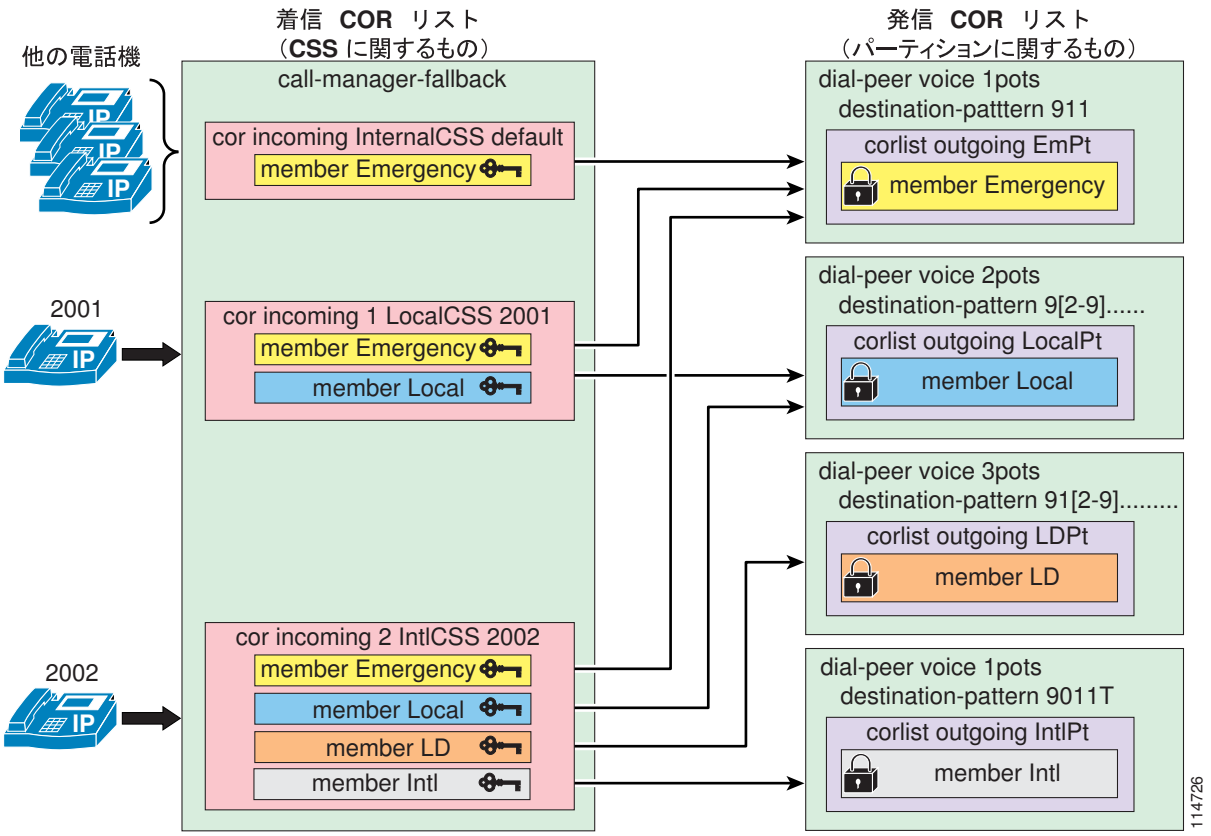
どちらの事例でも、Class Of Restriction（COR; 制限クラス）機能を使用して、サービス クラスを Cisco IOS ルータ内に定義します（COR の詳細については、「H.323 ダイヤル ピアを使用する Cisco IOS のコール特権」（P.9-137）を参照）。

次の主要ガイドラインに従うと、COR 機能を調整して、Cisco Unified CM のパーティションとコーリング サーチ スペースという概念を再現できます。

- 区別する必要のあるコールのタイプごとに、タグを定義する。
- 各コール タイプをルーティングするそれぞれの POTS ダイヤル ピアに対して、メンバー タグを 1 つだけ含んだ、「基本的な」発信 COR リスト（パーティションに相当）を割り当てる。
- 各種のサービス クラスに属している IP Phone に対して、メンバー タグのサブセットを含んだ、「複雑な」着信 COR リスト（コーリング サーチ スペースに相当）を割り当てる。

図 9-20 では、SRST に基づいた実装例を示しています。DN が 2002 の IP Phone は、無制限の公衆網アクセスを許可され、DN が 2001 の IP Phone は、ローカル公衆網アクセスのみを許可されています。その他のすべての IP Phone は、内部番号と緊急サービスにのみアクセスできるように設定されています。

図 9-20　COR を使用した Cisco SRST 用サービス クラスの構築



次の手順では、図 9-20 のような Cisco IOS ソリューションの実装例とガイドラインを示します。

ステップ 1　**dial-peer cor custom** コマンドを使用して、各種コールの内容をわかりやすく表しているタグを定義します（この例では、Emergency、VMail、Local、LD、Intl）。

```
dial-peer cor custom
  name Emergency
  name VMail
  name Local
  name LD
  name Intl
```

ステップ 2　**dial-peer cor list** コマンドを使用して、パーティションとして使用される基本的な COR リストを定義します。各リストには、タグを 1 つのみメンバーとして含めます。

```
dial-peer cor list EmPt
  member Emergency

dial-peer cor list VMailPt
  member VMail

dial-peer cor list LocalPt
  member Local

dial-peer cor list LDPt
  member LD

dial-peer cor list IntlPt
  member Intl
```

ステップ 3　**dial-peer cor list** コマンドを使用して、コーリング サーチ スペースとして使用される比較的複雑な COR リストを定義します。各リストには、必要となるサービス クラスに従って、タグのサブセットをメンバーとして含めます。

```
dial-peer cor list InternalCSS
  member Emergency
  member VMail

dial-peer cor list LocalCSS
  member Emergency
  member VMail
  member Local

dial-peer cor list LDCSS
  member Emergency
  member VMail
  member Local
  member LD

dial-peer cor list IntlCSS
  member Emergency
  member VMail
  member Local
  member LD
  member Intl
```

ステップ 4　**corlist outgoing** *corlist-name* コマンドを使用して、基本的な「パーティション」COR リストを、対応する POTS ダイヤル ピアに割り当てる発信 COR リストとして設定します。

```
dial-peer voice 100 pots
  corlist outgoing EmPt
  destination-pattern 911
  no digit-strip
  direct-inward-dial
  port 1/0:23

dial-peer voice 101 pots
  corlist outgoing VMailPt
  destination-pattern 914085551234
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 102 pots
  corlist outgoing LocalPt
  destination-pattern 9[2-9].....
  forward-digits 7
  direct-inward-dial
  port 1/0:23

dial-peer voice 103 pots
  corlist outgoing LDPt
  destination-pattern 91[2-9]..[2-9].....
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 104 pots
  corlist outgoing IntlPt
  destination-pattern 9011T
  prefix-digits 011
  direct-inward-dial
  port 1/0:23
```

ステップ 5　**cor incoming** コマンドを **call-manager-fallback** コンフィギュレーション モードで使用して、「コーリング サーチ スペース」として機能する複雑な COR リストを、各種の電話 DN に割り当てる着信 COR リストとして設定します。

```
call-manager-fallback
  cor incoming InternalCSS default
  cor incoming LocalCSS 1 3001 - 3003
  cor incoming LDCSS 2 3004
  cor incoming IntlCSS 3 3010
```

SRST 用の COR を配置する場合は、次の制限事項に注意してください。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

したがって、デフォルト以外の特権を持つユーザの電話 DN が連続しておらず、SRST サイトが比較的大きい場合は、SRST モードのサービス クラスの数を減らして、これらの制限値を超えずにすべての DN に対応できるようにする必要があります。

上の例は Cisco SRST に基づいていますが、Cisco Unified Communications Manager Express（Unified CME）配置にも同じ概念を適用できます。ただし、次の考慮事項があります。

- Unified CME を使用している場合は、サービス クラスを表現している COR リスト（コーリング サーチ スペースに相当するもの）を個々の IP Phone に直接割り当てることができます。割り当てるには、**cor** {**incoming** | **outgoing**} *corlist-name* コマンドを **ephone-dn** *dn-tag* コンフィギュレーション モードで使用します。
- COR リストの設定されていない IP Phone は、COR の一般規則に従って、発信 COR リストの内容に関係なくすべてのダイヤル ピアに無制限にアクセスできます。Unified CME は、すべての電話にデフォルトの制限を適用する、**cor incoming** *corlist-name* **default** コマンドに相当するメカニズムを備えていません。

コール カバレッジの配置

コール カバレッジ機能は、多くの IP テレフォニー配置で重要となる機能です。顧客サービスを重視する多くの企業では、顧客のコールを適切なサービス部門に迅速にルーティングすることが必須になります。この項では、ハント パイロット、ハント リスト、および回線グループに基づいたハンティング メカニズムを使用して、Cisco Unified CM Release 4.1 でコールを分配する場合の設計ガイドラインを中心に説明します。ここでは、次のトピックを主に扱います。

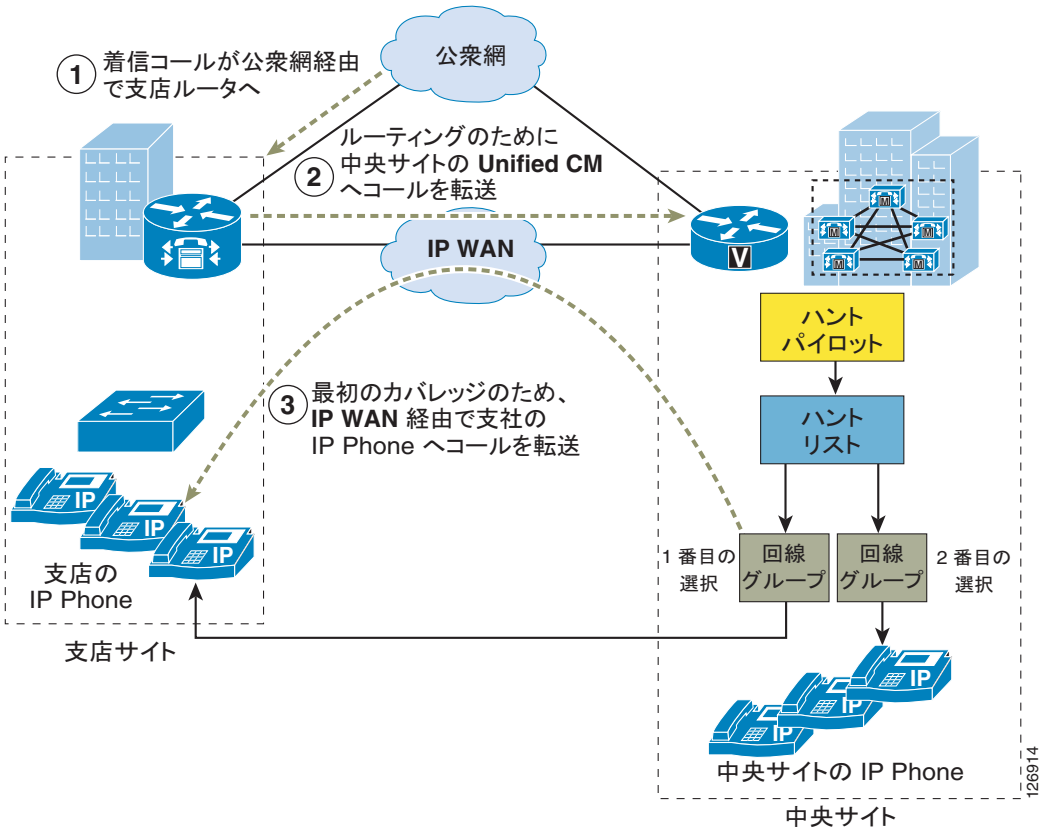
- 「マルチサイト集中型コール処理モデルへのコール カバレッジの配置」（P.9-71）
- 「マルチサイト分散型コール処理モデルへのコール カバレッジの配置」（P.9-72）

（注）　コール カバレッジ機能自体はコール キューを提供せず、発信側には、コールの宛先が見つかるまでリングバック トーンが送信されます。プロンプトや保留音などを提供するため、シスコでは Cisco Unified Customer Voice Portal（CVP）などの多数のコンタクト センター テクノロジーを用意しています。シスコから入手可能なコンタクト センター テクノロジーの詳細については、http://www.cisco.com/go/ucsrnd で入手可能な資料を参照してください。

マルチサイト集中型コール処理モデルへのコール カバレッジの配置

図 9-21 では、マルチサイトの集中型コール処理配置における、ハント リストの設定例を示しています。この例では、最初にリモート オフィスのオペレータを通じてハント パイロット コールが分配されることを前提としています。コールは、応答されなかった場合やコール アドミッション制御によって拒否された場合、中央サイトのオペレータまたはボイスメールにルーティングされます。

図 9-21　集中型コール処理配置における複数のサイト間でのコール カバレッジ



集中型の IP テレフォニー システムでは、Automated Alternate Routing（AAR）や Survivable Remote Site Telephony（SRST）などの機能を有効にすることで、高い可用性を実現できます。AAR 機能や SRST 機能を有効にしたうえでコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- Automated Alternate Routing（AAR）

  回線グループのメンバーは、複数のロケーションおよびリージョンに割り当てることができます。ロケーションを通じて実装したコール アドミッション制御は、想定どおりに動作します。ただし、ハント パイロットから分配されているコールは、WAN の帯域幅が不足していたためにいずれかの回線グループ メンバーへのコールが Unified CM によってブロックされた場合には、AAR を使用して再ルーティングされることはありません。代わりに、Unified CM はコールを使用可能な次のメンバーまたは回線グループに分配します。

（注） AAR のみを使用する場合は、回線グループ内でボイスメール ポートを使用することを強く推奨します。

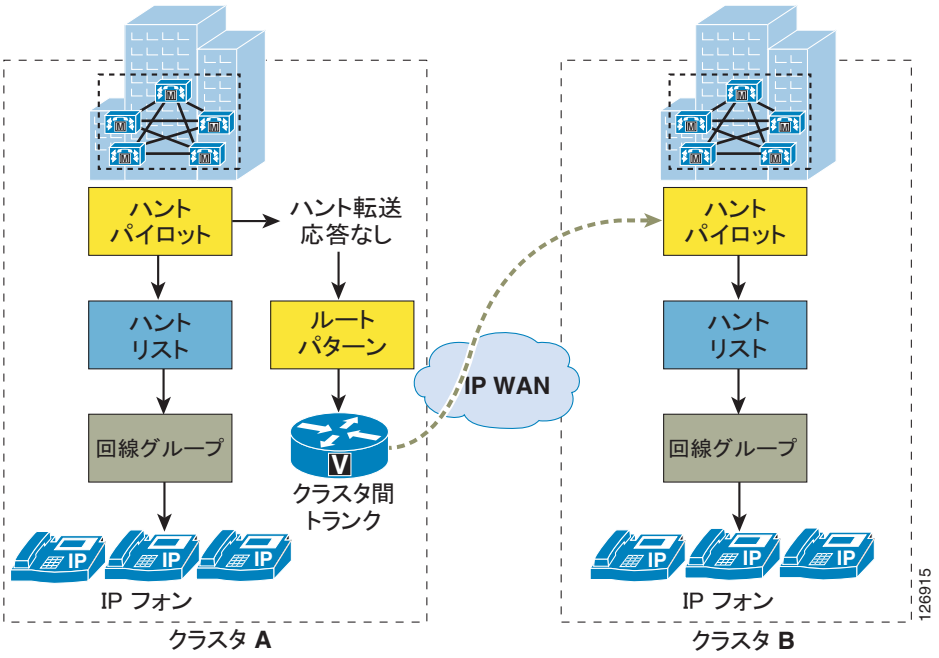
- Survivable Remote Site Telephony（SRST）
  - Unified CM がハント パイロットのコールを受信したとき、その回線グループ メンバーの一部が、SRST モードで動作しているリモート サイトにある場合、Unified CM はそれらのメンバーをスキップし、使用可能な次の回線グループ メンバーにコールを分配します。Unified CM から見ると、SRST モードで動作しているメンバーは未登録であり、ハント パイロットのコールは未登録メンバーには転送されません。
  - SRST モードで動作しているルータがハント パイロットのコールを受信したときは、コール カバレッジ機能を使用できません。このコールは、使用可能な登録済み内線番号にコールを再ルーティングする設定が追加されていない場合、失敗します。**alias** コマンドまたは **default-destination** コマンドを Cisco IOS の **call-manager-fallback** モードで使用すると、ハント パイロットを宛先とするコールをオペレータ内線またはボイスメールに再ルーティングできます。

マルチサイト分散型コール処理モデルへのコール カバレッジの配置

Cisco Unified CM Release 4.1 以降では、ルート グループをハント リストに追加することができなくなりました。このため、ハント リストを使用して、コールを他のクラスタまたはリモート ゲートウェイに送信することはできません。ただし、Cisco Unified CM Release 4.1 で導入されたハント パイロットのハント オプション設定を使用して、ゲートウェイまたはトランクを指すルート パターンに対応付けることができます。

図 9-22 は、クラスタ間トランクを使用する分散型コール処理配置における、ハント リストの設定例を示しています。この例では、ハント パイロットのコールが最初にクラスタ A の内部に配置されます。コールに対する応答がない場合は、ルート パターンに一致する Forward Hunt No Answer 設定を使用して、コールがコール分配のためにクラスタ B に再ルーティングされます。このルート パターンは、クラスタ B に向かうクラスタ間トランクを指しています。

図 9-22　分散型コール処理配置におけるクラスタ間でのコール カバレッジ



ヒント　分散型コール処理配置では、Cisco VoIP ゲートウェイとゲートキーパーを使用して、着信するハント パイロット コールのロード シェアリングを管理できます。あるクラスタ内でコールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することもできます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

ガイドライン

コール カバレッジ機能を分散型コール処理モデルに配置する場合、コールが複数のクラスタに分配されると、ルート パターンは発信または着信のルート グループ デバイス上で実行される番号変換を考慮に入れて、ルート パターンを適切に設定する必要があります。番号変換が実行されない場合、設定するルート パターンとハント パイロットは、すべてのクラスタ上で同一にする必要があります。同一でない場合は、コールが適切に分配されません。

ハント パイロットのスケーラビリティ

トップダウン、循環、および最長アイドル時間の各アルゴリズムを使用してコール カバレッジを配置する場合は、次のガイドラインを参考にすることを推奨します。

- Unified CM クラスタは、最大で 15,000 のハント リスト デバイスをサポートします。
- ハント リスト デバイスは、1,500 個のハント リストそれぞれに 10 台の IP Phone を入れた組み合せにすることも、750 個のハント リストそれぞれに 20 台の IP Phone を入れた組み合せにすることもできます。

（注）　コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Attempts（BHCA）の数によって制限されます。ブロードキャスト アルゴリズムを使用して、10 台の電話機を含むハント リストまたはハント グループを指すハント パイロットに対して 10 回の BHCA を行うことは、10 回の BHCA を行う 10 台の電話機と同じです。

- 1 つの回線グループ内に、コールをすべての DN に同時に送信することを目的として設定するディレクトリ番号の数は、最大で 35 までにすることを推奨します。また、ブロードキャスト回線グループの数は、BHCC によって決まります。Unified CM システム内に複数のブロードキャスト回線グループがある場合、回線グループ内のディレクトリ番号の数は、35 よりも少なくする必要があります。すべてのブロードキャスト回線グループの Busy Hour Call Attempt（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。

ダイヤル プランの要素

この項では、Cisco Unified Communication システムに含まれている次のダイヤル プラン要素について、設計と設定のガイドラインを示します。

- 「SCCP 電話機でのユーザ入力」（P.9-75）
- 「タイプ A の SIP 電話機でのユーザ入力」（P.9-76）
- 「タイプ B の SIP 電話機でのユーザ入力」（P.9-78）
- 「SIP ダイヤル規則」（P.9-80）
- 「Unified CM におけるコール ルーティング」（P.9-82）

IP Phone でのユーザ インターフェイス

さまざまな種類の IP 電話で、キーパッド入力が使用でき、視覚的な情報をさまざまな方法で提供します。この章では説明のため、次のタイプの電話機を定義します。

- タイプ A 電話機：Cisco Unified IP Phone 7905、7912、7940、および 7960
- タイプ B 電話機：Cisco Unified IP Phone 6901、6911、6921、6941、6945、6961、7906、7911、7921、7925、7931、7941、7942、7945、7961、7962、7965、7970、7971、7975、8961、9951、および 9971

IP Phone での発信側の変換

発信側トランスフォーメーション パターンを使用すると、電話機へのコールのルーティングに使用する発信側のグローバル形式の番号を、ユーザ指定のローカル形式に適応させることができます。

トランスフォーメーション パターンは、照合される発番号の数値表現で構成されます。使用される構文は、ルート パターン、トランスフォーメーション パターン、ディレクトリ番号などのその他パターンの構文と同じです。

変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号が含まれます。この演算子によって、発信側電話番号表示（Default、Allowed、または Restricted）が制御されます。発信側トランスフォーメーション パターンを設定することで、発信側の外部電話番号マスクを発番号として使用できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどの電話機に適用するかどうかが制御されます。電話機では、デバイス プールの発信側トランスフォーメーション コーリング サーチ スペース（CSS）またはデバイス固有の発信側トランスフォーメーション CSS を優先順位の低い順に使用できます。電話機に送信されるコールは、着信側トランスフォーメーション パターンを使用して処理されるのではありません。

電話機の場合は、発信側トランスフォーメーション パターンによって、電話機の呼び出し中に表示される番号が影響を受けます。不在コールと受信コールのディレクトリ内の対応するエントリは、変換された番号と元の変換前の番号の両方を保持します。変換された番号はディレクトリのリストに表示されますが、コールバックに使用される番号は変換前の番号です。

電話機での + ダイヤリングのサポート

タイプ A 電話機では、キーパッドを使用して + 記号をダイヤルすることはできません。タイプ B 電話機では、0 キー（Cisco Unified IP Phones 7921 および 7925）または * キー（他のすべての電話機モデル）のいずれかを押したままにして + 記号をダイヤルできます。Cisco Unified Personal Communicator エンドポイントでは、+ 記号はコンピュータのキーボードを使用して入力するか、エンドポイントのクリックツーダイヤル機能の使用時に入力文字列の一部として入力します。

タイプ A の電話機では、+ 記号の表示はサポートされていません。

タイプ B の電話機および Cisco Unified Personal Communicator では、着信コールは + を番号の一部として発番号として表示できます。コールが電話機に提供されたとき、呼び出し中の電話機に表示される番号は、設定された発番号トランスフォーメーション パターンによって処理されます。不在コールと受信コールのディレクトリは、元の変換前の番号と変換された番号の両方を保持します。リストに表示される番号は変換された番号になり、変換前の番号はエントリの詳細を確認したときにだけ表示されます。ディレクトリからダイヤルされた番号は元の変換前の番号であり、発信番号の一部として + 記号が使用された以前の受信コールをワンタッチでダイヤルできるようになります。

例 9-1　　+ ダイヤリングを使用する発番号

New York にあるタイプ B 電話機が +1 408 526 4000 からのコールを受信します。発信側トランスフォーメーション パターンは、電話機のデバイス プールの発信側変換 CSS に配置されています。パターンの 1 つは +1.!（ドットの前の番号を削除）と設定されています。

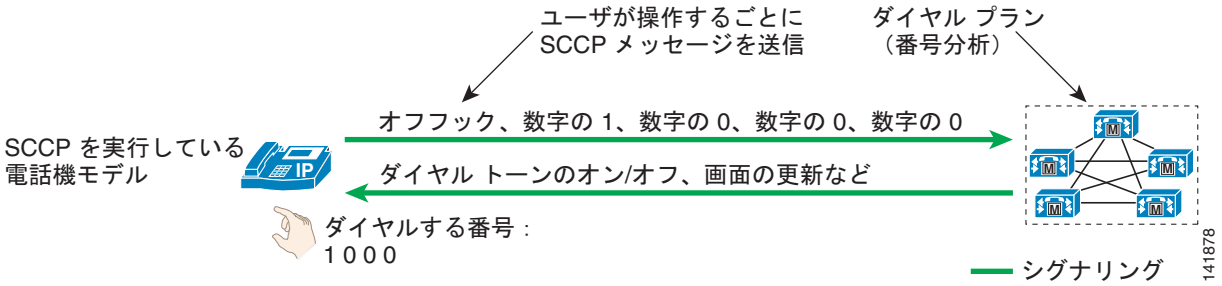
コールが鳴ると、着信側電話機に着番号 4085264000 が表示されます。コールに応答し、コールを解放した後、受信コール ディレクトリには最後のコールが 408 526 4000 として表示されますが、ユーザがディレクトリ エントリからコールバックを開始したときの着信番号は +1 408 526 4000 です。

SCCP 電話機でのユーザ入力

SCCP を使用する IP Phone は、すべてのユーザ入力イベントをただちに Unified CM に報告します。たとえば、ユーザがオフフックにするとすぐに、その電話機が登録されている Unified CM サーバに電話機からシグナリング メッセージが送信されます。電話機は 1 つの端末と考えることができ、Unified CM サーバに設定されたダイヤル プランによって、ユーザ入力に起因するすべての決定がその端末で下されます。

その他のユーザ イベントが電話機で検出されると、そのイベントは個別に Unified CM にリレーされます。オフフックして 1000 をダイヤルしたユーザは、電話機から Unified CM に 5 つの独立したシグナリング イベントをトリガーすることになります。その結果としてユーザに提供されるフィードバック、たとえば画面メッセージ、ダイヤル トーンの再生、2 次ダイヤル トーン、リングバック、リオーダーなどは、Unified CM がダイヤル プラン設定に基づいて電話機へ発行するコマンドです（図 9-23 を参照）。

図 9-23　SCCP 電話機でのユーザ入力とフィードバック



SCCP を実行する IP Phone 上にダイヤル プラン情報を設定する必要はなく、また設定できません。ダイヤル プラン機能は、ユーザ入力が収集されたときのダイヤリング パターンの認識も含めて、すべて Unified CM クラスタに含まれています。

ユーザのダイヤルしたパターンが Unified CM に拒否された場合は、そのパターンが Unified CM の番号分析でベストマッチになるとすぐに、そのユーザに対してリオーダー トーンが再生されます。たとえば、1 分刻みで課金される番号計画エリア（または市外局番）976 へのコールがすべて拒否される場合は、ユーザが 91976 をダイヤルするとすぐに、そのユーザの電話機にリオーダー トーンが送信されます。

タイプ A の SIP 電話機でのユーザ入力

タイプ A 電話機はタイプ B 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（「タイプ B の SIP 電話機でのユーザ入力」（P.9-78）を参照）。

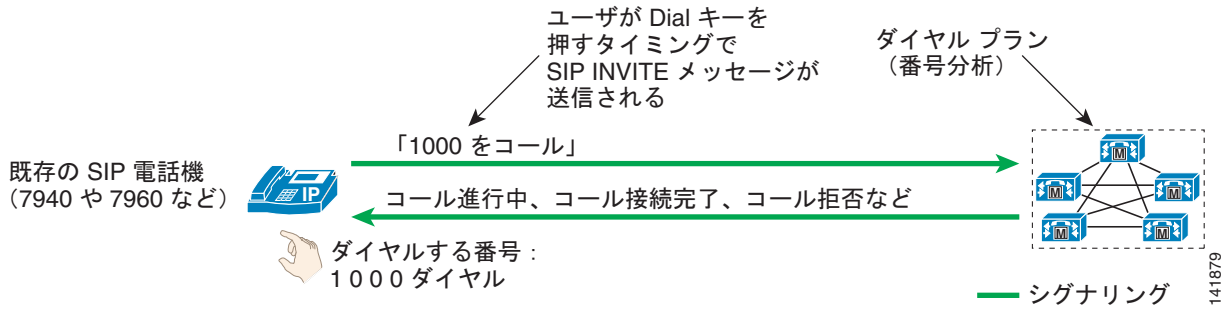
SIP を使用するタイプ A の IP Phone には、次の 2 つの異なる動作モードがあります。

- 「電話機に SIP ダイヤル規則が設定されていない場合」（P.9-76）
- 「電話機に SIP ダイヤル規則が設定されている場合」（P.9-77）

電話機に SIP ダイヤル規則が設定されていない場合

図 9-24 は、電話機にダイヤル プラン規則が設定されていない SIP タイプ A 電話機の動作を表しています。このモードでは、電話機はユーザが # キーを押すか [Dial] ソフトキーを押すまで、すべてのユーザ入力イベントを蓄積します。この機能は、多くの携帯電話で使用されている「送信」ボタンによく似ています。たとえば、内線 1000 にコールするユーザは、1、0、0、0 を押した後に [Dial] ソフトキーまたは # キーを押す必要があります。その後、電話機は Unified CM に SIP INVITE メッセージを送信し、内線 1000 へのコールの要求を示します。コールが Unified CM に到達すると、その電話機のダイヤル プラン設定に従います。その設定には、Unified CM のダイヤル プランに実装されているすべてのサービス クラスおよびコール ルーティング ロジックが含まれます。

図 9-24　ダイヤル規則が設定されていないタイプ A の SIP 電話機でのユーザ入力とフィードバック



ユーザが番号をダイヤルした後に [Dial] ソフトキーや # キーを押さなかった場合、電話機は桁間タイムアウト（デフォルトでは 15 秒）だけ待ってから、SIP INVITE メッセージを Unified CM に送信します。図 9-24 の例では、1、0、0、0 をダイヤルして桁間タイムアウトの時間だけ待つと、電話機は 10 秒後に内線 1000 にコールをつなぎます。

（注）　ユーザが [ReDial] ソフトキーを押した場合は、ただちに処理が行われるため、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません。

ユーザが Unified CM に拒否されるパターンをダイヤルした場合、そのユーザはパターン全体を入力して Dial キーを押し、INVITE メッセージを Unified CM に送信した後でなければ、コールが拒否されたという通知（リオーダー トーン）は発信元に送信されません。たとえば、NPA 976 へのコールが拒否される場合は、919765551234 をダイヤルして Dial を押してから、リオーダー トーンが再生されます。

電話機に SIP ダイヤル規則が設定されている場合

SIP ダイヤル規則を使用すると、ユーザがダイヤルしたパターンを電話機が認識できます。認識作業が完了すると、SIP INVITE メッセージが Unified CM に自動的に送信され、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（詳細については、「SIP ダイヤル規則」（P.9-80）を参照してください）。

たとえば、企業の支店で同一支店内の電話機間のコールに 4 桁の内線番号をダイヤルする必要がある場合は、4 桁のパターンを認識するように電話機を設定すれば、ユーザが Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（図 9-25 を参照）。

図 9-25　ダイヤル規則が設定されているタイプ A の SIP 電話機でのユーザ入力とフィードバック

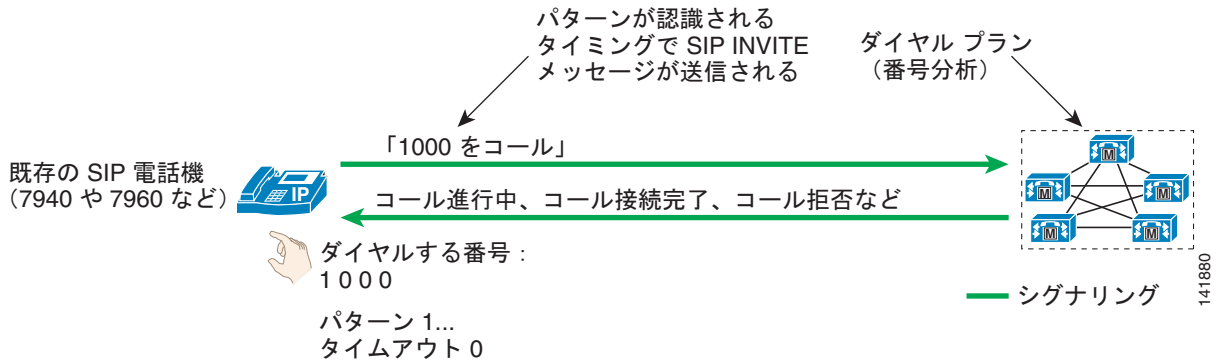


図 9-25 で、電話機は 1 で始まる 4 桁のパターンをすべて認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、SIP INVITE メッセージがすぐに Unified CM に送信され、ユーザが Dial キーを押す必要はありません。

SIP ダイヤル規則を使用するタイプ A 電話機では、電話機上に明示的に設定されていないパターンをダイヤルすることもできます。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは Dial キーを押すか、桁間タイムアウトを待ちます。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（最後の 4 のキーを押した後）にリオーダー トーンを受信します。

タイプ B の SIP 電話機でのユーザ入力

タイプ B 電話機はタイプ A 電話機と動作が少し異なり、タイプ B 電話機では Key Press Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（「タイプ A の SIP 電話機でのユーザ入力」（P.9-76）を参照）。

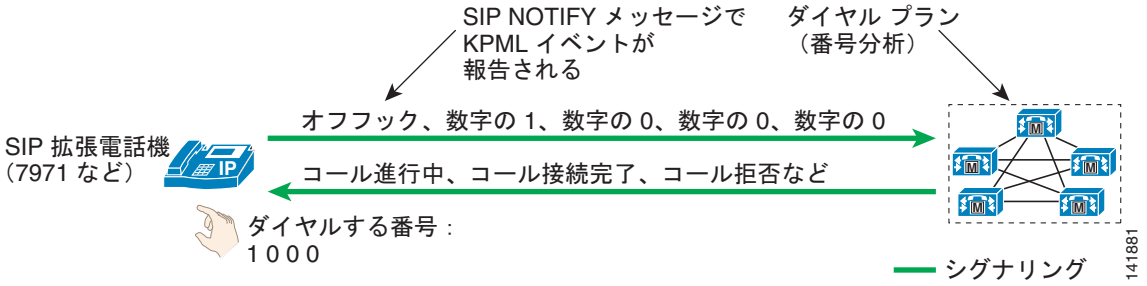
SIP を実行するタイプ B の IP Phone には、次の 2 つの異なる動作モードがあります。

- 「電話機に SIP ダイヤル規則が設定されていない場合」（P.9-78）
- 「電話機に SIP ダイヤル規則が設定されている場合」（P.9-79）

電話機に SIP ダイヤル規則が設定されていない場合

タイプ B の IP Phone は、Key Press Markup Language（KPML）に基づいて、ユーザによるキー操作を報告する機能を提供します。ユーザ入力イベントの 1 つ 1 つにより、Unified CM に対して KPML をベースとした独自のメッセージが生成されます。ユーザの個々の操作をすぐに Unified CM にリレーするという点では、この操作モードは SCCP を実行している電話機の操作モードと非常によく似ています（図 9-26 を参照）。

図 9-26　ダイヤル規則が設定されていないタイプ B の SIP 電話機でのユーザ入力とフィードバック



ユーザのすべてのキー操作によって、Unified CM に対する SIP NOTIFY メッセージがトリガーされることで、ユーザが押したキーに対応する KPML イベントが報告されます。このメッセージ機能により、Unified CM の番号分析はユーザが合成する部分パターンをその都度認識し、無効な番号がダイヤルされるとすぐにリオーダー トーンを再生するなど、適切なフィードバックを提供できます。

ダイヤル規則なしに SIP を実行しているタイプ A の IP Phone とは異なり、タイプ B の SIP 電話機には、ユーザ入力の終わりを示す Dial キーがありません。図 9-26 では、1000 をダイヤルするユーザは、最後の 0 をダイヤルした後、Dial キーを押さなくても、コール プログレス トーン（リングバック トーンかリオーダー トーン）を受け取ります。この動作は、SCCP プロトコルを実行する電話機のユーザ インターフェイスとの整合性が取れています。

電話機に SIP ダイヤル規則が設定されている場合

タイプ B の IP Phone では、ダイヤルされたパターンの認識が電話機によって行われるように SIP ダイヤル規則を設定できます（図 9-27 を参照）。

図 9-27　ダイヤル規則が設定されているタイプ B の SIP 電話機でのユーザ入力とフィードバック

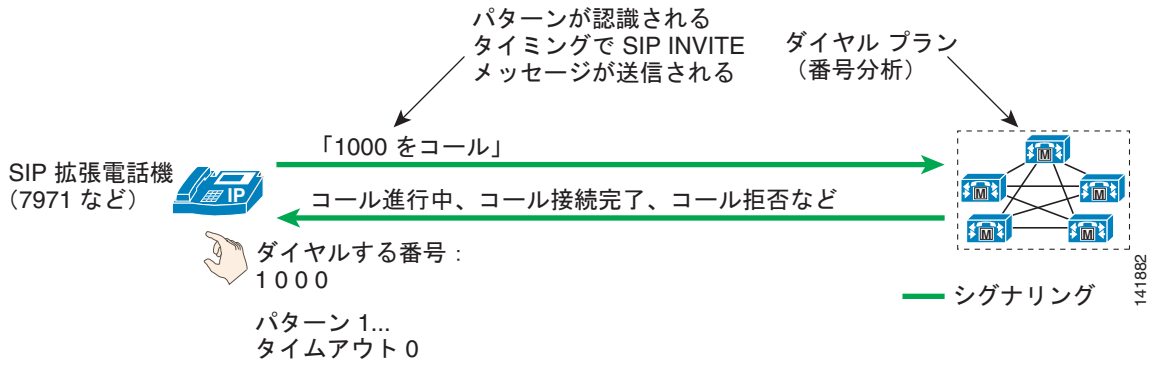


図 9-27 で、電話機は 1 で始まる 4 桁のパターンすべてを認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、Unified CM への SIP INVITE メッセージの送信がトリガーされます。

（注） SIP ダイヤル規則がタイプ B の IP Phone に実装されるとすぐに、KPML ベースのダイヤリングは無効になります。ユーザが SIP ダイヤル規則と一致しない番号ストリングをダイヤルした場合は、個々の桁のイベントが、いずれも Unified CM にリレーされません。その代わり、ダイヤリングが完了すると（桁間タイムアウトの発生後）、ダイヤルされたストリング全体が Unified CM にまとめて送信されます。

SIP ダイヤル規則を使用するタイプ B 電話機では、電話機上に明示的に設定されていないパターンをダイヤルする方法は 1 つだけです。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは桁間タイムアウトを待った後でなければ、Unified CM に SIP NOTIFY メッセージが送信されません。タイプ A の IP Phone とは異なり、タイプ B の IP Phone にはオンフック ダイヤルを使用した場合を除いて、ダイヤリングの終わりを示す Dial キーがありません。その場合、ユーザはいつでも「Dial」キーを押すことで、ダイヤルしたすべての桁の Unified CM への送信をトリガーできます。

（注） タイプ B 電話機を SRST ルータに登録した場合、設定した SIP ダイヤル規則は無効になります。

特定のパターンが電話機で認識され、それが Unified CM によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Unified CM ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（4 のキーを押した後）にリオーダー トーンを受信します。

SIP ダイヤル規則

Cisco Unified CM には、ユーザ入力が収集されたときに電話機でパターン認識を実行できるように、SIP ダイヤル規則機能が備わっています。たとえば、誰もが知る 911 というパターンを認識したら Unified CM にメッセージを送信し、すぐに緊急コールが開始されるように電話機を設定できます。それと同時に、ユーザが国際電話番号の可変長のパターンを入力できるようにも設定できます。

注意すべき重要な点は、SIP ダイヤル規則を使用して電話機にパターン認識を設定しても、Unified CM のサービス クラスとルート プランの設定の方が優先されることです。ある電話機が長距離通話のパターンを認識するように設定されていても、その電話機がローカル コールのみを許可するサービス クラスに割り当てられていると、Unified CM がそのコールをブロックします。

SIP ダイヤル規則には、それらの規則を設定する電話機のモデルに基づいて、次の 2 つのタイプがあります。

- 7905_7912（Cisco Unified IP Phone 7905 および 7912 に使用）
- 7940_7960_OTHER（上記以外のすべての IP Phone モデルに使用）

ダイヤル規則の一部として使用できる基本的なダイヤル パラメータは、次の 4 つです。

- パターン

  このパラメータは、パターンの実際の数値表現です。数字、ワイルドカード、2 次ダイヤル トーンを再生する命令を含めることができます。次の表は、2 つのタイプのダイヤル規則について、値とその効果を示しています。

	ダイヤル規則のタイプ	
パターン	**7905_7912**	**7940_7960_OTHER**
数字の 0 ～ 9	対応する数字。	対応する数字。
.	任意の数字（0 ～ 9）と一致します。	任意の文字（0 ～ 9、*、#）と一致します。
-	続けて追加の数字が入力される場合があることを示します。個々の規則の末尾に置く必要があります。	適用対象外
#	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は # キーが入力終了として認識されます。たとえば、9>#... と指定すると、9 が押された後は、いつでも # 文字が認識されます。	適用対象外
t*n*	*n* 秒のタイムアウト値を示します。たとえば、1...t3 は 1000 と一致し、3 秒後に Unified CM への Invite の送信をトリガーします。	適用対象外
r*n*	最後の文字を *n* 回繰り返します。たとえば、1.r3 は 1... に相当します。	適用対象外
S	パターンに修飾子 S が含まれていると、このパターン以後の他のダイヤル規則がすべて無視されます。実質的に、S によって規則照合が終了します。	適用対象外

	ダイヤル規則のタイプ	
パターン	7905_7912	7940_7960_OTHER
*	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は * キーが入力終了として認識されます。	1 文字以上と一致します。たとえば、パターン 1* は 10、112、123456 などと一致します。
,	適用対象外	電話機で 2 次ダイヤル トーンを再生します。たとえば、8,.... と指定すると、ユーザには 8 を押した後に 2 次ダイヤル トーンが聞こえます。

- IButton

  このパラメータは、ダイヤル パターンの適用対象となるボタンを指定します。ユーザが回線ボタン 1 でコールを開始しようとしている場合は、ボタン 1 用に指定されたダイヤル パターンのみが適用されます。このオプション パラメータを設定しなかった場合、ダイヤル パターンは電話機のすべての回線に適用されます。このパラメータは、Cisco SIP IP Phone 7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、および 7975 のみに適用されます。ボタン番号は、画面横にあるボタンの上から下の順に対応し、一番上のボタンが 1 になります。

- Timeout

  このパラメータは、システムがタイムアウトになり、ユーザが入力した番号にダイヤルするまでの時間を秒単位で指定します。ダイヤルされた番号がすぐにダイヤルされるようにするには、0 を指定します。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータを省略した場合は、電話機のデフォルトの桁間タイムアウト値（デフォルトは 10 秒）が使用されます。

- User

  このパラメータは、ダイヤルされた番号に自動的に追加されるタグを表します。有効な値は、**IP**（Unified CM 以外の SIP コール エージェントが配置される場合）と **Phone** です。このパラメータは、7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータはオプションであり、Unified CM が唯一のコール エージェントとなる配置では省略してください。

（注） Cisco Unified IP Phone 7905 および 7912 は、パターンを SIP ダイヤル規則内で作成された順に選択します。これに対し、その他の電話機モデルでは、最長一致のパターンが選択されます。次の表は、ユーザが 95551212 をダイヤルした場合に選択されるパターンを示しています。

SIP ダイヤル規則	7905_7912	7940_7960_OTHER
.……. 9……..	最初に一致するパターンの ..... が選択されます。	最長一致パターンの 9..... が選択されます。

Unified CM におけるコール ルーティング

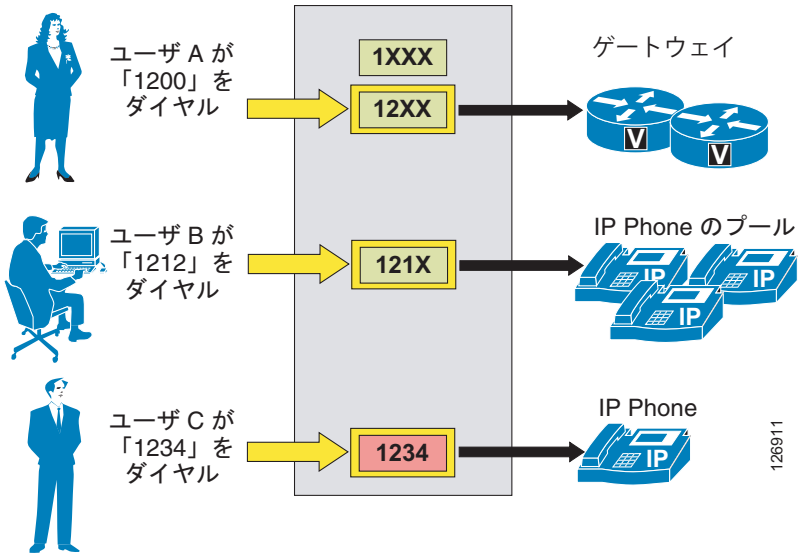
Unified CM 内に設定されるダイヤリング宛先は、すべて内部のコール ルーティング テーブルにパターンとして追加されます。このような宛先としては、IP Phone 回線、ボイスメール ポート、ルート パターン、トランスレーション パターン、および CTI ルート ポイントがあります。

番号がダイヤルされると、Unified CM では closest-match ロジックを使用し、コール ルーティング テーブルにあるすべてのパターンの中から一致パターンを選択します。一致する可能性のあるパターンが複数ある場合は、次の基準に基づいて宛先パターンを選択します。

- ダイヤルされたストリングに一致するもの。
- 一致する可能性のあるパターンのうち、ダイヤルされたストリング以外に一致するパターンが最も少ないもの。

たとえば、図 9-28 の場合を考えます。ここでは、コール ルーティング テーブルにパターン 1XXX、12XX、および 1234 が保持されています。

図 9-28　　Unified CM のコール ルーティング ロジックの例



ユーザ A がストリング 1200 をダイヤルすると、Unified CM は、この番号をコール ルーティング テーブル内のパターンと比較します。この場合は、一致する可能性のあるパターンが 2 つあります（1XXX と 12XX）。両方ともダイヤルされたストリングに一致していますが、1XXX は合計 1,000 個のストリングに一致する一方で（1000 ～ 1999）、12XX は 100 個のストリングに一致します（1200 ～ 1299）。したがって、12XX がこのコールの宛先として選択されます。

ユーザ B がストリング 1212 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 121X）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、121X に一致するストリングは 10 個しかありません。したがって、このパターンがコールの宛先として選択されます。

ユーザ C がストリング 1234 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、および 1234）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、1234 に一致するストリングは 1 個しかありません（ダイヤルされたストリング）。したがって、このパターンがコールの宛先として選択されます。

（注）　Cisco Unified CM でディレクトリ番号（DN）を設定すると、それぞれのデバイス（IP Phone など）が登録済みかどうかにかかわらず、その番号はコール ルーティング テーブルに配置されます。この仕様によって、アプリケーション（およびそのプライマリ パターン）が未登録である場合は、セカンダリの一致パターンを利用してフェールオーバー機能をアプリケーションに提供することができなくなりました。プライマリ パターンがコール ルーティング テーブルに必ず存在するため、セカンダリ パターンに一致するかどうかは検索されません。

パターンにおける + 記号のサポート

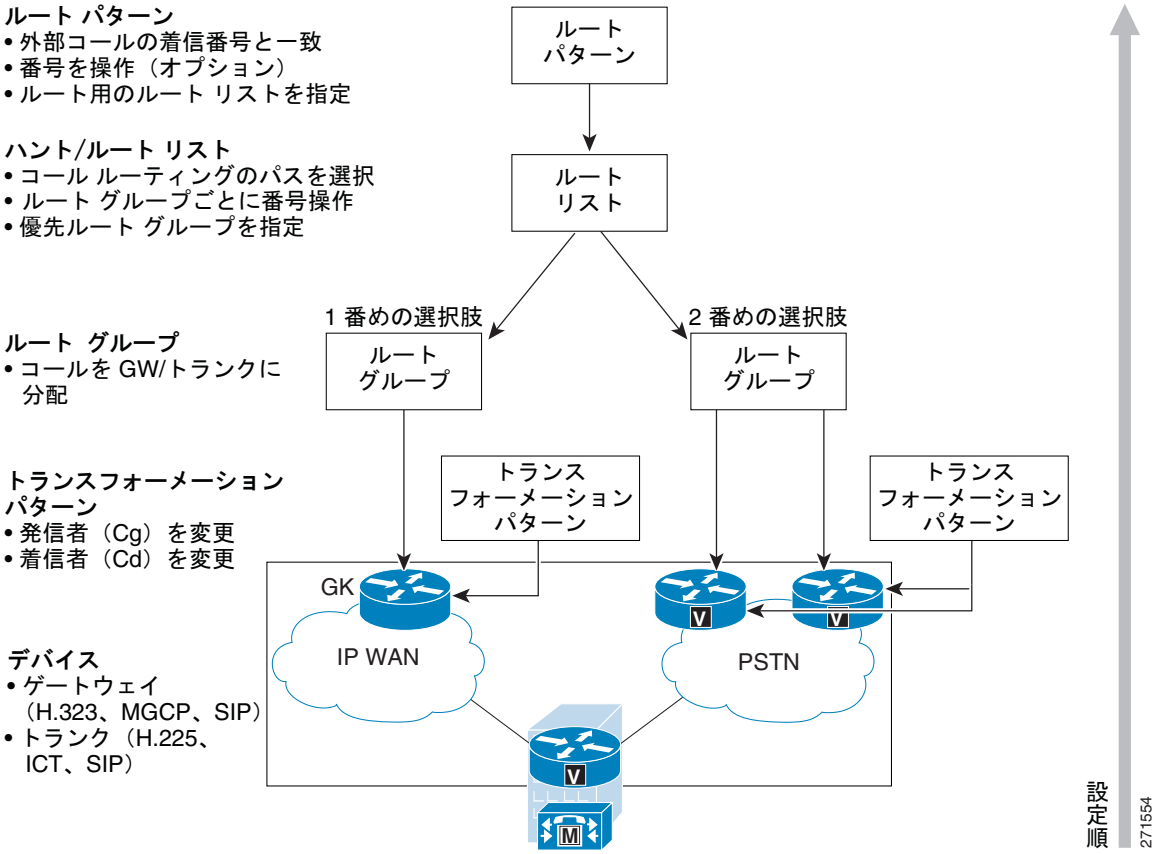
Unified CM 内のすべてのパターン（ルート パターン、トランスレーション パターン、ディレクトリ番号など）では、+ 記号を使用できます。+ を文字どおりの意味で使用するには、+ の前にエスケープ文字 \ を入力することで、先行文字の 1 つ以上のインスタンスを意味する正規表現演算子の + と区別します。次の例を参考にしてください。

- \+14085264000 は +14085264000 を意味します。
- 2+ は 2、22、222 などを意味します。

Unified CM の外部ルート

Unified CM は、同じクラスタ内の内部宛先にコールをルーティングする方法を自動的に「認識」します。公衆網ゲートウェイ、H.323 ゲートキーパー、またはその他の Unified CM クラスタなどの外部宛先の場合、外部ルート コンストラクト（次の項で説明）を使用して、明示的にルーティングを設定する必要があります。このコンストラクトは、3 層式のアーキテクチャに基づいています。このアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。Unified CM は、外部ダイヤル ストリングと一致する設定済みルート パターンを検索し、それを使用して、対応するルート リストを選択します。ルート リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、ルート グループと呼ばれ、従来の PBX でトランク グループと呼ばれていたものに非常によく似ています。図 9-29 では、Unified CM 外部ルート コンストラクトの 3 層式アーキテクチャを示しています。

図 9-29　外部ルート パターンのアーキテクチャ



次の各項では、Unified CM の外部ルート コンストラクトの個々の要素について説明します。

- 「ルート パターン」（P.9-84）
- 「ルート リスト」（P.9-88）
- 「ルート グループ」（P.9-88）
- 「ルート グループ デバイス」（P.9-91）

ルート パターン

ルート パターンは、コールを外部エンティティにルーティングするために Unified CM で設定された、数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ルート パターンでは、コールをルーティングするゲートウェイを直接指すことも、ルート リストを指すこともできます。ルート リストはルート グループを指しており、最終的にゲートウェイを指します。

ルート パターン、ルート リスト、およびルート グループ コンストラクトを完全パスで指定することを強く推奨します。その理由は、この構造を使用するとコール ルーティング、番号操作、および将来のダイヤル プランの拡張を最も柔軟に行うことができるからです。

@ ワイルドカード

- @ ワイルドカードは、特殊なマクロ関数であり、特定の国の番号計画全体を表す一連のパターンに拡張されます。たとえば、フィルタ処理されていない単一のルート パターン（たとえば、9.@）を北米番号計画を使用して設定すると、実際には、Unified CM の内部ダイヤル プラン データベースに 166 個の個別ルート パターンが追加されます。
- その他の国別番号計画を受け入れるように Unified CM を設定できます。この作業が完了すると、[Route Pattern] 設定ページの [Numbering Plan] フィールドで選択した値に応じて、同じ Unified CM クラスタ内で、複数の番号計画に対して @ ワイルドカードを使用できるようになります。詳細については、次の Web サイトで入手可能な『*Cisco Unified CallManager Dial Plan Deployment Guide*』を参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html
- @ ワイルドカードは、いくつかの中小規模の配置では十分に実務で使用できますが、大規模な配置では、管理とトラブルシューティングが困難になる可能性があります。これは、@ ワイルドカードを利用する場合、ルート フィルタを使用して、管理者が特定のパターンをブロックする必要があるためです（「ルート フィルタ」（P.9-85）を参照してください）。

ルート フィルタ

- ルート フィルタは、@ ワイルドカードによって作成されるルート パターン数を減らすために、@ ルート パターンと一緒にのみ使用します。@ ワイルドカードを含まないパターンに適用されるルート フィルタは、発生するダイヤル プランに影響を与えません。
- ルート フィルタと一緒に入力する論理式は、NOT-SELECTED フィールドを除いて、最大 1024 文字にできます。
- ルート フィルタ内の論理文節数が増えるにつれて、設定ページのリフレッシュ時間も増え、容認できないほど長くなる場合があります。
- 大規模な配置の場合、@ ワイルドカードとルート フィルタではなく、明示ルート パターンを使用してください。この方法を利用すると、管理とトラブルシューティングも容易になります。これは、Unified CM で設定されているすべてのパターンが、[Route Pattern] 設定ページから簡単に参照できるからです。

国際および可変長ルート パターン

- 国際間の宛先は、通常、任意の桁数を表す ! ワイルドカードを使用して設定されます。たとえば、北米では通常、国際コール用にルート パターン 9.011! が設定されています。欧州諸国のほとんどでは、0.00! ルート パターンを使用することで同じ結果が得られます。
- ! ワイルドカードは、ダイヤルされた番号の長さが変化する国では配置にも使用されます。このような場合、Unified CM は、ダイヤルがいつ完了するかわからないので、コールの送信前に 15 秒待機します。この遅延は、次の方法のいずれかで短縮できます。
  - ダイヤルの終わりを指定する T302 タイマー（サービス パラメータ TimerT302_msec）の値を減らします。ただし、ユーザがダイヤルを終了する前のコールの早期送信を防止するために、4 秒以上に設定します。
  - # ワイルドカードで終了する同じパターンのルートパターンを設定し（たとえば、北米の場合 9.011!#、欧州の場合 0.00!#）、ダイヤルの終わりを示すために # をダイヤルするようにユーザに指示します。この処理は、携帯電話で送信ボタンを押すことに相当します。

重複送信と重複受信

国内の番号計画を静的ルート パターンで定義することが難しい国では、Unified CM に重複送信および重複受信を設定できます。

重複送信とは、エンド ユーザがダイヤルする番号を Unified CM で収集しながら、番号がダイヤルされると同時に公衆網に渡すことを意味します。重複送信を可能にするには、[Route Pattern] 設定ページの [Allow Overlap Sending] チェックボックスをオンにします。以前の Unified CM リリースで重複送信を使用可能にするには、SendingCompleteIndicator サービス パラメータを False に設定します。ルート パターンには、公衆網アクセス コード（たとえば、北米では 9、欧州諸国の多くでは 0）を含めるだけです。

重複受信とは、ダイヤルされる番号を PRI 公衆網ゲートウェイから Unified CM で 1 つずつ受信し、ストリングのダイヤルが完了するまで待機し、その後でコールを内部宛先にルーティングすることを意味します。重複受信を可能にするには、OverlapReceivingFlagForPRI サービス パラメータを True に設定します。以前の Unified CM リリースでは、パラメータ名は OverlapReceivingForPriFlag です。

ルート パターンにおける番号操作

- コールで最終的に利用するルート グループに関係なく、ルート パターンで設定する番号操作は、発番号および着番号に影響を与えます。ルート リスト ビューにあるそのメンバーのルート グループに設定される番号操作が影響するのは、ルートに対してだけです。つまり、コールの発信に使用するルート グループに設定されている変換のみが実行されます。
- ルート リスト ビューにあるそのルート グループの番号操作は、ルート パターンに設定される番号操作よりも優先されます。
- ルート パターンやルート リストに設定される番号変換による発番号および着番号は、選択したルート グループに含まれるデバイスに設定されているトランスフォーメーション パターンで処理されます。
- ルート パターンで番号操作を設定する場合、コール詳細レコード（CDR）は、番号操作が行われた後のダイヤル番号を記録します。ルート グループのみで番号操作を設定する場合、CDR は、番号操作が行われる前の実際のダイヤル番号を記録します。
- 同様に、ルート パターンでの番号操作を設定すると、発信側の IP Phone ディスプレイには、操作後の番号が示されます。ルート グループのみで番号操作を設定する場合、この操作はエンド ユーザには見えなくなります。

発呼回線 ID

- 発呼回線 ID の表示は、ゲートウェイで使用可能または使用不可にできます。また、サイトの要件に基づいて、ルート パターンで操作することもできます。
- [Use Calling Party's External Phone Number Mask] オプションを選択する場合、外部コールは、コールを発信する IP Phone に指定された発呼回線 ID を使用します。このオプションを選択しない場合、[Calling Party Transform Mask] フィールドに指定されたマスクが、発信者番号識別の生成に使用されます。

緊急プライオリティ

- [Urgent Priority] チェックボックスは、一般に、パターンに一致したコールを T302 タイマーの満了を待たずにすぐルーティングする目的で使用されます。たとえば、北米でパターン 9.911 と 9.[2-9]XXXXXX が設定されている場合、ユーザが 9911 をダイヤルすると、Unified CM は T302 タイマーが終了するまで待機し、その後でコールをルーティングします。これは、9911 の後に数字が入力されると、9.[2-9]XXXXXX に一致する場合があるためです。9.911 ルート パターンについて緊急プライオリティを有効にすると、Unified CM はユーザが 9911 とダイヤルした直後にルーティング処理を実行し、T302 タイマーの満了までは待機しません。

- [Urgent Priority] チェックボックスをオンにした場合に実行されるのは、設定済みのパターンがダイヤルされた番号とのベストマッチになったとき、その直後に T302 タイマーを満了させることです。つまり、緊急パターンが他のパターンよりも高い優先順位を持っているわけではありません。「Unified CM におけるコール ルーティング」（P.9-82）の項で説明した closest-match ロジックは、依然として有効です。

  たとえば、ルート パターン 1XX が緊急パターンとして設定され、パターン 12! が通常のルート パターンとして設定されているとします。ユーザが 123 をダイヤルした場合、Unified CM は 3 番めの数字を受信した直後にルーティング処理を実行しません。これは、1XX は緊急パターンであっても、ベストマッチではないからです（12! が合計 10 個のパターンに一致するのに対して、1XX は 100 個のパターンに一致）。パターン 12! では、ユーザがさらに番号を入力できるため、Unified CM は桁間タイムアウトを待ってから、コールをルーティングする必要があります。

  別の例として、パターン 12[2-5] に緊急のマークが付けられ、12! が通常のパターンとして設定されているとします。ユーザが 123 とダイヤルすると、パターン 12[2-5] はベストマッチになります（12[2-5] が合計 4 個のパターンに一致するのに対し、12! は 10 個のパターンに一致）。緊急プライオリティ パターンがベストマッチなので、T302 タイマーは打ち切られ、それ以上のユーザ入力は想定されません。Unified CM は、パターン 12[2-5] を使用してコールをルーティングします。

コール分類

- このルート パターンを使用しているコールは、オンネットまたはオフネットのコールとして分類できます。このルート パターンを使用すると、オフネット間でのコール転送を禁止したり、オンネット通話者がいないカンファレンス ブリッジを終了したりすることによって、料金詐欺を防止できます（これらの機能は、どちらも Unified CM Administration の Service Parameters を使用して制御します）。
- [Allow device override] チェックボックスをオンにすると、コールは、関連するゲートウェイまたはトランク上で、コール分類設定に基づいて分類されるようになります。

強制アカウント コード（FAC）

- [Forced Account Codes] チェックボックスを使用すると、個々のルート パターンを使用して発信コールが制限されます。ルート パターンに対して FAC を有効にすると、ユーザは、目的のコール受信者に到達するための承認コードを入力するように要求されます。
- ユーザのダイヤルした番号が、FAC が有効になったルート パターンを通じてルーティングされるものである場合、システムは承認コードの入力を求めるトーンを再生します。コールを確立するには、ユーザ承認コードが、ダイヤルされた番号のルーティングに必要となる承認レベルを満たしているか、そのレベルを超えている必要があります。
- コール詳細レコード（CDR）に表示されるのは、承認名のみです。承認コードは CDR には表示されません。
- FAC 機能は、[Allow overlap sending] チェックボックスがオンの場合は使用できません。

クライアント識別コード（CMC）

- [Client Matter Code] チェックボックスを使用すると、個々のルート パターンを使用して特定番号へのコールがトラッキングされます。たとえば、企業で使用すると、特定のクライアントへのコールをトラッキングできます。
- ルート パターンに対して CMC を有効にすると、ユーザは目的の宛先に到達するためのコードを入力するように要求されます。
- ユーザのダイヤルした番号が、CMC が有効になったルート パターンを通じてルーティングされるものである場合、システムはコードの入力を求めるトーンを再生します。コールを確立するには、ユーザが正しいコードを入力する必要があります。

- クライアント識別コードは、コール詳細レコードに表示されます。これは、クライアントの課金およびアカウンティングに関するレポートを生成するための、CDR の分析およびレポート ツールで使用できるようにするためです。
- CMC 機能は、[Allow overlap sending] チェックボックスがオンの場合は使用できません。
- CMC と FAC を両方とも有効にすると、ユーザは番号をダイヤルするとき、FAC の入力を求められたら入力し、次のプロンプトで CMC を入力します。

ルート リスト

ルート リストは、発信コールに使用できるパス（ルート グループ）が優先順位順に並べられたリストです。ルート リストの標準的な用途は、リモートの宛先に 2 つのパスを指定することです。この場合、第一選択のパスは、IP WAN を介したパスであり、第二選択のパスは、公衆網ゲートウェイを介したパスです。

ルート リストには次の特性があります。

- 複数のルート パターンが同一ルート リストを指すことができます。
- ルート リストは、所定の宛先への代替パスの役目をするルート グループが、優先順位順に並べられたリストです。たとえば、ルート リストを使用して最低料金選択機能をサポートできます。この場合、リスト内のプライマリ ルート グループが、コールあたりのコストがより低くなるようにします。プライマリ ルート グループが「all trunks busy（全トランク使用中）」状態、または IP WAN リソースの不足により使用できない場合だけ、セカンダリ ルート グループが使用されます。
- ルート リスト内の各ルート グループは、独自の番号操作を行うことができます。たとえば、ルート パターンが 9.@ であるときに、ユーザが 9 1 408 555 4000 をダイヤルした場合、IP WAN ルート グループは 9 1 を削除し、公衆網ルート グループは 9 だけを削除することが可能です。
- 複数のルート リストに、同じルート グループを含むことができます。ルート グループの番号操作は、そのルート グループを指定する特定のルート リストに関連しています。
- ルート パターンまたはルート グループ内で複数の番号操作を実行すると、変換が実行される順序が、コールに使用される、変換結果の発番号および着番号に影響を与える可能性があります。Unified CM は、次に示す主要なタイプの番号操作を表示されている順に実行します。
  1. 番号を破棄する
  2. 発着信側変換
  3. 番号をプレフィックスとして付加する
  4. 発着信側トランスフォーメーション パターン

ルート グループ

ルート グループは、一般にゲートキーパーまたはリモート Unified CM クラスタとのゲートウェイ（MGCP、SIP、または H.323）、H.323 トランク、または Cisco Unified Border Element である特定のデバイスを制御し、それを指定します。Unified CM は、割り当てられている分配アルゴリズムに従ってコールをデバイスに送信します。Unified CM では、トップダウン アルゴリズムと循環アルゴリズムをサポートしています。

発信側および着信側トランスフォーメーション パターン

発信側トランスフォーメーション パターンを使用すると、発番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

着信側トランスフォーメーション パターンを使用すると、着番号のグローバル形式を、ゲートウェイ、トランクなどのルート グループ デバイスに接続されているオフクラスタ ネットワークで必要となるローカル形式に適応させることができます。

（注）　着信側トランスフォーメーション パターンは、電話機に影響を与えません。また、デバイス プールの着信側トランスフォーメーション パターン CSS も、そのパターンが割り当てられている電話機に影響を与えません。

両方のトランスフォーメーション パターン タイプは、一致する発番号または着番号の数値表現で構成されます。使用される構文は、ルート パターン、トランスフォーメーション パターン、ディレクトリ番号などのその他パターンの構文と同じです（図 9-30 を参照）。

変換演算子には、数字破棄命令（ドット前の番号など）、発信側トランスフォーメーション マスク、プレフィックス番号が含まれます。この演算子によって、発信側電話番号表示（Default、Allowed、または Restricted）が制御されます。発信側トランスフォーメーション パターンを設定することで、発信側の外部電話番号マスクを発番号として使用できます。

パーティションおよびコーリング サーチ スペースによって、どの発信側トランスフォーメーション パターンをどのゲートウェイまたはトランクに適用するかどうかが制御されます。ゲートウェイまたはトランクでは、関連するデバイス プールの発信側変換 CSS またはデバイス固有の発信側変換 CSS を優先順位の低い順に使用できます。同じメカニズムを使用して、着信側トランスフォーメーション パターンの適用を制御します。

[Call Routing Information] > [Outbound Calls] の [Gateway Configuration] ページで設定された発信側および着信側トランスフォーメーション パターンは、ゲートウェイに送信される発番号または着番号と、発信側または着信側の番号タイプおよび番号計画に影響します。[Incoming Calling Party Settings] で適用される発信側トランスフォーメーション パターンは、ゲートウェイから送信されるコールに適用されます。

図 9-30　発信側および着信側トランスフォーメーション パターン

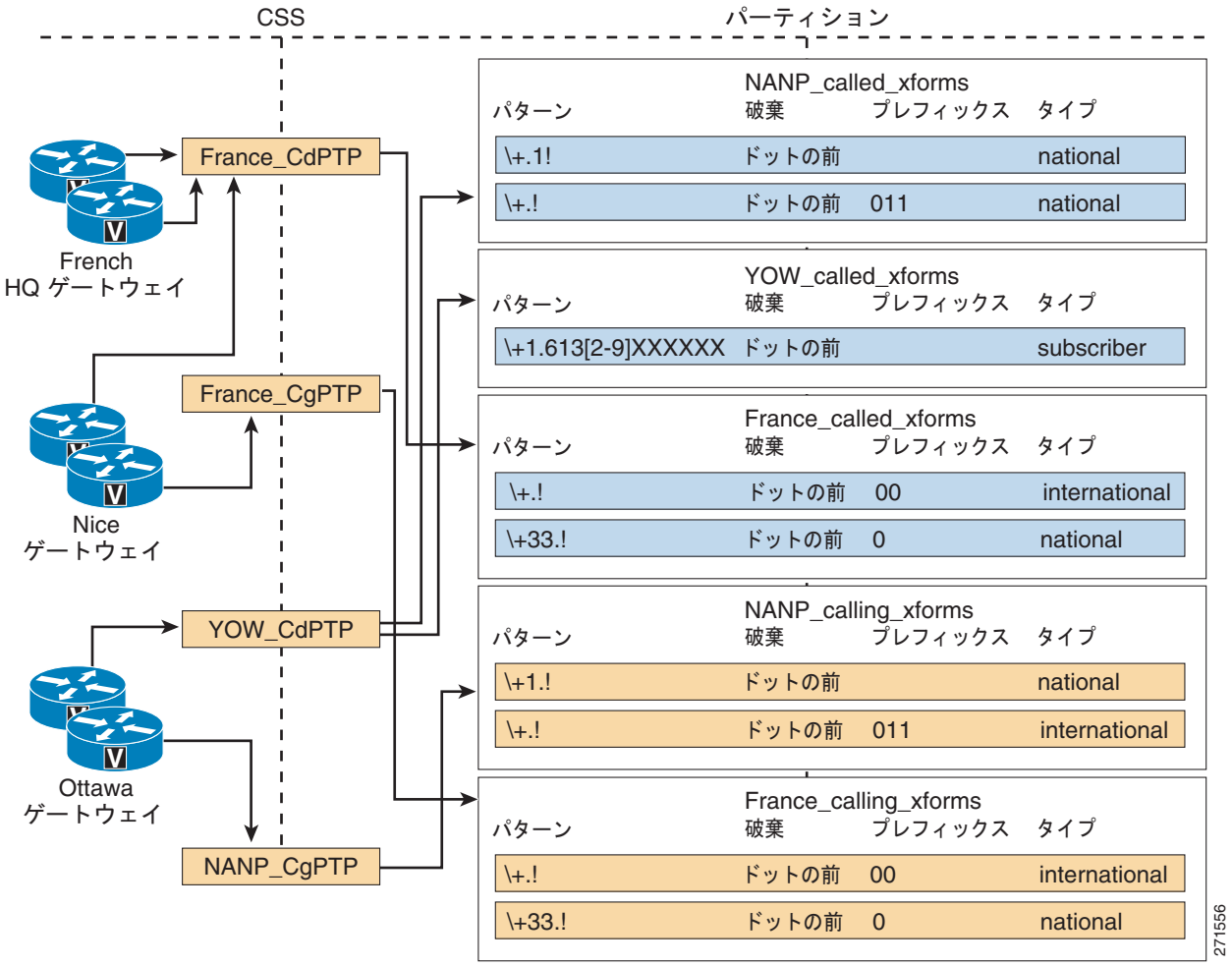


図 9-30 は、発信側および着信側トランスフォーメーション パターンを、さまざまな公衆網で公衆網に接続しているゲートウェイの異なるグループに適用する方法を示しています。

北米番号計画（NANP）では、カナダの Ottawa（空港コード YOW）にあるゲートウェイは、パーティション NANP_calling_xforms が含まれている、発信側変換 CSS NANP_CgPTP に割り当てられます。発番号が +1 で始まる（つまり、NANP 内から発信される）コールは、パーティション NANP_calling_xforms 内で設定されている両方のパターンに一致します。best-match ロジックの後、最初のパターンが選択され、発番号から + 記号と NANP 国コード 1 が削除されます。残りの発番号部分は公衆網に送信される発番号として使用され、番号タイプは National に設定されます。

たとえば、+1 613 555 1234 からのコールを YOW ゲートウェイに送信した場合、その発番号は 613 555 1234 に変換され、番号タイプは National に設定されます。

同じ発信側からのコールをフランスにあるゲートウェイに送信した場合には、一連の異なる発信側トランスフォーメーション パターンが適用されます。たとえば、+1 613 555 1234 からのコールをフランスの Nice（空港コード NCE）にあるゲートウェイに送信した場合、パーティション France_calling_xforms に含まれている発信側トランスフォーメーション パターンが適用されます。この場合、発番号は 001 613 555 1234 に変換され、番号タイプは International に設定されます。

（注）　コールをゲートウェイに送信すると、発番号変換が無効になることがあります。多くのサービス プロバイダーでは、現地のサービス契約や規制で定められているように、特定の範囲外で発番号を使用することを許可していません。

同じプロセスは、着番号トランスフォーメーション パターンにも適用されます。Ottawa ゲートウェイの場合、割り当てられた受信側変換 CSS は YOW_CdPTP です。これは、パーティション NANP_Called_xforms および YOW_Called_xforms に含まれています。番号計画エリア 613 内の宛先番号に発信されるコールは、これらの 2 つのパーティションに含まれているすべてのパターンに一致します。ただし、ベストマッチ プロセスによってパターン \+1.613[2-9]XXXXXX が選択されます。

たとえば、Ottawa ゲートウェイ経由で +1 613 555 9999 にコールを発信すると、着番号は 516 555 9999 に変換され、番号タイプは Subscriber に設定されます。

着信側の設定（ゲートウェイ別）

個々のゲートウェイには、優先順位に従ってデバイス プール レベルまたはサービス パラメータ レベルで着信側の設定を行うことができます。各番号タイプ（Subscriber、National、International、または Unknown）には、Unified CM で適切なプレフィックス番号を設定できます。さらに、番号を削除したり、着番号として指定した番号にプレフィックス番号を付けたりできます。表記形式は PP:SS です。PP はプレフィックスとして付加される番号を表し、SS は削除される桁数を表します。最初に番号削除操作が着信側の番号で実行され、次にその結果の番号にプレフィックス番号が付加されます。たとえば、プレフィックス番号フィールドを +33:1 と設定し、着信側の番号が 01 58 40 58 58 である場合、+33 1 58 40 58 58 となります。

Cisco Unified CM 7.1 では、発信側トランスフォーメーション パターンをコールに適用するために使用するコーリング サーチ スペースを各番号タイプに設定できます。コーリング サーチ スペースには、発信側トランスフォーメーション パターンだけが存在するパーティションが保持される必要があります。これによって、厳密に番号タイプに基づくのではなく、発番号の構造に基づいた変更を発番号に適用できます。発信側トランスフォーメーション パターンでは、正規表現を使用して発番号が照合されます。複数の一致項目から選択するには、best-match プロセスが使用され、選択されたパターンの発信側変換がコールに適用されます。

ルート グループ デバイス

ルート グループ デバイスは、ルート グループによってアクセスされるエンドポイントであり、一般に、ゲートキーパーまたはリモート Unified CM とのゲートウェイまたはトランクで構成されます。次のタイプのデバイスは、Unified CM で設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイ
- SIP ゲートウェイ
- H.323 ゲートウェイ
- H.225 トランク、ゲートキーパー制御：ゲートキーパーを介した標準 H.323 ゲートウェイとのトランク
- クラスタ間トランク、非ゲートキーパー制御：別の Unified CM クラスタとの直接トランク
- クラスタ間トランク、ゲートキーパー制御：ゲートキーパーを介した他の Unified CM クラスタまたは H.323 ゲートウェイとのトランク
- SIP トランク：別の Unified CM クラスタとのトランク、Cisco Unified Border Element、Session Border Controller、または SIP プロキシ

（注）　H.225 トランクとクラスタ間トランク（ゲートキーパー制御）はどちらも、相手方エンドポイントが標準 H.323 ゲートウェイであるか、Unified CM であるかを自動的に検出し、それに応じて H.225 または Intercluster Trunk プロトコルを選択します。

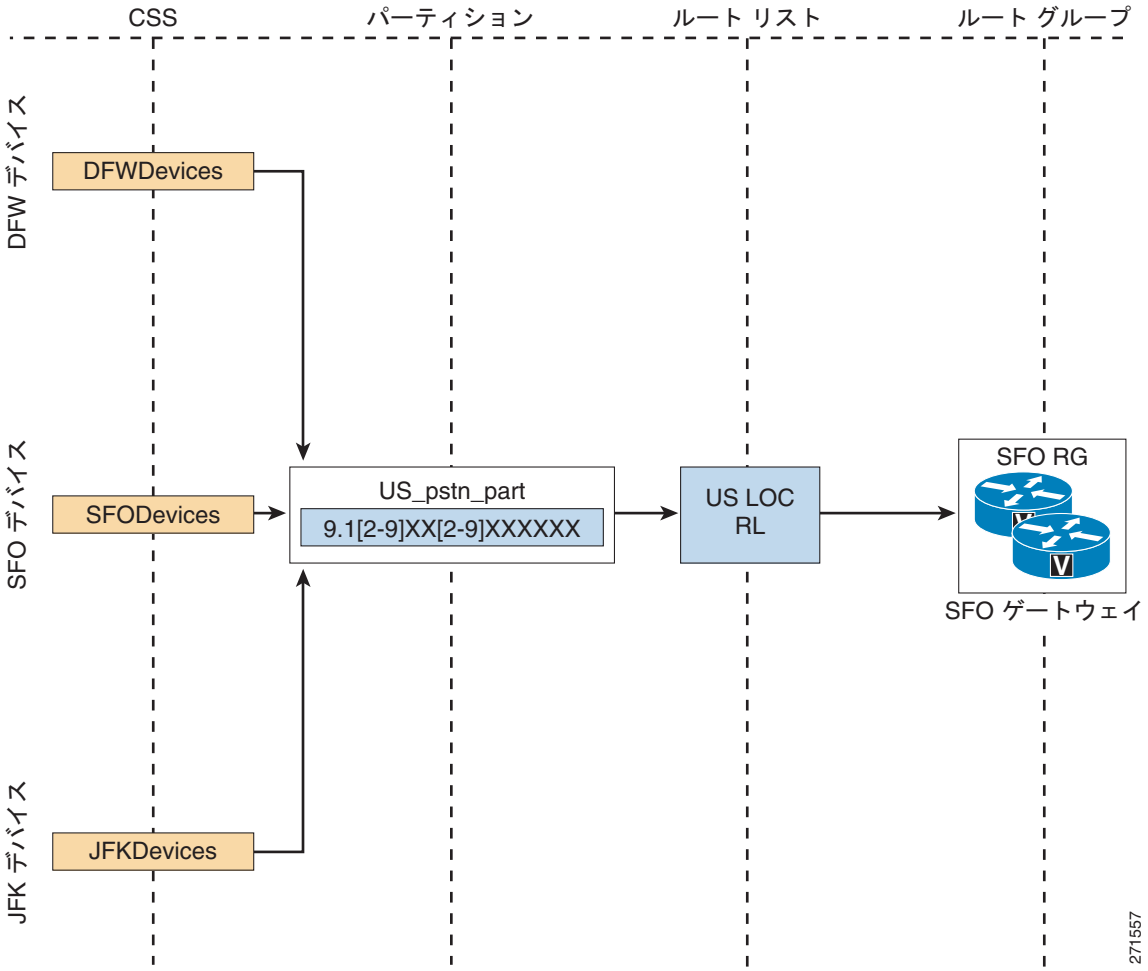
ローカル ルート グループ

デバイス プールは、ローカル ルート グループに関連付けることができます。ローカル ルート グループを使用したルート パターンには、固有の特性があります。つまり、コールの発信元デバイスに基づいて出口ゲートウェイを動的に選択できます。それに対し、静的ルート グループを使用したルート パターンによってルーティングされるコールでは、コールの発信元デバイスに関係なく、コールが同じゲートウェイにルーティングされます。

例 9-2　　ローカル ルート グループと非ローカル ルート グループの比較

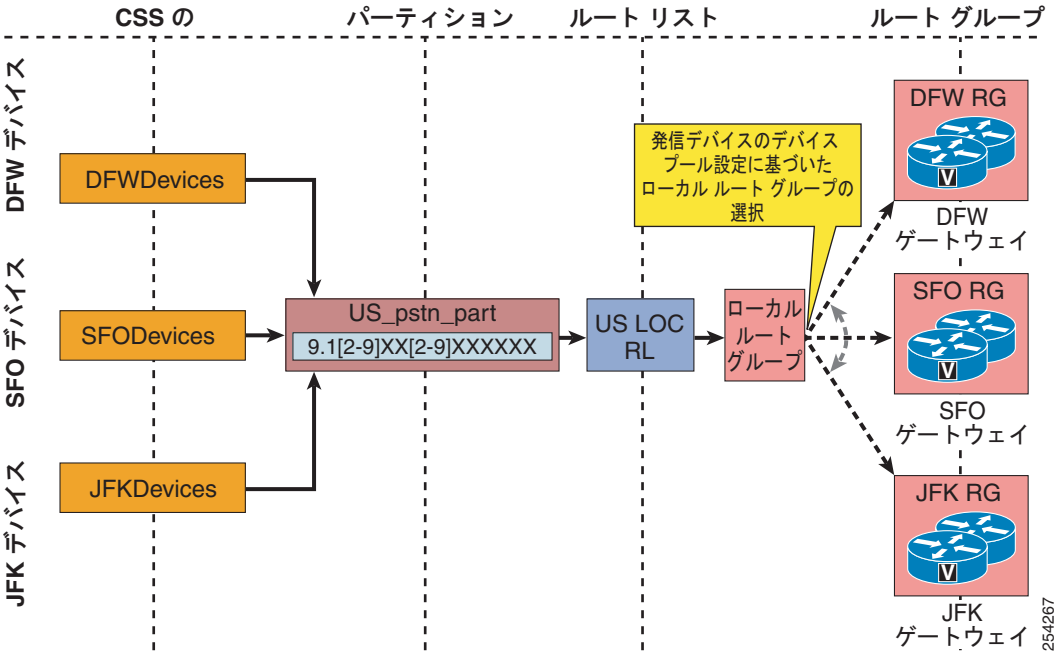
図 9-31 では、9.1[2-9]XX[2-9]XXXXXX と定義されたルート パターンは、San Francisco ゲートウェイを含む非ローカル ルート グループを参照するルート リストを指しています。このルート パターンが Dallas、San Francisco、および New York の電話機のコーリング サーチ スペースに含まれているパーティションにある場合、それらの 3 つの都市にあるデバイスからの国内コールの出口は San Francisco の公衆網となります。

図 9-31　非ローカル ルート グループの動作



一方、図 9-32 に示すように、同じルート パターンを変更して、標準ローカル ルート グループを含むルート リストを指すようにした場合、Dallas サイトから発信されるコールの出口は Dallas ゲートウェイを経由した公衆網となり、New York サイトから発信されるコールの出口は New York ゲートウェイを経由した公衆網となり、San Francisco サイトから発信されるコールの出口は San Francisco ゲートウェイを経由した公衆網となります。

図 9-32　ローカル ルート グループの動作



デバイス モビリティ機能を使用すると、ローミングしている現在のサブネットに基づいて、デバイス プールをエンドポイントに割り当てることができます。これにより、電話機の現在のサイトに基づいた、ローカル ルート グループの割り当てが可能になります。

例 9-3　デバイス モビリティ

電話機を San Francisco サイトから New York サイトに移動するとします。電話機の新しい IP アドレス（New York サイトに関連付けられた IP サブネット部分）に基づいて、New York のデバイス プールがその電話機に割り当てられます。ローミング電話機によって発信される次のコールは、標準ローカル ルート グループを含むルート リストを使用したルートと一致し、New York ゲートウェイを経由してルーティングされます。

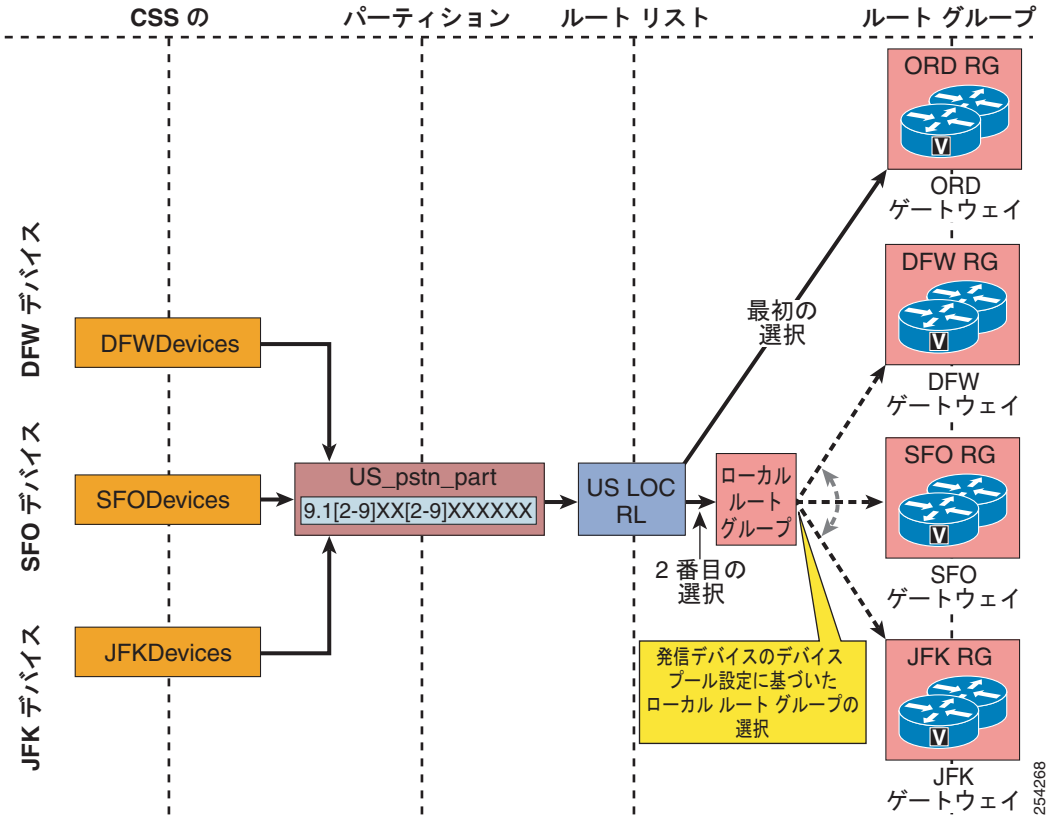
公衆網へのローカル フェールオーバーを使用した中央ゲートウェイ

中央ゲートウェイが設定されているシステムの場合、ローカル ルート グループによって、公衆網へのローカル フェールオーバーが簡素化されます。発信側サイトでゲートウェイへのローカル フェールオーバーが許可されているときに、単一のルート リストを使用することで、複数サイトの公衆網コールをルーティングできます。

例 9-4　中央ゲートウェイとローカル フェールオーバー

ある会社が、Chicago にあるトランクのグループに有利な公衆網相互接続レートをネゴシエートするとします。ルート リストに、1 番めの項目として Chicago にあるゲートウェイを含むルート グループが含まれ、2 番めの項目として標準ローカル ルート グループが含まれている場合、処理されるコールは最初に Chicago にある低コストの推奨ゲートウェイに送信されます。Chicago ゲートウェイが使用可能でない、フリー ポートがない、あるいは発信側電話機と Chicago ゲートウェイ間で使用できる帯域幅が十分でない場合は、発信側電話機のデバイス プール設定でローカル ルート グループによって決定されている、2 番めの項目を使用して、発信側電話機と同じ場所にあるゲートウェイを経由したコールのルーティングが試行されます（図 9-33 を参照）。

図 9-33　公衆網へのローカル フェールオーバーを使用した中央ゲートウェイ



Unified CM におけるコール特権

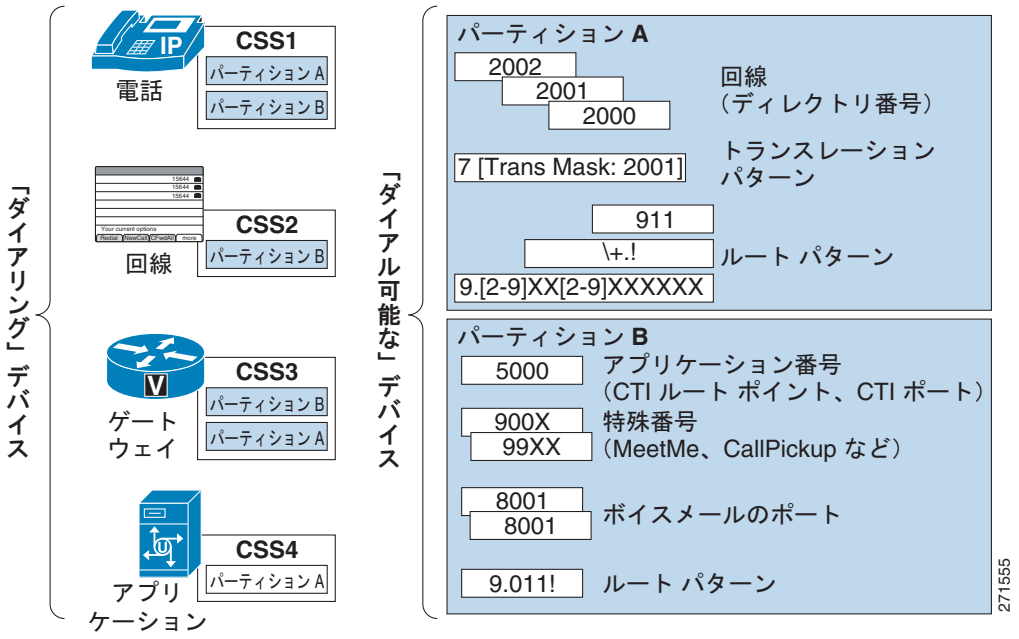
ダイヤリング特権は、特定のエンドポイント（電話、ゲートウェイ、または CTI アプリケーションなど）にどのタイプのコールを許可する（または禁止する）かを制御するために設定されます。Unified CM で処理されるすべてのコールは、次の要素の設定で実装されたダイヤリング特権の対象になります。

- 「パーティション」（P.9-96）
- 「コーリング サーチ スペース」（P.9-97）

*パーティション*は、同じアクセス可能性を持つディレクトリ番号（DN）のグループです。*コーリング サーチ スペース*は、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。デバイスは、コーリング サーチ スペースに含まれているパーティション内の DN だけを呼び出すことができます。

図 9-34 に示すように、パーティション内に配置できるすべての項目は、ダイヤリングの対象となるパターンを持っています。このような項目としては、電話回線、ルート パターン、トランスレーション パターン、CTI ルート グループ回線、CTI ポート回線、ボイスメール ポート、および Meet-Me 会議番号があります。逆に、コーリング サーチ スペースを持つ項目は、コールをダイヤルできるすべてのデバイスです。たとえば、電話機、電話回線、ゲートウェイ、アプリケーション（CTI ルート グループまたはボイスメール ポート経由）などです。

図 9-34　パーティションとコーリング サーチ スペース

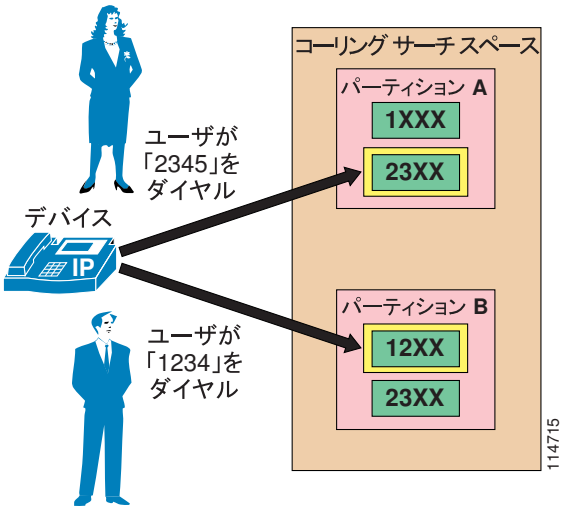


パーティション

パーティションに含めることができるダイヤル プラン項目には、IP Phone のディレクトリ番号、トランスレーション パターン、ルート パターン、CTI ルート ポイント、およびボイスメール ポートがあります。「Unified CM におけるコール ルーティング」（P.9-82）で説明するように、複数のダイヤル プラン項目（ディレクトリ番号、ルート パターンなど）が重複する場合、Unified CM は、ダイヤルされた番号と一致するか、または最も近い（最も固有性の高い一致）項目を選択します。2 つのダイヤル プラン項目が、ダイヤルされたパターンに等しく一致した場合、Unified CM は、コールを発信するデバイスのコーリング サーチ スペース内で最初に表示されているダイヤル プラン項目を選択します。

たとえば、図 9-35 について考えます。ルート パターン 1XXX と 23XX はパーティション A の一部であり、ルート パターン 12XX と 23XX はパーティション B の一部です。発信側デバイスのコーリング サーチ スペースには、パーティション A:パーティション B の順にパーティションがリストされています。このデバイスのユーザが 2345 をダイヤルすると、Unified CM では、パーティション A のルート パターン 23XX を一致項目として選択します。これは、このパターンが発信側デバイスのコーリング サーチ スペースで最初に示されているためです。ただし、ユーザが 1234 をダイヤルした場合には、Unified CM ではパーティション B のルート パターン 12XX を一致項目として選択します。これは、パーティション A の 1XXX よりも一致率が大きいためです。コーリング サーチ スペースに含まれているパーティションの順序は、closest-match ロジックに基づいて均等一致項目が複数あった場合に、競合を解消する要素としてのみ使用されます。

図 9-35　マッチング ロジックにおけるパーティション順序の影響



（注）　均等一致項目が同じパーティションに複数ある場合、Unified CM は、ローカルのダイヤル プラン データベース内で最初にリストされている項目を選択します。ダイヤル プラン データベース内でダイヤル プラン項目がリストされる順序は、設定することができません。したがって、同じパーティション内で均等一致項目が共存しないようにすることを強く推奨します。これはこのような場合に発生するダイヤル プラン ロジックが予測できないからです。

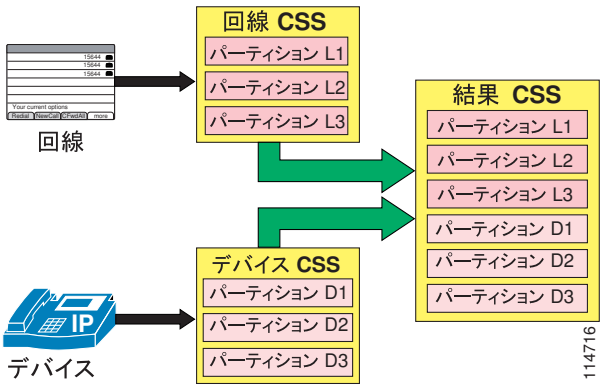
日時に基づいてパーティションをアクティブまたは非アクティブにできます。パーティションをアクティブまたは非アクティブにするには、まず、Unified CM Administration で期間とスケジュールを設定し、次に個々のタイム スケジュールを各パーティションに割り当てます。スケジュールに指定した日時の範囲外では、このパーティションは非アクティブになります。このパーティションに含まれているパターンは、Unified CM コール ルーティング エンジンによってすべて無視されます。この機能の詳細については、「時間帯ルーティング」（P.9-121）を参照してください。

コーリング サーチ スペース

コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。所定のコーリング サーチ スペースが割り当てられるデバイスは、そのコーリング サーチ スペースにリストされているパーティションだけにアクセスできます。そのコーリング サーチ スペース以外のパーティションの DN へのダイヤルは失敗します。発信者にはビジー信号が聞こえます。

IP Phone 回線とデバイス（電話機）自体の両方でコーリング サーチ スペースを設定する場合、Unified CM は、この 2 つのコーリング サーチ スペースを図 9-36 に示すように連結し、デバイスのコーリング サーチ スペースの前に、回線のコーリング サーチ スペースを置きます。

図 9-36　IP Phone の回線とデバイスのコーリング サーチ スペース（CCS）の連結



（注）　デバイス モビリティを使用しない場合、デバイスのコーリング サーチ スペースは静的となり、デバイスをネットワークの別の場所に移動しても同じままです。デバイス モビリティを有効にした場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、デバイスのコーリング サーチ スペースを動的に決定できます。詳細については、「デバイス モビリティ」（P.9-108）を参照してください。

同じルート パターンが、2 つのパーティション（回線のコーリング サーチ スペースに含まれているパーティションとデバイスのコーリング サーチ スペースに含まれているパーティション）に指定されている場合、Unified CM は、「パーティション」（P.9-96）の項で説明している規則に従って、パーティションの連結リスト内で最初にリストされているルート パターン（この場合、回線のコーリング サーチ スペースに関連したルート パターン）を選択します。

回線とデバイスのコーリング サーチ スペースを設定する方法に関する推奨事項については、「従来のアプローチによる Unified CM のサービス クラスの構築」（P.9-55）と 「回線 / デバイス アプローチによる Unified CM のサービス クラスの構築」（P.9-59）の項を参照してください。

結合されたコーリング サーチ スペース（デバイスと回線）の最大長は、各パーティション名間の区切り文字を含めて、1024 文字です（たとえば、ストリング「partition_1:partition_2:partition_3」は 35 文字です）。したがって、コーリング サーチ スペース内の最大パーティション数は、パーティション名の長さに応じて変動します。また、コーリング サーチ スペースの文節は、デバイスのコーリング サーチ スペースと回線のコーリング サーチ スペースを結合するので、個々のコーリング サーチ スペースの最大文字の上限は、512 文字（結合されたコーリング サーチ スペース文節の上限 1024 文字の半分）です。

したがって、パーティションとコーリング サーチ スペースを作成するときは、コーリング サーチ スペースに含める予定のパーティション数を基準にして、パーティション名を短くしてください。コーリング サーチ スペースの設定の詳細は、次の Web サイトで入手可能なオンラインの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com

パーティションまたはコーリング サーチ スペースを設定する前に、すべての DN は、<None> という名前が付いた特別なパーティションに置かれ、すべてのデバイスには、<None> という名前が付いたコーリング サーチ スペースが割り当てられます。カスタム パーティションとコーリング サーチ スペースを作成する場合は、作成するどのコーリング サーチ スペースにも、<None> パーティションが含まれています。一方、<None> コーリング サーチ スペースには、<None> パーティション*だけ*が入っています。

（注）　<None> パーティションに残っているどのダイヤル プラン項目も、コールを発信する*任意*のデバイスから暗黙的に到達可能です。したがって、予期しない結果を避けるために、<None> パーティションにダイヤル プラン項目を残さないように強く推奨します。

（注）　<None> と定義されたままのコーリング サーチ スペースを残さないでください。そのままにしておくと、ダイヤル プランの動作が予測困難になる可能性があります。

トランスフォーメーション パターンの特別な考慮事項

発信側および着信側トランスフォーメーション パターンは、パーティションにも配置されます。それらのパーティションは、コーリング サーチ スペース（CSS）に含まれますが、コール特権を制御するためのものではありません。トランスフォーメーション パターンのパーティションの役割は、どの変換をどのゲートウェイ、トランク、または電話機に適用するかを選択することです。発信側トランスフォーメーション パターン CSS に含まれるパーティションには、発信側トランスフォーメーション パターンのみが含まれていなければなりません。同様に、着信側トランスフォーメーション パターン CSS に含まれるパーティションには、着信側トランスフォーメーション パターンのみが含まれていなければなりません。

自動転送コーリング サーチ スペース

（注）　この機能が電話機によってアクティブになっている場合、Call Forward All 動作は、宛先番号が個々のユーザによって入力されるその他の自動転送動作とは異なります。

自動転送コーリング サーチ スペースを有効にする方法を決定できます。Calling Search Space Activation Policy（コーリング サーチ スペースのアクティベーション ポリシー）によって指定されている、選択可能なオプションは次の 3 つです。

- Use System Default

  Calling Search Space Activation Policy を Use System Default に設定した場合、クラスタ全体のサービス パラメータである CFA CSS Activation Policy によって、使用される Forward All コーリング サーチ スペースが決定されます。CFA CSS Activation Policy サービス パラメータを With Configured CSS または With Activating Device/Line CSS に設定できます（下記を参照してください）。デフォルトでは、CFA CSS Activation Policy サービス パラメータは With Configured CSS に設定されています。

- With Configured CSS

  With Configured CSS オプションを選択した場合、Directory Number Configuration ウィンドウで明示的に設定されている Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースによって、不在転送のアクティブ化と自動転送が制御されます。Forward All コーリング サーチ スペースを None に設定した場合、Forward All に対して CSS は設定されません。そのため、パーティションおよびディレクトリ番号に対する不在転送のアクティブ化の試行は失敗します。不在転送のアクティブ化中に、Forward All コーリング サーチ スペースおよび Forward All のセカンダリ コーリング サーチ スペースの変更は発生しません。

- With Activating Device/Line CSS

  Forward All コーリング サーチ スペースを明示的に設定せずに、ディレクトリ番号のコーリング サーチ スペースとデバイスのコーリング サーチ スペースの組み合せを使用する場合には、Calling Search Space Activation Policy に対して With Activating Device/Line CSS を選択します。Forward All が電話機によってアクティブになっている場合にこのオプションを選択すると、Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースに、ディレクトリ番号のコーリング サーチ スペースとアクティブ化デバイスのデバイス コーリング サーチ スペースが自動的に入力されます。Unified CM Administration から宛先への Forward All を設定した場合、Forward All コーリング サーチ スペースとセカンダリ コーリング サーチ スペースは自動的にはデータが格納されず、明示的に設定しなければなりません。その 2 つのコーリング サーチ スペースが連結され、連結されたコーリング サーチ スペースを使用することで、Call Forward All 宛先として入力されている番号を検証します。詳細については、「回線/デバイス アプローチによる Unified CM のサービス クラスの構築」（P.9-59）を参照してください。

  不在転送が電話機によってアクティブになっているときに、Forward All コーリング サーチ スペースを None に設定した場合にこの設定（Calling Search Space Activation Policy を With Activating Device/Line に設定）を使用すると、ディレクトリ番号のコーリング サーチ スペースとアクティブになっているデバイス コーリング サーチ スペースを使用することで、不在転送の試行を検証します。

（注）　通常、Call Forward All 設定では、2 つの要件を満たす必要があります。その 2 つの要件とは、デバイスでコールの転送が許可されている宛先を制御することと、さまざまな発信地点から発信するコールが Call Forward All 宛先に転送されるときに最適なコール ルーティングを実現することです。両方の要件を満たすためには、回線/デバイス ダイヤル プラン アプローチによる宛先の制御を可能にする With Configured CSS アクティベーション ポリシーを使用することを推奨します。Call Forward All CSS を使用して、ブロック パターンによる制限セットを実装します。通常のサービス クラスを Call Forward All に使用する場合、Call Forward All CSS は、回線で設定されているのと同じコーリング サーチ スペースに設定できます。その後、標準ローカル ルート グループにコールをルーティングするように、Secondary Calling Search Space for Call Forward All を設定する必要があります。デバイスのデバイス プールで設定されている、発信側（転送）デバイスのローカル ルート グループに基づいて、コールのルーティングに使用される実際のルート グループがコール時に決定されます。

SIP を実行しているタイプ A の IP Phone では、Call Forward All がその電話機自体から起動された場合、転送されるコールにデバイスの Rerouting Calling Search Space が使用されます。Forward All 動作が [Unified CM User] ページまたは [Unified CM Administrative] ページから起動される場合、その電話機から開始される Forward All 動作とは無関係になります。

たとえば、SIP を実行するタイプ A の IP Phone に、[Unified CM] ページで内線 3000 への Forward All が指定されているとします。同時に、その電話機自体には、内線 2000 への Forward All が設定されています。この場合、その電話機に対するすべてのコールは、内線 3000 に転送されます。

（注）　SIP を実行するタイプ A の IP Phone では、[Unified CM User] ページまたは [Administrative] ページからの Forward All の起動は、電話機に反映されません。電話機には、コールの転送に関する確認は何も表示されません。

SCCP を実行する IP Phone または SIP を実行するタイプ B の IP Phone から Forward All が起動された場合、ユーザ入力は入力と同時に、設定済みの Forward All コーリング サーチ スペースの中で許可されるパターンと比較されます。無効な宛先パターンが設定されていると、ユーザにはリオーダー トーンが聞こえます。SIP を実行するタイプ A の IP Phone から Forward All が起動された場合、Forward All ユーザ入力は電話機上にローカルに保管され、Unified CM 内のコーリング サーチ スペースとは照合されません。ユーザ入力が無効な宛先に対応している場合でも、ユーザへの通知はありません。その電話機へのコールに対しては、電話機が無効な宛先番号に対して SIP 再ルーティング動作を開始しようとしたときに、リオーダー トーンが再生されます。

その他の自動転送タイプ

さまざまな自動転送タイプ（Forward Busy、Forward No Answer、Forward No Coverage、Forward on CTI Failure、Forward Unregistered）に対して設定されているコーリング サーチ スペースは、他のどのコーリング サーチ スペースとも連結されないスタンドアロン値です。

Call Forward 設定（Forward All を除く）は、内部または外部のコール タイプ別に設定できます。たとえば、電話機で外部発信者のボイスメールに Call Forward No Answer を設定しても、発信者がネットワーク上の別の IP Phone から発信している社員である場合には、ボイスメールを携帯電話番号に転送できます。これを可能にするには、内線と外線の Call Forward 設定に対して、異なる設定を使用します。

Forward All コーリング サーチ スペースが <None> のままになっている場合、処理の結果は Unified CM のリリースによって異なり、予想することは困難です。このため、自動転送コーリング サーチ スペースを設定する場合は、次のベスト プラクティスに従うことを推奨します。

- 自動転送コーリング サーチ スペースは、常に <None> 以外の値を使用して設定する。この設定により混乱を避けることができ、トラブルシューティングが容易になります。転送されるコールにどのコーリング サーチ スペースが使用されるかについて、ネットワーク管理者が正確に把握できるためです。
- Call Forward Busy コーリング サーチ スペースと Call Forward No Answer コーリング サーチ スペースは、ボイスメール パイロットおよびボイスメール ポートの DN に到達可能で、かつ外部公衆網番号以外の値を使用して設定する。
- Call Forward All コーリング サーチ スペースと Forward All のセカンダリ コーリング サーチ スペースは、どちらも企業のポリシーに従って設定する。多くの企業では、コールを社内の番号にしか転送できないように制限しています。この方法によって、ユーザが IP Phone の回線を長距離電話の番号に転送したり、私用電話の長距離通話料金がかからないようにするためにローカル IP Phone の番号に公衆網からダイヤルしたりすることを防止します。

Call Forward Unregistered（CFUR）機能は、一時的に登録から外されている宛先の電話機に発信されたコールを再ルーティングする手段です。CFUR の設定は、主に次の 2 つの要素で構成されます。

- 宛先の選択

  DN が登録から外されているときに、コールを次のいずれかの宛先に再ルーティングできます。

  - ボイスメール

    ボイスメールのチェックボックスをオンにし、CFUR コーリング サーチ スペースを設定して、ボイスメールのパイロット番号を含めることで、コールをボイスメールに送信できます。

  - 公衆網を経由した電話機への到達に使用するディレクトリ番号

    このアプローチが適切となるのは、WAN リンクがダウンするサイト内に電話機がある場合です。そのサイトに Survivable Remote Site Telephony（SRST）が装備されている場合は、電話機（および同じ場所にある 公衆網ゲートウェイ）が同じ場所にある SRST ルータに再登録されます。その後、電話機は、その公衆網 DID 番号に発信されたコールの受信を行うことができます。

    この場合、適切な CFUR 宛先は、対応する元の宛先 DN の PSTN DID 番号です。宛先フィールドにこの PSTN DID を設定します。+ 記号を含む E.164 形式で設定することを推奨します（たとえば、+1 415 555 1234）。これによって、同じオフネット アクセス コードと公衆網プレフィックスを登録から外された電話機として使用するかどうかに関係なく、発信側電話機のローカル ルート グループによる CFUR 宛先の処理が可能になります。

- コーリング サーチ スペース

  Unified CM では、着信側 DN の CFUR コーリング サーチ スペースを使用することで、設定済みの宛先番号へのコールのルーティングを試行します。CFUR コーリング サーチ スペースは、対象の電話機に設定され、登録から外されている電話機に発信するすべてのデバイスで使用されます。つまり、すべての発信側デバイスでは、ルート パターン、ルート リスト、ルート グループの同じ組み合せを使用して、コールを発信します。標準ローカル ルート グループを参照するルート リストを指すパターンを使用して、コール を CFUR 宛先にルーティングするために、CFUR コーリング サーチ スペースを設定することを推奨します。これによって、発信側デバイスに基づいて公衆網への出口ゲートウェイが選択されるようになります。

電話機が単にネットワークから切断されている場合と同様に、電話機が登録から外されている一方で、電話機の DID 番号に関連付けられているゲートウェイが依然として Unified CM の制御下にある場合に、Call Forward Unregistered 機能を使用すると、テレフォニー ルーティング ループが発生することがあります。このような場合、電話機への初期化コールによって、電話機の DID への最初のコールが公衆網経由で試行されます。次に、同じ電話機の DN に到達するために、その結果の着信公衆網コールによって、別の CFUR 試行がトリガーされ、さらに、公衆網を経由して公衆網の中央ゲートウェイから別の CFUR コールがトリガーされます。システム リソースが使い果たされるまで、このサイクルが繰り返されます。

MaximumForwardUnRegisteredHopsToDn サービス パラメータによって、DN に対して同時に許可される CFUR コールの最大数が制御されます。デフォルト値 0 は、カウンタが無効であることを意味します。公衆網経由で CFUR を再ルーティングするように DN を設定した場合には、ループを防止する必要があります。このサービス パラメータを値 1 に設定すると、CFUR のメカニズムで 1 つのコールを発信するとすぐに、CFUR 試行が停止されます。CFUR が設定されている場合には、この設定によって、1 つのコールだけをボイスメールに転送することも可能です。このサービス パラメータを値 2 に設定すると、最大 2 人の同時発信者が、ボイスメールに対して CFUR 設定が設定されている DN のボイスメールに到達でき、CFUR 設定によって公衆網を経由してコールが送信される DN に対して、発生する可能性があるループを 2 つに制限できます。

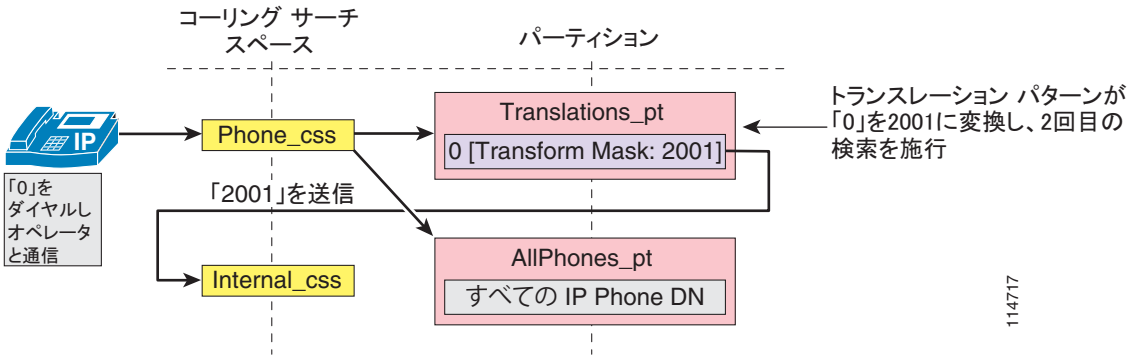
（注） Call Forward Unregistered コールを DN に関連付けられている PSTN DID に送信するために、エクステンション モビリティの DN を設定しないでください。ログアウト状態になっている、エクステンション モビリティ プロファイルの DN は登録から外されていると見なされます。そのため、ログアウト状態の DN の公衆網 DID 番号へのコールによって、ルーティング ループがトリガーされます。ログアウト状態になっている、エクステンション モビリティの DN へのコールがボイスメールに確実に送信されるように、対応する Call Forward Unregistered パラメータを設定してコールがボイスメールに送信されることを確認します。

トランスレーション パターン

トランスレーション パターンは、Unified CM で最も強力な番号操作ツールであり、あらゆるタイプのコールに対して使用できます。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。しかし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Unified CM は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンは、図 9-37 の例に示すように、さまざまな用途に使用できます。

図 9-37　トランスレーション パターンの応用例



この例では、管理者は、0 をダイヤルすると到達できるオペレータ サービスをユーザに提供し、一方で定型の内部番号計画をそのまま維持することを考えています。IP Phone は、Translations_pt パーティションを（他のパーティションとともに）含んでいる Phone_css コーリング サーチ スペースを使用して設定されています。このパーティションには、トランスレーション パターン 0 が定義されています。設定済みの Called Party Transform Mask によって、ダイヤルされたストリング（0）を新しいストリング 2001 で置き換えるように Unified CM に指示しています。2001 は、オペレータの電話機の DN に対応しています。2 回めの（この場合は 2001 の）ルックアップが、Internal_css コーリング サーチ スペースを使用して、コール ルーティング エンジンを通じて強制的に実行されます。この時点で、AllPhones_pt パーティションに含まれている実際のオペレータ DN（2001）までコールを伸ばすことができます。

（注）　ダイヤルされた番号をトランスレーション パターンを使用して操作すると、その変換後の番号が、コール詳細レコード（CDR）に記録されます。ただし、番号操作がルート リスト内で発生した場合、CDR には変換後の番号ではなく、ダイヤルされた元の番号が表示されます。IP Phone の Placed Calls ディレクトリには、常にユーザがダイヤルしたストリングがそのまま表示されます。

Automated Alternate Routing

Automated Alternate Routing（AAR）機能を使用すると、Unified CM で音声メディア用の代替パスを確立できます。このパスが確立されるのは、同じクラスタ内の 2 つのエンドポイント間にある優先パスで、コール アドミッション制御用のロケーション メカニズムによって決定される使用可能な帯域幅が使い果たされたときです。

AAR 機能の主な適用対象は、WAN 経由で接続されているサイトを使用する配置です。たとえば、支店 A の電話から支店 B の電話にコールする場合、支店間の WAN リンクで使用可能な帯域幅（ロケーション メカニズムによって計算）が不足しているときは、AAR によって公衆網経由でコールを再ルーティングできます。コールの音声パスは、発信元の電話からローカルの（支店 A の）公衆網ゲートウェイまでは IP ベース、このゲートウェイから公衆網を経由して支店 B のゲートウェイまでは TDM ベース、支店 B のゲートウェイから宛先の IP Phone までは IP ベースです。

AAR による処理は、ユーザには見えません。ユーザが着信側電話のオンネット（たとえば 4 桁の）ディレクトリ番号にしかダイヤルできないように AAR を設定すると、公衆網などの代替ネットワーク経由で宛先に到達するときに、ユーザによる追加入力が不要になります。

（注）　AAR では、CTI ルート ポイントがコールの発信元や宛先になることはサポートしていません。また、ユーザが複数のサイトにわたってローミングする場合、AAR はエクステンション モビリティ機能と共存できません。詳細については、「エクステンション モビリティ」（P.9-110）を参照してください。

AAR を正常に動作させるには、AAR の次の主要要素を指定する必要があります。

- 「宛先公衆網番号の確立」（P.9-104）
- 「必要なアクセス コードの付加」（P.9-105）
- 「適切なダイヤル プランおよびルートの選択」（P.9-106）

宛先公衆網番号の確立

コールを再ルーティングするには、公衆網などの代替ネットワーク経由でルーティングできる宛先番号を使用する必要があります。AAR では、ダイヤルされた番号を使用してコールのオンクラスタでの宛先を特定し、その番号を着信側の AAR 宛先マスクと結合します。AAR 宛先マスクが設定されていない場合には、その代わりに外部電話番号マスクが使用されます。ダイヤルされた番号と適切なマスクを結合することで、代替ネットワークによってルーティング可能な、完全修飾番号を生成する必要があります。

または、AAR 設定でボイスメールのチェックボックスをオンにすることで、コールをボイスメールのパイロット番号に転送できます。この選択では、発信者によってダイヤルされた元の番号を利用しませんが、ボイスメール プロファイル設定に従ってコールがルーティングされます。

（注）　デフォルトでは、ディレクトリ番号設定によってコールの AAR レッグがコール履歴に保持されます。これによって、音声メッセージング システムへの転送で適切なボイスメールボックスが選択されます。「Remove this destination from the call forwarding history」を選択した場合には、コールの AAR レッグがコール履歴に保持されません。そのため、ボイスメールボックスが自動的に選択されなくなり、発信者に汎用ボイスメール グリーティングが提供されます。

AAR 宛先マスクを使用することで、外部電話番号マスクと無関係に、宛先の電話番号を決定できます。たとえば、会社の発信者 ID ポリシーに基づいて、電話機の外部電話番号マスクをオフィスの代表電話番号（415 555 1000 など）にする必要がある場合、AAR に電話機固有の公衆網番号を提供するために、AAR 宛先マスクを +1 415 555 1234 に設定できます。

たとえば、San Francisco にある電話機 A（DN = 2345）から、New York にある電話機 B 上に設定されているオンネット DN（1234）にダイヤルするとします。ロケーションベースのコール アドミッション制御によってコールが拒否された場合、AAR は New York の電話機の外部電話番号マスク（+1212555XXXX）を取得して使用し、公衆網上でルーティング可能な番号（+12125551234）を導出します。

AAR 宛先マスクを設定して + 記号を含む完全修飾 E.164 番号を生成することが最善の方法となります。その理由は、この方法によって AAR 設定全体が大幅に簡素化されるためです。たとえば、Paris にある電話機は AAR 宛先マスク +33 1 58 04 58 58 で設定されます。この番号は完全修飾 E.164 番号であるため、発信側電話機がフランスやカナダにあるか、世界のどこにあるかに関係なく、発信側電話機の公衆網へのゲートウェイによって要求されるルーティング可能な PSTN 番号を導出するために、Cisco Unified Communications システムに必要なすべての情報がこの番号に含まれています。次の項では、このアプローチについて詳しく説明します。

必要なアクセス コードの付加

AAR 宛先で + 記号を含む完全修飾 E.164 番号を生成する場合

これが最も単純なケースです。AAR 宛先には、ワイルドカードとして + が含まれています。+ は、各ゲートウェイで必要となる適切なアクセス コードに置き換えられます。適切なルート パターンにルーティングされるように宛先番号が準備されます。その後、適切な着信側トランスフォーメーション パターンによって宛先番号が公衆網への出口点で変換されます。

例 1 : カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + が適切な国際アクセス コード 011 に置き換えられます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 2 : フランスの Nice にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は +33 1 58 04 58 58 です。発信側電話機の AAR コーリング サーチ スペースには、コールを標準ローカル ルート グループにルーティングするルート パターン \+! が含まれています。コールは、Nice にあるローカル ゲートウェイにルーティングされ、そこで、着信側トランスフォーメーション パターンによって + 33 が適切な国内アクセス コード 0 に置き換えられます。その結果、01 58 04 58 58 にコールが発信されます。

AAR 宛先マスクで国コードを含む番号を生成する場合

宛先番号（国コードが含まれると前提）が元の支店のダイヤル プランによって正常にルーティングされるためには、プレフィックスが必要になる場合があります。また、発信地点が別のエリア コードまたは別の国に配置されている場合、ダイヤルされたストリングの一部として、国際ダイヤル アクセス コード（たとえば、00、011）などの他のプレフィックスが必要になる場合があります。

AAR を設定する場合は、DN を AAR グループ内に配置します。AAR グループのペアごとに、同じ AAR グループ内で発信または終端するコールのプレフィックス番号も含めて、その 2 グループ間のコールで DN に追加するプレフィックス番号を設定できます。

一般的な規則として、複数の DN が各国間で同じダイヤリング構造を共有している場合は、それらの DN を同じ AAR グループに配置します。たとえば、UK 国外にある UK ダイヤル番号のすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。フランスおよびベルギーにあるすべての電話機は、0 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 00 が続きます。NANP にあるすべての電話機は、9 を PSTN アクセス コードとして使用し、その後に国際アクセス コードの 011 が続きます。

これによって、AAR グループ設定は次のようになります。

AAR グループ	NANP	Cent_EU	UK
NANP	9	9011	9011
Cent_EU	000	000	000
UK	900	900	9

例 3 : カナダの Ottawa にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機の AAR グループは NANP であり、宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 9011 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Ottawa のルート リストにルーティングして 9 を削除する、サイト固有のルート パターン 9011! が含まれています。コールは、Ottawa にあるローカル ゲートウェイにルーティングされます。その結果、011 33 1 58 04 58 58 にコールが発信されます。

例 4 : ベルギーの Brussels にある電話機が Paris にある電話機に発信していますが、WAN の帯域幅が不足しているために AAR がトリガーされます。AAR 宛先は 33 1 58 04 58 58 です。発信側電話機および宛先番号の AAR グループは Cent-EU です。したがって、プレフィックス 000 が付加されます。発信側電話機の AAR コーリング サーチ スペースには、コールを Brussels のルート リストにルーティングして先行する 0 を削除する、サイト固有のルート パターン 000! が含まれています。コールは、Brussels にあるローカル ゲートウェイにルーティングされます。その結果、00 33 1 58 04 58 58 にコールが発信されます。

ボイスメールの考慮事項

AAR は、コールをボイスメールに転送できます。通常、オフネット アクセス コードなしでボイスメールのパイロット番号がダイヤルされます（ボイスメールのパイロット番号が 8 555 1000 などの完全修飾のオンネット番号である場合）。コールをボイスメールに送信するために AAR を設定すると、AAR グループ メカニズムによって、設定済みのアクセス コードも付加されます。この設定には、AAR グループを作成する必要があります。AAR グループは、必要な AAR 宛先がボイスメール（たとえば、vmail_aar_grp）となっているすべての DN によって使用されます。他の AAR グループの DN からコールを受信するときに、このボイスメールの AAR グループでプレフィックス番号を使用しないことを確認してください。

例 : San Francisco サイトおよび New York サイトにある DN が、AAR グループ NANP で設定され、そのグループにある任意の 2 つの DN 間のコールに 9 が付加されるとします。San Francisco にある DN を設定して AAR コールをボイスメールに送信した場合（たとえば、8 555 1000）、985551000 にコールが発信されますが、そのコールは失敗します。その代わりに、San Francisco にある DN を AAR グループ vmail で設定します。次の表に示すように、AAR グループ NANP から AAR グループ vmail へのコールのプレフィックス番号は <none> です。これで、コールが正常に 85551000 に発信されます。

AAR グループ	NANP	Cent_EU	UK	vmail
NANP	9	9011	9011	<none>
Cent_EU	000	000	000	<none>
UK	900	900	9	<none>

（注） デバイス モビリティを使用しない場合、DN ドメインの AAR グループ設定は、デバイスがネットワークの別の場所に移動しても同じままです。デバイス モビリティを使用した場合、電話機の IP アドレスによって決定された、ネットワークで電話機が物理的に配置されている場所に基づき、ARR グループを動的に決定できます。詳細については、「デバイス モビリティ」（P.9-108）を参照してください。

適切なダイヤル プランおよびルートの選択

AAR コールは、発信元の電話と同じロケーションにあるゲートウェイを通じて出力する必要があります。これによって、完成されたダイヤル ストリングが、発信元サイトのダイヤル プランを通じて送信されます。このように設定するには、Unified CM Administration のデバイス設定ページで、適切な AAR コーリング サーチ スペースを選択します。AAR コーリング サーチ スペース内で、オフネット ダイヤル プラン項目（たとえば、ルート パターン）を、同じ場所にあるゲートウェイを指し、公衆網にコールを転送する前にアクセス コードを削除するように設定します。

たとえば、San Francisco サイトの電話を設定する場合は、91-NPA-NXX-XXXX としてダイヤルされた長距離電話を許可し、アクセス コード（9）を削除して San Francisco のゲートウェイに送信する AAR コーリング サーチ スペースを使用します。

ローカル ルート グループを使用し、さらに完全修飾 E.164 アドレス（+ 記号を含む）を AAR 宛先マスクとして使用すると、AAR コーリング サーチ スペース設定を大幅に簡素化することできます。単一のパーティションで設定され、単一のルート パターン \+! が含まれ、さらに標準ローカル ルート グループを備えた単一のルート リストを指している単一のコーリング サーチ スペースを使用することで、クラスタ全体のすべてのサイトですべてのコールをルーティングできます。これは、適切なゲートウェイ固有の着信側トランスフォーメーション パターンを利用して、宛先番号のユニバーサル形式を、各サイトでコールが送信されるサービス プロバイダー ネットワークで必要となるローカル形式に適応させます。

（注）　オンネット社内コールを強制的に公衆網コールとしてダイヤルする追加のルート パターンを設定した場合は、それらのパターンが AAR 機能のものと一致しないことを確認します。詳細については、「マルチサイト配置用の設計ガイドライン」（P.9-35）を参照してください。

（注）　コール アドミッション制御による再ルーティングされたコールの拒否を避けるため、AAR 機能は、各エンドポイントとそれに関連する公衆網へのゲートウェイとの間で、IP パスとして LAN を使用する必要があります。したがって、AAR ダイヤル プランでは、公衆網へのアクセスに集中型ゲートウェイを使用することはできません。

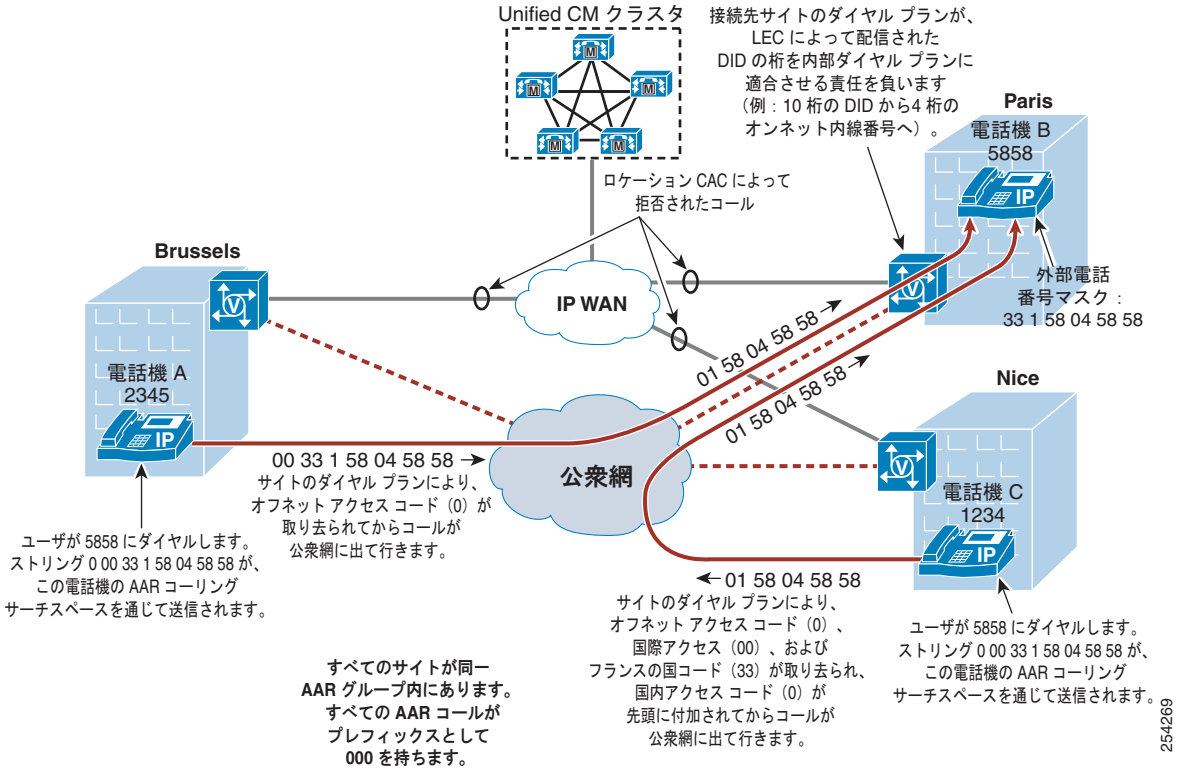
（注）　デバイス モビリティを設定した場合、電話機の IP アドレスによって決定されている、ネットワークで電話機が物理的に配置されている場所に基づいて、ARR コーリング サーチ スペースを動的に決定できます。詳細については、「デバイス モビリティ」（P.9-108）を参照してください。

同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項

場合によっては、同じ AAR グループに属する電話機のサイト間でダイヤリングを使用できるように AAR ダイヤル ストリングをローカルに修正する必要があります。たとえば、フランスにある 2 つのサイトが、同じ国コード 33 を共有しているとします（図 9-38 を参照）。この場合は、0 00 33 1 58 04 58 58 としてダイヤルされた番号を 01 58 04 58 58 に変換する必要があります。この変換が必要となるのは、AAR 設定で着信側トランスフォーメーション パターンを利用しない場合だけです。

この変換を実行する最良の方法は、サイト固有のトランスレーション パターン 00033.[1-6]XXXXXXXX を設定することです（ドットの前の番号を削除して、先頭に 0 を付加します）。このトランスレーション パターンは、フランスのサイトの AAR コーリング サーチ スペースのメンバー パーティションにのみ配置します。ベルギーのサイトからは、この同じ宛先に 0 00 33 1 58 04 58 58 として到達する必要があります。

図 9-38　サイト間 AAR コールにおけるダイヤル番号の変換



（注）　AAR 機能は、宛先の電話が到達不能であることが検出されてもトリガーしません。したがって、WAN の障害によって AAR 機能がトリガーすることはありません。

この状況を十分に理解するために、London（英国）、Paris（フランス）、Nice（フランス）にサイトがある Unified CM クラスタの例を考えます。Paris の DID 範囲の E.164 アドレスは、+33145678XXX です。ただし、フランスの公衆網内からコールする場合、これらの内線には、通常は 0145678XXX として到達します。London のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、そのストリングは 90033145678XXX です。一方で、Nice のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、そのストリングは 00145678XXX です。

単一の単純な ARR 設定を使用して上記の 3 つのケースを可能にするには、完全修飾 E.164 番号（+ 記号を含む）で AAR 宛先マスクを設定することが最善の方法となります。これによって、発信側電話機ごとに解釈できる宛先番号が作成されます。

デバイス モビリティ

デバイス モビリティには、IP ネットワーク内にあるデバイスのモビリティが向上するように設計された機能が備わっています（たとえば、本来 San Francisco で使用するように設定されている電話機を物理的に New York に移動させます）。デバイスは依然として同じ Unified CM クラスタに登録されますが、電話機が置かれている新しいサイトに基づいて、デバイスの一部の動作が調整されます。これらの変更は、電話機のある IP サブネットによってトリガーされます。

ローミングするとき、電話機はデバイスの現在のサブネットに関連付けられているデバイス プールに関連付けられているパラメータを継承します。ダイヤル プランから見て、次の 5 つの主要な設定パラメータの機能は、電話機の物理的な場所により変更できます。変更するこれらのパラメータについて、デバイスはホーム ロケーションの外部をローミングしているが、ホーム デバイスのモビリティ グループ内にいると見なされます。

- ローカル ルート グループ

  ローミング デバイス プールのローカル ルート グループが使用されます。たとえば、San Francisco から New York にデバイスがローミングする場合、パターンが標準ローカル ルート グループを呼び出すルート リストを指している場合は常に、公衆網へのコールのルーティングに New York デバイス プールのローカル ルート グループが使用されます。

- 発信側変換 CSS

  ローミング デバイス プールの発信側変換 CSS が使用されます。これにより、電話機は発信側電話番号表示モード（訪問した場所にある電話機の慣習的表示モード）を継承できます。

- デバイス コーリング サーチ スペース

  デバイス設定ページで設定されているデバイス コーリング サーチ スペースではなく、ローミング デバイス プールのデバイス モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールのデバイス モビリティ コーリング サーチ スペースが、ローミング電話機のデバイス コーリング サーチ スペースとして使用されます。サービス クラスに対して回線/デバイス アプローチを使用している場合、このアプローチは公衆網コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- AAR コーリング サーチ スペース

  デバイス設定ページで設定されている AAR コーリング サーチ スペースではなく、ローミング デバイス プールの AAR モビリティ コーリング サーチ スペースが使用されます。たとえば、デバイスが San Francisco から New York にローミングしているとき、New York デバイス プールの AAR コーリング サーチ スペースが、ローミング電話機の AAR コーリング サーチ スペースとして使用されます。このコーリング サーチ スペースは発信 AAR 公衆網コールが取るパスを確立し、ローカルな New York ゲートウェイにルーティングします。

- DN の AAR グループ

  着信 AAR コールの場合、DN のホスト電話機がローミングしているかどうかにかかわらず、DN に割り当てられている AAR グループが保持されます。これにより、AAR 宛先番号に対して確立された到達可能性の特性が保持されます。

  発信 AAR コールの場合、発信 DN の AAR グループでは、DN の設定ページで選択された AAR グループではなく、ローミング デバイス プールの AAR グループが使用されます。この AAR グループは、ローミング デバイス上のすべての DN に適用されることに注意してください。たとえば、New York から Paris にローミングするデバイス上のすべての DN（どちらの場所も同じデバイス モビリティ グループであることを前提とする）は、Paris デバイス プールの発信コールに対して設定されている AAR グループを継承します。この AAR グループはローミング デバイス上のすべての DN に割り当てられます。また、ローミング電話機上の DN から行われた AAR コールに対して適切なプレフィックスを付加することを許可します。

ローミング中の Call Forward All

デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、Unified CM ではローカル ゲートウェイへの到達にデバイス モビリティ CSS を使用します。ユーザが電話機で Call Forward All を設定している場合、CFA CSS が None に設定されていて、CFA CSS Activation Policy が With Activating Device/Line CSS に設定されていると、次のようになります。

- デバイスがホーム ロケーションにあるときに CFA CSS としてデバイス CSS と 回線 CSS が使用されます。
- デバイスが同一のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてローミング デバイス プールからのデバイス モビリティ CSS と回線 CSS が使用されます。
- デバイスが別のデバイス モビリティ グループ内をローミングしているとき、CFA CSS としてデバイス CSS と回線 CSS が使用されます。

「デバイス モビリティ」（P.25-15）の項で、この機能について詳しく説明します。

エクステンション モビリティ

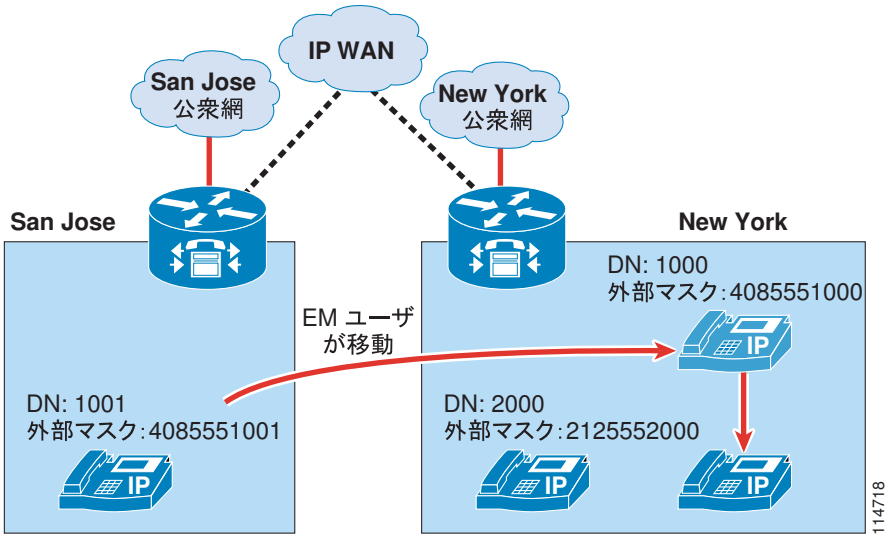
エクステンション モビリティ機能を使用すると、ユーザが IP Phone にログインしたとき、内線番号、スピード ダイヤル、Message Waiting Indicator（MWI; メッセージ待機インジケータ）ステータス、コール特権を含めて、そのユーザのプロファイルが自動的にその電話機に適用されるようになります。このメカニズムは、それぞれのエクステンション モビリティ ユーザに関連付けられる、デバイス プロファイルを作成することで成り立っています。デバイス プロファイルは、実質的には仮想 IP Phone であり、1 つまたはそれ以上の回線を設定したり、コール特権やスピード ダイヤルなどを定義したりできます。

IP Phone がログアウト状態になっている（つまり、エクステンション モビリティ ユーザがログインしていない）とき、この IP Phone の特性は、デバイス設定ページと回線設定ページによって決まります。ユーザが IP Phone にログインすると、デバイス設定は変更されませんが、既存の回線設定は Unified CM データベースに保存され、ユーザのデバイス プロファイルの回線設定によって置き換えられます。

エクステンション モビリティの重要な利点の 1 つは、ユーザがどこにいるかにかかわらず、同じ Unified CM クラスタによって制御されている IP Phone にユーザがログインできれば、そのユーザに対して、そのユーザ固有の内線番号で到達できることです。集中型コール処理を使用しているマルチサイト配置に対してエクステンション モビリティを適用すると、地理的に互いに分離している複数のサイトに対して、この機能を展開できます。

ただし、エクステンション モビリティ機能を「Automated Alternate Routing」（P.9-103）の項で説明している AAR 機能と組み合せる場合は、一定の制限事項があります。図 9-39 に示した例について考えます。エクステンション モビリティと AAR を集中型コール処理の Unified CM クラスタに配置していて、San Jose と New York にそれぞれ 1 つのサイトがあります。

図 9-39　エクステンション モビリティと AAR



この例では、通常、San Jose を拠点としているエクステンション モビリティ ユーザが、DN 1000 と DID 番号 (408) 555-1000 を持っているとします。このユーザの外部電話番号マスクは、4085551000 と設定されています。このユーザが New York サイトに移動し、ログインします。さらに、San Jose と New York 間の IP WAN 帯域幅がすべて使用されているとします。

San Jose にいる内線番号 1001 のユーザが 1000 にコールすると、AAR がトリガーされ、発信側の AAR コーリング サーチ スペースと発信側、着信側の AAR グループに基づいて、914085551000 への新しいコールが、San Jose の電話機によって試行されます。このコールは、San Jose のゲートウェイを使用して公衆網にアクセスしますが、DID (408) 555-1000 が同じゲートウェイによって所有されているため、公衆網はコールをこのゲートウェイに戻します。San Jose のゲートウェイは、内線番号 1000 を持つ電話へのコールを確立しようとしますが、この電話は現在 New York にあります。New York にアクセスするための帯域幅を使用できないため、AAR 機能がもう一度呼び出され、次の 2 つのうち、いずれかのシナリオが発生します。

- ゲートウェイの AAR コーリング サーチ スペースに外部公衆網ルート パターンが含まれている場合、ループが開始され、San Jose サイトにあるすべての公衆網トランクが使い果たされる。
- 逆に、ゲートウェイの AAR コーリング サーチ スペースに内部の番号のみが含まれている場合は、コールが失敗し、発信者にはファーストビジー トーンが聞こえる。この場合は、1 つの公衆網コールが発生して 1 つが受信されるため、コールのセットアップ中、San Jose のゲートウェイでは 2 つの公衆網トランクが使用されます。

ヒント　ここで説明したようなルーティング ループを防止するには、ゲートウェイ設定ページでコーリング サーチ スペースを設定するときに、必ず内部の宛先のみを含め、同じゲートウェイを含んでいるルート グループやルート リストを指すルート パターンを一切含めないようにします。

この例では、エクステンション モビリティが Cisco Unified Communications の動的な側面を利用しているため、サイト間のコール ルーティングで IP ネットワークを使用する必要があることを中心に説明しています。公衆網に定義されている E.164 番号は静的なものであり、公衆網ネットワークはエクステンション モビリティ ユーザの移動を認識しません。AAR 機能は、コール ルーティングを公衆網に依存しているため、ホーム サイト以外のサイトに移動したエクステンション モビリティ ユーザに対して、この機能を使用して到達することはできません。

（注）　ただし、エクステンション モビリティ ユーザが自分のホーム サイトと同じ AAR グループに属するリモート サイトに移動した場合には、使用可能な IP WAN 帯域幅が十分にないとき、そのユーザは AAR 機能を使用して他のサイトへのコールを発信できます。これは、コールの発信元の電話機の AAR コーリング サーチ スペースによってそれらのコールのパスが決定されるためです。この AAR コーリング サーチ スペースはユーザがエクステンション モビリティにログイン、またはログアウトしても変更されません。また、このスペースは訪問したリモート サイトのゲートウェイを使用するように設定する必要があります。

ヒント　登録解除されたエクステンション モビリティ プロファイル DN がボイスメールにコールを送信するように設定してください。詳細については、「自動転送コーリング サーチ スペース」（P.9-99）を参照してください。

Cisco Unified Mobility 固有の考慮事項

Cisco Unified Mobility（「Cisco Unified Mobility」（P.25-37）についての項を参照）では、コールのルーティングに直接影響を与える機能に依存しています。ダイヤル プランに関連する Cisco Unified Mobility パラメータの影響を理解するには、次の例について考えてみます。

（注）　この説明で必要なパラメータのみを、ここで示しています。

ユーザ Paul は、次のように設定された IP Phone を所有しています。

DN：8 555 1234

DID 番号：+1 408 555 1234

外部電話番号マスク：408 555 1234

回線コーリング サーチ スペース：P_L_CSS

デバイス コーリング サーチ スペース：P_D_CSS

Paul の DN は、次のように設定されたリモート宛先プロファイル（RDP）に関連付けられています。

コーリング サーチ スペース：P_RDP_CSS

再ルーティング コーリング サーチ スペース：P_RDP_Rerouting_CSS

発信側変換 CSS：P_CPT_CSS

Paul の RDP は、次のように設定されたリモート宛先に関連付けられています。

宛先番号：+1 514 000 9876（これは Paul の携帯電話番号。シングルモードまたはデュアルモードのいずれかの電話機）

Paul または Ringo の DID 番号にかけられた公衆網からのコールは、次のように設定されたゲートウェイによって処理されます。

コーリング サーチ スペース：GW_CSS

有効桁：7

プレフィックス DN：8

ユーザ Ringo は、次のように設定された IP Phone を所有しています。

DN：8 555 0001

DID 番号：408 555 0001

外部電話番号マスク：408 555 0000（これは企業の代表番号）

回線コーリング サーチ スペース：R_L_CSS

デバイス コーリング サーチ スペース：R_D_CSS

次の項では、コール ルーティングでの上記のモビリティ パラメータの影響について説明します。

リモート宛先プロファイル

リモート宛先プロファイル（RDP）はディレクトリ番号（たとえば、ユーザの IP Phone の DN）およびリモート宛先（たとえば、ユーザの携帯電話番号）と関連付けられています。RDP は IP Phone と、リモート宛先として設定された外部番号（たとえば、携帯電話）間のやり取りを制御します。

（注）　リモート宛先は、オンクラスタ DN を宛先番号として設定することはできません。

リモート宛先プロファイルの再ルーティング コーリング サーチ スペース

リモート宛先プロファイルに関連付けられている DN にコールが発信された場合、コールは DN と、リモート宛先として設定されている番号の両方にコールします。

発信者が宛先 IP Phone に到達できるかどうかは、発信者のコーリング サーチ スペース設定によって制御されます。ただし、コールがリモート宛先に分岐（転送）されるかどうか（たとえば、携帯電話）は、着信側モビリティ ユーザの再ルーティング コーリング サーチ スペースによって制御されます。

例：
Ringo は、自分の IP Phone から 8 555 1234 とダイヤルすることによって Paul にコールします。Paul の IP Phone が鳴り、彼の携帯電話も鳴ります。

Ringo が Paul の DN に到達できるかどうかは、Ringo の IP Phone の回線およびデバイス コーリング サーチ スペースによって制御されています。ダイヤルした宛先（8 555 1234）は、連結されたコーリング サーチ スペース R_L_CSS および R_D_CSS にあるパーティションにあります。

このコールが Paul の携帯電話に分岐（転送）されるようにするには、設定されたリモート宛先（+1 514 000 9876）がコーリング サーチ スペース P_RDP_Rerouting_CSS にあるパターンと一致する必要があります。

（注）　Ringo の電話機に割り当てられたダイヤリング特権で外部コールが許可されていなくても、リモート宛先へのコールは、Paul のリモート宛先プロファイルに関連付けられた再ルーティング コーリング サーチ スペースによって処理されます。

リモート宛先プロファイルのコーリング サーチ スペース

Cisco Unified CM 6.0 では、リモート宛先と定義された番号から発信されたコールのルーティングに RDP のコーリング サーチ スペースが使用されます。このスペースは DN の回線 CSS と関連付けられています。連結の順序は、回線 CSS の後に RDP の CSS です。

クラスタに発信された外部コールの発番号がリモート宛先として定義される番号と一致した場合、発番号は、一致したリモート宛先に関連付けられた回線の DN に置き換えられます。また、コールのルーティングに使用されるコーリング サーチ スペースは、次のスペースを連結したものです。

- 一致したリモート宛先番号に関連付けられた DN の回線コーリング サーチ スペース
- 一致したリモート宛先に関連付けられた RDP のコーリング サーチ スペース

Unified CM 6.1 およびそれ以降のリリースでは、新しいサービス パラメータ（Inbound Calling Search Space for Remote Destination）が、クラスタのリモート宛先のいずれかから発信されたコールのルーティングに使用されるコーリング サーチ スペースを制御します。デフォルト設定は Trunk or Gateway Inbound Calling Search Space です。これはすべての着信コールをトランクまたはゲートウェイの設定済み CSS を使用してルーティングします。サービス パラメータが Remote Destination Profile + Line Calling Search Space に設定されている場合、動作はすべての Unified CM 6.*x* リリースで同じになります。この新しいサービス パラメータには、発番号の置換に影響はありません。

（注）　Unified CM 6.1 およびそれ以降のリリースのデフォルト動作は、リモート宛先と定義された番号から発信された着信コールのルーティングに関して、Unified CM 6.0 の動作とは異なります。コールのルーティングが簡素化されるため、シスコは Unified CM 6.1 のデフォルト設定を使用することを推奨します。

同じクラスタ内のリモート宛先として定義されているすべての番号は、クラスタに着信する任意の外部コールで一致するものを検索します。

次の例では、Unified CM 6.1 およびそれ以降のリリースで、Inbound Calling Search Space for Remote Destination サービス パラメータが Trunk or Gateway Inbound Calling Search Space に設定されていることを前提としています。

例：
Paul は、Ringo の卓上電話にコールするために自分の携帯電話を使用しています。コールは公衆網からゲートウェイに着信します。発番号は 514 000 9876 で着番号は 408 555 0001 です。コールは Ringo の電話機にルーティングされます。Ringo の電話機に発番号として表示される番号は、Paul の卓上電話番号 8 555 1234 です。これにより、Paul の携帯電話番号は表示されず、Missed および Received コール リストから発信された Ringo のコールが Paul の IP Phone を鳴らします。このようにして企業モビリティ機能の完全なセットが使用できるようになります。

コールがゲートウェイに着信するとき、公衆網では発番号を 514 000 9876、着番号を 408 555 0001 と表示します。ゲートウェイの設定は着信番号の末尾から 7 桁の有効桁を保持し、先頭に 8 のプレフィックスを付加し、宛先番号として 8 555 0001 を生成します。

システムは発番号が Paul のリモート宛先番号と一致するかどうかを検出します。一致を検出すると、次の処理が行われます。

1. 発番号を Paul の DN、8 555 1234 に変更します。
2. 着信ゲートウェイのコーリング サーチ スペースを使用して、コールを着信番号にルーティングします。具体的には、ルーティングは GW_CSS コーリング サーチ スペースを介して行われます。

ゲートウェイにより提示される宛先（着信）番号は、電話機の DN である必要があります。また、上記の手順 1 で示した発信側の置換では、Missed/Received コール リストからワンタッチ ダイヤルを使用した方法を示しています。

（注）　リモート宛先番号をパーティションに分類する方法はありません。複数のユーザ グループ（異なる会社、請負業者など）で同じクラスタを使用している場合、この点に注意する必要があります。Unified CM 6.1 およびそれ以降のリリースで、Inbound Calling Search Space for Remote Destination サービス パラメータが Trunk or Gateway Inbound Calling Search Space に設定されている場合、発信番号がリモート宛先に一致するかどうかにかかわらず、コールのルーティングは、着信トランクまたはゲートウェイの CSS に基づきます。ただし、発番号の置換は、発信側がリモート宛先に一致した場合でも行われます。これは、テナントのリモート宛先番号から別のテナントの DID 番号へのコールが、発信側のオンネット エクステンション DN と一致する、変換済み発番号で提示されることを意味します。

（注）　発番号が使用できない着信外部コールは、着信ゲートウェイの CSS に従ってルーティングされます。これは、SIP または H.323 トランクなどの IP トランクからの着信コールにも当てはまります。

リモート宛先プロファイルの発信側変換 CSS とトランスフォーメーション パターン

企業の IP Phone からモビリティ対応の DN に発信されたコールは、企業の 宛先 IP Phone の DN と、1 つの（または複数の）外部宛先の両方に分岐（転送）されます。これによる 1 つの課題は、それぞれの宛先電話機のダイヤル プランに適合した発番号を送信することです。これは、Missed および Received コール リストからのコールのリダイヤルを可能にするために必要です。企業の電話機の場合、発番号はリダイヤル可能な企業の電話番号である必要があります。公衆網のリモート宛先の場合（自宅の電話機または携帯電話）、発番号は、発信側 IP Phone と関連付けられている企業の番号から、公衆網からリダイヤル可能な番号（一般に、発信側電話機の DID 番号）に変換する必要があります。

コールがモビリティ対応の企業 DN に発信された場合、発信者の発番号に一致するものを検索するために、関連付けられたリモート宛先プロファイルのコーリング サーチ スペースが使用されます。このスペースには、トランスフォーメーション パターンを含むパーティションが含まれています。

トランスフォーメーション パターンは、企業形式から公衆網形式への発番号の適合を制御しています。トランスフォーメーション パターンは、着信番号ではなく、発番号をマッチングするという点で、Unified CM の他のすべてのパターンと異なります。マッチング処理は、正規表現（たとえば、8 555 XXXX）を使用して行われます。そして変換処理では、発信側 DN の外部電話番号マスクのほかに、トランスフォーメーション パターンを使用し、番号をプレフィックスとして付加できます。

一致すると、設定済みのすべての変換が実行されます。そして一致したリモート宛先プロファイルに関連付けられているすべてのリモート宛先への到達に、変換後の発番号が使用されます。

例：
Ringo が Paul にコールすると、Paul の IP 電話には発番号が 8 555 0001 と表示され、Paul の携帯電話には 408 555 0001 と表示されるようにします。

この場合、次のパラメータを使用してトランスフォーメーション パターンを作成します。

Pattern：8 555 XXXX

Partition：SJ_Calling_Transform

Use calling party's external phone number mask：チェックしない

Calling Party Transformation mask：555 XXXX

Prefix Digits (outgoing calls)：408

パーティション SJ_Calling_Transform がコーリング サーチ スペース P_CPT_CSS に配置されていることを確認する必要もあります。

Ringo からのコールが Paul の電話機に固定されている場合、2 つの別々のコール レッグが試行されます。最初のコール レッグは Paul の IP Phone を鳴らし、発信者の DN を発番号（つまり 8 555 0001）と表示します。2 番めのコール レッグは Paul のリモート宛先プロファイルを介して試行されます。参照されるすべてのパーティションのトランスフォーメーション パターン内にある 8 555 0001 の一致を検索するために、RDP の発信側変換 CSS（P_CPT_CSS）が使用されます。パターン 8 555 XXXX はパターン SJ_Calling_Transform でマッチングされます。トランスフォーメーション マスクが発番号に適用され、555 0001 が生成されます。プレフィックス番号が追加され、リモート宛先にコールが発信された場合に変換された発番号 408 555 0001 が使用されます。

この例では、Ringo の DID 番号と異なる番号に設定されているため、外部電話番号マスクを使用していないことに注意してください。これにより、オフネットの宛先に提示される発番号が発信者と着信側で異なっている必要がある場合に、柔軟性が提供されます。Ringo から Paul へのコールは同僚間のも

のであるため、Ringo の DID 番号が公開されるのは許容されると見なされます。Ringo の次のコールは顧客に対するものである可能性があります。この場合、企業の代表番号 408 555 0000 が、宛先に提示されるのに最も望ましい発番号です。

（注）　発信側トランスフォーメーション コーリング サーチ スペースには <none> パーティションが暗黙的に含まれていません。そのため、<none> パーティションに残っているトランスフォーメーション パターンはどの発信側トランスフォーメーション コーリング サーチ スペースにも適用されません。これは Unified CM 内の他のすべてのパターンと異なります。Unified CM では、<none> パーティション内に残るすべてのパターンは暗黙的にすべてのコーリング サーチ スペースに含まれます。

適用ダイヤル規則

リモート宛先と定義される番号は、着信コールを企業のモビリティ コールとして識別し、固定するためにも使用されます。公衆網がコールを識別する形式は、企業のダイヤル プランがコールを外部番号にダイヤルする場合の形式と異なることがよくあります。適用ダイヤル規則は、リモート宛先で、コールをリモート宛先に分岐（転送）する際に必要な形式に設定するために使用できます。これらの規則では、リモート宛先として設定された番号から、数字を削除したり、数字をプレフィックスとして付加したりできます。

例：
番号 514 000 9876 は Paul のリモート宛先番号として設定されています。この番号は、企業に着信するコールを識別するために公衆網が使用する形式に対応します。ただしこれは、発信コールで企業のダイヤル プランが使用する形式（91 をプレフィックスとして付加する必要があります）とは異なります。この場合、リモート宛先の形式を企業ダイヤル プランの形式に適合させるために、適用ダイヤル規則を作成する必要があります。

適用ダイヤル規則：

名前：514000_ten

説明：プレフィックス 91 を 514000 で始まる 10 桁の番号に付加するために使用

番号の先頭：514000

桁数：10

削除する桁数：0

パターンで付加するプレフィックス：91

この例では、Paul の携帯電話から企業へかけられたコールは、514 000 9876 からのものと識別されます。これは、Paul の番号がリモート宛先と設定されている形式に一致します。このため、マッチングが行われ、Paul の卓上電話コールの固定をトリガーします。またオンネットの宛先に表示される発番号の最適化も行われます（たとえば、コールが Ringo の DID 番号に対して行われた場合、Ringo にはその着信が 8 555 1234 から来たものと表示されます）。

コールが Paul の企業 DN 番号に対して行われた場合、Paul のリモート宛先番号に分岐（転送）されたコール レッグは、上記の適用ダイヤル規則によって処理されます。ストリング 514 000 は Paul のリモート宛先番号の先頭と一致します。また、この番号は 10 桁であるため、数字は削除されず、91 がプレフィックスとして付加されます。これにより、Paul のリモート宛先プロファイル コーリング サーチ スペース（この場合は P_RDP_CSS）を介してルーティングされる番号として、91 514 000 9876 が生成されます。

（注）　このアプローチでは、IP Phone から行われたコールのルーティングのためにすでに定義済みのコーリング サーチ スペースを再利用する機能を提供します。発信コールに対してプレフィックスを付加する必要のない新しいコーリング サーチ スペース（つまり、直接 514 000 9876 にコールをルーティングできる）は好ましくありません。外部パターンとオンネット パターンが重複する状況が発生する可能性があるためです。

Immediate Divert（iDivert）

Immediate Divert（iDivert）機能は、コールを直接ボイスメールに送信するために使用します。コールが鳴っているとき（着信）、コールが保留中のとき、またはコールが接続されたときに呼び出すことができます。iDivert 機能では、着信コールが呼び出した電話機のボイスメール ボックスまたは着信側のボイスメール ボックスのいずれかに迂回されます。拡張機能は、転送されたコールやアプリケーションによってリダイレクトされたコールなどの迂回されたコールにのみ適用可能です。

Cisco Unified CM 5.1 の iDivert 機能拡張

iDivert 機能は Cisco Unified CM 5.1 で拡張され、呼び出した電話機のボイスメール ボックス（従来の処理）または着信側のボイスメール ボックス（拡張された処理）のいずれかに着信コールを迂回させることができるようになりました。拡張機能は、転送されたコールやアプリケーションによってリダイレクトされたコールなどの迂回されたコールにのみ適用可能です。

次の例を参考にしてください。

> 電話機 A が電話機 B にコールするとします（電話機 B のコールは電話機 C に転送されます）。電話機 C が鳴っているとき、電話機 C 側にいるユーザは [iDivert] ソフトキーをアクティブにします。これにより、2 つの選択肢が提供されます。1 つめの選択肢では、コールが発信側のボイスメール（この場合、電話機 B のボイスメール ボックス）に送信されます。2 つめの選択肢では、コールが iDivert 呼び出し側のボイスメール（この場合、電話機 C のボイスメール ボックス）に送信されます。コールが鳴っているとき、接続中、または保留中の場合のいずれかに、電話機 C がこの機能を呼び出しても、同じ選択肢を選択できます。

iDivert 機能を呼び出す前に、コールが Auto Call Pickup、Call Transfer、Call Park、Call Park Reversion、Conference、または MeetMe Conference によって処理されると、コールは「迂回された」コールとは見なされなくなり、この場合で使用できる iDivert 機能は、従来の iDivert 処理だけになります（つまり、コールを呼び出し側のボイスメールに送信します）。たとえば、電話機 A が電話機 B にコールするとします。電話機 B のコールは電話機 C に転送され、その後電話機 C はコールを電話機 D に転送します。コールに適用された最後のアクションが電話機 D への転送であるため、これは迂回されたコールでは*ありません*。電話機 D が iDivert 機能を呼び出すと、コールは電話機 D のボイスメール ボックスに送信されます。

上で説明した iDivert の完全な機能を有効にするには、Unified CM サービス パラメータ **Use Legacy Immediate Divert** を **False** に設定します。有効にすると、拡張された iDivert は自動的に QSIG トランクを介してこの機能を使用することを許可します。このため、呼び出し側のボイスメール ボックスが、QSIG を介して接続されているテレフォニー システムでホストできます。

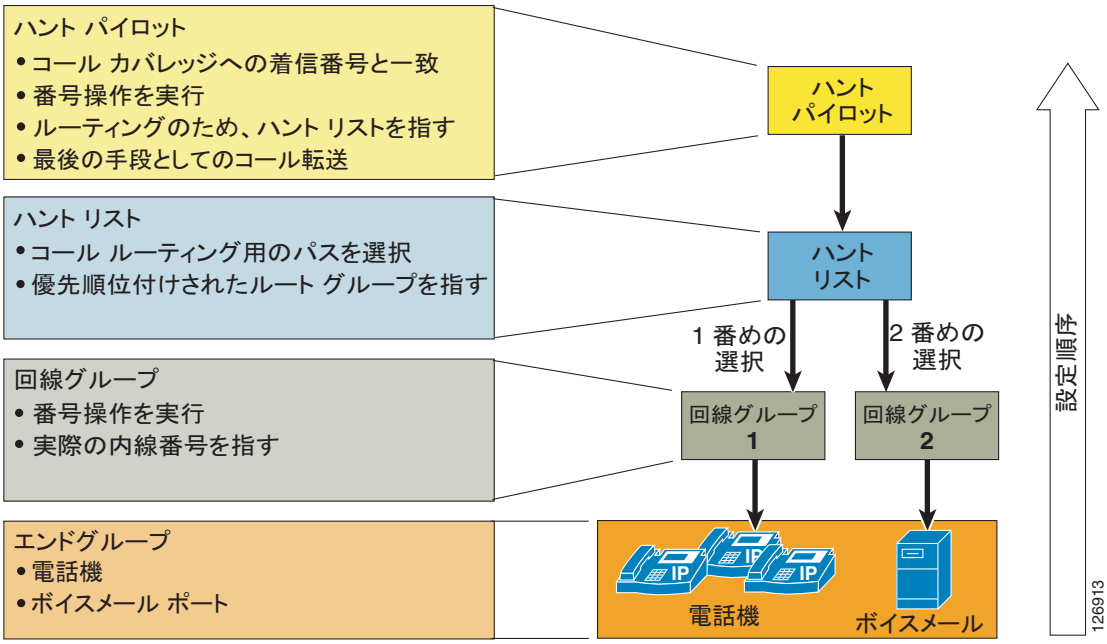
iDivert が、QSIG を使用して他の電話システムに接続しているクラスタで使用している場合、コールを受信したときに従来の iDivert 機能のみ（使用できる選択肢はコールを呼び出し側のボイスメールに送信することのみ）が電話機に提供されます。たとえば、電話機 A および B がクラスタ 1 にあり、電話機 X が QSIG に接続された別のテレフォニー システムであるとします。電話機 A が電話機 X にコールし、電話機 X のコールが電話機 C に転送されます。コールが電話機 C に接続されると、iDivert は、QSIG パスの置き換えが実行されていない場合に限り、従来（呼び出し側のボイスメール）と拡張（着信側のボイスメール）の宛先の両方を提供します。QSIG パスの置き換え後、電話機 C が iDivert を呼び出した場合、選択可能な宛先は電話機 C のボイスメール ボックスのみです。

ハント リストと回線グループ

*ハント パイロット*は、通常はコール カバレッジや、Skinny Client Control Protocol（SCCP）エンドポイントを通じたコール分配に使用されます。コールの分配には、ハント コンストラクトを使用できます。このハント コンストラクトは、3 層式のアーキテクチャに基づいています。外部コールのルーティングに使用されるアーキテクチャに似たこのアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。

Unified CM は、着信番号と一致する設定済みハント パイロットを検索し、それを使用して、対応するハント リストを選択します。ハント リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、*回線グループ*と呼ばれます。図 9-40 では、Unified CM のハント コンストラクトの 3 層式アーキテクチャを示しています。

図 9-40　　Unified CM のハント コンストラクトの 3 層式アーキテクチャ



ハント パイロット

ハント パイロットは、コールをディレクトリ番号にルーティングするために Unified CM で設定された、ルート パターンのように数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ハント パイロットは、ハント リストを直接指しています。ハント リストは回線グループを指しており、回線グループは、最終的に SCCP エンドポイントを指しています。

ハンティングが次のいずれかまたは両方の理由で失敗した場合、コールを最終的な宛先にリダイレクトできます。

- すべてのハンティング オプションを使い果たしても、コールはまだ応答されていない。
- タイムアウト期間が満了した。

このコール リダイレクションは、[Hunt Pilot] 設定ページの [Hunt Forward Settings] セクションで設定します。このリダイレクトの宛先は、次のいずれかから選択できます。

- Unified CM の内部コール ルーティング テーブルに含まれている、特定のパターン。

- 個人用プリファレンス。このプリファレンスは、もともとの着信番号の Call Forward No Coverage 設定を指しています。

たとえば、個人用プリファレンス オプションを実装するには、[Forward No Answer] フィールドに従ってコールをハント パイロットへリダイレクトするようにユーザの電話を設定して、コールに応答できるユーザが他にいないかどうか検索できるようにします。すべてのハンティング オプションが使い果たされたか、タイムアウト期間が満了したためにコール ハンティングが失敗した場合、コールを当初の宛先ユーザが設定している宛先に転送できます。たとえば、ユーザの DN 設定ページにある [Forward No Coverage] フィールドにボイスメール番号を設定すると、ハンティングが失敗した場合、コールはそのユーザのボイスメール ボックスに送信されます。

ハント パイロットの処理するコールには、次の考慮事項が適用されます。

- コール ピックアップとグループ コール ピックアップは、ハント パイロットが分配するコールではサポートされません。回線グループのメンバーは、回線グループの他のメンバーに提供されたハント パイロット コールについては、メンバー同士が同じコール ピックアップ グループに属している場合でもピックアップできません。
- ハント パイロットは、自身の回線グループのメンバーとハント パイロットが別のパーティションに配置されている場合でも、コールを自身の回線グループのいずれかのメンバーに分配できます。ハント パイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント リスト

ハント リストは、コール カバレッジに使用できるパス（回線グループ）が優先順位順に並べられたリストです。ハント リストには次の特性があります。

- 複数のハント パイロットが同一ハント リストを指すことができます。
- ハント リストは、ハント パイロット番号へのコールが行われたときに提供される代替電話機セットとして機能する回線グループが、優先順位順に並べられたリストです。たとえば、特定のサイトにある一連の電話機の中から、コールを受け取る電話機を見つけるために使用できます。コールが受け取られない場合、ハント リストは別のサイトにある電話機を指定する、別の回線グループを通じたコールの提供を試みます。
- ハント リストは、番号操作は一切実行しません。
- 複数のハント リストに、同じ回線グループを含めることができます。

回線グループ

回線グループのメンバーは、Unified CM が制御しているユーザ内線番号です。このため、コールを回線グループのメンバー間に分配するときは、Unified CM がコールを制御します。コールが応答されなかった場合や、内線番号が使用中または未登録の場合は、ハント オプションをコールに適用できます。

回線グループは、コールが分配される順序を制御し、次の特性を持っています。

- 回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。
- 1 つの内線番号が複数の回線グループに含まれていることがあります。
- コンピュータ テレフォニー インテグレーション（CTI）ポートと CTI ルート ポイントは、回線グループに追加できません。したがって、CTI アプリケーション（Cisco Customer Response Solutions（CRS）や IP 音声自動応答装置（IP IVR）など）を通じて制御されるエンドポイントには、コールを分配できません。

- Unified CM は、割り当てられている分配アルゴリズムに従ってコールを各デバイスに分配します。Unified CM は、次のアルゴリズムをサポートしています。
  - トップダウン
  - 循環
  - 最長アイドル時間
  - ブロードキャスト
- No-Answer、Busy、Not-Available のいずれかのイベントが発生すると、分配されたコールを回線グループがハント オプションに基づいて内線番号にリダイレクトします。Unified CM は、次のハント オプションをサポートしています。
  - 次のメンバーにアクセスし、その後はハント リスト内の次のグループにアクセスする。
  - 次のメンバーにアクセスするが、次のグループにはアクセスしない。
  - 残りのメンバーをスキップして、次のグループに直接アクセスする。
  - ハンティングを停止する。

ハント グループのログアウト

ユーザは、[HLog] ソフトキーをアクティブにすることによって、ハント グループからログアウトできます。いったんアクティブにすると、この機能では実質的に、電話機上で設定されているすべての回線が、どのハント グループにも含まれていないように動作させます。電話機には「Logged out of Hunt Group」と表示されます。回線グループにシェアド ラインが含まれている場合、デバイス上でログアウト状態のシェアド ラインのすべてのインスタンスは呼び出されません。反対に、デバイス上でログイン状態のシェアド ラインのすべてのインスタンスは呼び出されません。

どのハント グループにも含まれていない回線は、HLog 機能の状態に関係なく、通常どおり呼び出されます。

HLog 機能は Unified CM Administration からアクティブにできます。デフォルトでは、[HLog] ソフトキーはソフトキー テンプレートでは設定されません。いったん、ソフトキー テンプレートに追加されると、電話機が接続状態、保留状態、またはオンフック状態のときに HLog ボタンがディスプレイに表示されます。

Hunt Group Logoff Notification サービス パラメータでは、回線グループから来るコールがログオフ状態の電話機に着信した場合の着信音のオプションを提供します。Hunt Group Logoff Notification サービス パラメータは、[Service Parameters Configuration] ページの Clusterwide Parameters (Device - Phone) セクションにあります。この機能を有効にするには、TFTP サーバ上に有効な着信音ファイルがあることを確認してください。無効なファイル名が指定されると、何も音が再生されません。

ハント アルゴリズムとハント オプションの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com

回線グループ デバイス

回線グループ デバイスは、回線グループがアクセスするエンドポイントであり、次のいずれかのタイプに該当します。

- Skinny Client Control Protocol（SCCP）エンドポイント（Cisco Unified IP Phones など）
- SIP エンドポイント
- ボイスメール ポート（Cisco Unity）

- H.323 クライアント
- MGCP ゲートウェイに接続されている FXS

時間帯ルーティング

この機能を使用するには、次の要素を設定します。

- 期間
- タイム スケジュール

期間を利用すると、営業開始時刻と終了時刻を設定できます。この開始時刻と終了時刻は、コールをルーティングできる期間を示しています。これらの時刻に加えて、毎週または毎年発生するイベントを設定することもできます。さらに、Start Time オプションと End Time オプションにある No business hours を選択して、休業時間を設定することもできます。このオプションを選択した場合は、すべての着信コールがブロックされます。

タイム スケジュールは、パーティションに割り当てられている特定の期間をグループにまとめたものです。このタイム スケジュールによって、指定した期間中にパーティションがアクティブまたは非アクティブのどちらになっているかが判断されます。一致したパターンやダイヤリング パターンには、そのダイヤリング パターンの配置されているパーティションがアクティブになっている場合のみ到達できます。

図 9-41 では、同じコール パターン（8000）を持つ 2 つのハント パイロットが、2 つのパーティション（RTP_Partition、SJC_Partition）内に設定されています。これらのパーティションには、一連の定義済み期間を保持したタイム スケジュールがそれぞれ割り当てられています。たとえば、RTP の電話には、ハント パイロット 1 を使用することで、月曜日から金曜日の午前 8 時～午後 12 時（東部標準時。GMT - 5.00）まで、および日曜日の午前 8 時から午後 5 時まで到達できます。同様に、SJC の電話には、ハント パイロット 2 を使用することで、月曜日から金曜日の午前 8 時～午後 5 時（太平洋標準時。GMT - 8.00）まで、および土曜日の午前 8 時～午後 5 時まで到達できます。この例では、どちらのハント パイロットも 7 月 4 日は非アクティブです。

図 9-41　時間帯ルーティング

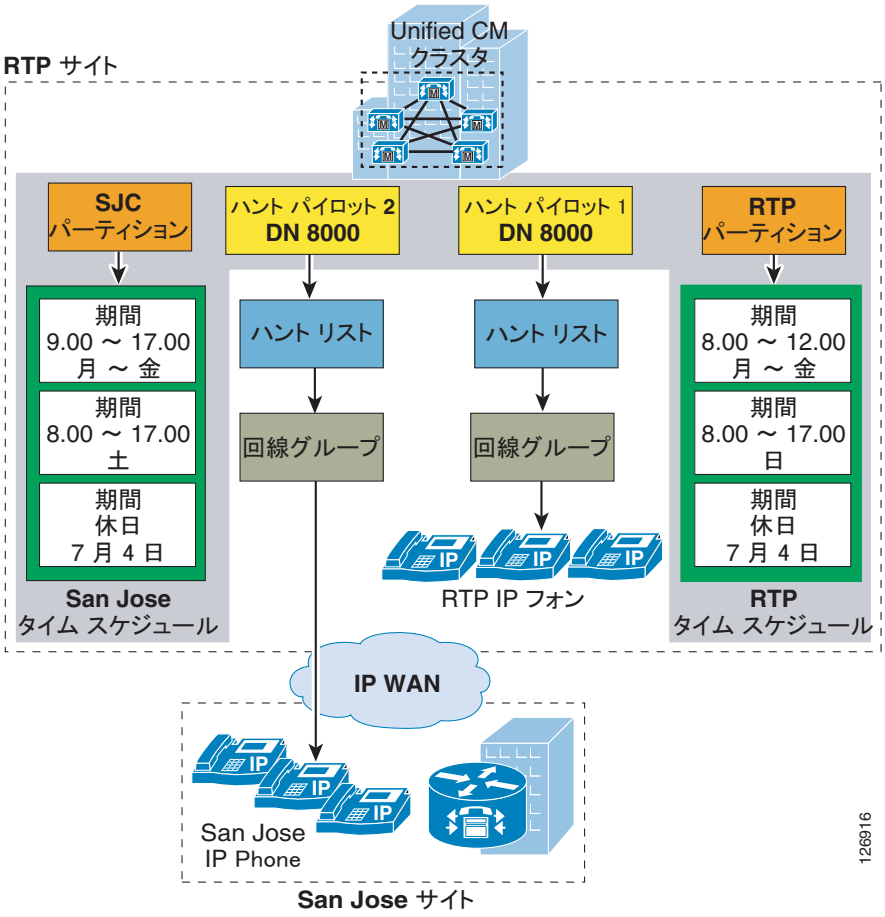


図 9-41 の例では、水曜日の午後 3 時にハント パイロット（8000）に着信したコールは、SJC の電話に転送されます。一方、このハント パイロットに 7 月 4 日にコールした人は、別のパターンが 8000 に一致しない限り、ファーストビジー トーンを受信します。

論理パーティション

論理パーティションには、次の要素が含まれます。

- デバイス タイプ。電話機は *interior* として分類され、ゲートウェイとトランクは *border* として定義されます。表 9-9 に、各デバイスのエンドポイント タイプを示します。
- ジオロケーション。エンドポイントにはポリシーの決定に使用される住所が割り当てられます。
- ジオロケーション フィルタ。ポリシーの決定は、ジオロケーション オブジェクトのサブセットに対して行うことができます。
- ポリシー。エンドポイント間の通信は、それらの相対的な（フィルタ処理された）ジオロケーションとデバイス タイプに基づいて許可または拒否されます。

（注）　コールのすべての参加者が *interior* として分類されないと、ポリシーは適用されません。つまり、同じクラスタにある電話機間のコールに論理パーティション ポリシーが適用されることはありません。

（注）　ジオロケーションは、Unified CM で設定するコール アドミッション制御用のロケーションや、デバイス モビリティに使用される物理ロケーションと混同されることはありません。

表 9-9　デバイス タイプ

論理パーティションのデバイス タイプ	Cisco Unified Communications Manager デバイス
Border	• ゲートウェイ（H.323 ゲートウェイなど） • Inter-cluster Trunk（ICT）（ゲートキーパー制御および非ゲートキーパー制御の両方） • H.225 トランク • SIP トランク • MGCP ポート（E1、T1、PRI、BRI、FXO）
Interior	• 電話機（SCCP、SIP、またはサードパーティ） • CTI ルート ポイント • VG224 アナログ電話 • MGCP ポート（FXS） • Cisco Unity ボイスメール（SCCP）

論理パーティションのデバイス タイプ

Unified CM は、エンドポイントを *interior* または *border* に分類します。この分類は固定されており、システム管理者が変更することはできません。

ジオロケーションの作成

(RFC) 4119 規格には、ジオロケーションの基本情報が記載されています。ジオロケーションには、次のオブジェクトによって指定される住所形式が使用されます。

- 名前
- 説明
- 2 文字の短縮形を使用した国名
- 州、地区、または地域（A1）
- 国または行政区（A2）
- 市町村（A3）
- 自治区（A4）
- 地区（A5）
- 街（A6）
- N や W など、街の先頭の方角指示（PRD）
- SW など、街の末尾のサフィックス（POD）
- 通りや区画など、住所のサフィックス（STS）
- 番地（HNO）

- A、1/2 など、番地のサフィックス（HNS）
- ランドマーク（LMK）
- 部屋番号など、ロケーションの補足情報（LOC）
- フロア（FLR）
- 会社または居住者の名前（NAM）
- 郵便番号（PC）

（注）　Unified CM では、ジオロケーションを手動で定義する必要があります。

ジオロケーションの割り当て

デバイスには、優先順位に従ってデバイス ページ、デバイス プール、またはエンタープライズ パラメータで設定されたデフォルトのジオロケーションのいずれかからジオロケーションが割り当てられています。

ジオロケーション フィルタの作成

ジオロケーション フィルタでは、異なるエンドポイントのジオロケーションを比較するときに使用するジオロケーション オブジェクトを定義します。たとえば、電話機のグループには、それらの電話機が置かれている部屋やフロアを除いて、同じジオロケーションが割り当てられる可能性があります。ポリシーによっては、同じ建物内のエンドポイントを同じ非公開ユーザ グループに所属するものと見なし、通信を許可する場合もあります。各電話の実際のジオロケーションは異なりますが、フィルタ処理されたジオロケーションは同じになります。この方法は、ジオロケーションの最上位のフィールドだけにポリシーを適用する必要がある場合に役立ちます。たとえば、異なる都市にある電話機とゲートウェイ間の通信を拒否し、同じ都市内の電話機とゲートウェイ間の通信は許可するポリシーは、都市よりも詳細なオブジェクトを無視してフィルタ処理された相対的なジオロケーションを基にできます。

ジオロケーション フィルタの割り当て

電話機は、デバイス プールのフィルタの割り当てを継承します。ゲートウェイとトランクには、優先順位に従ってデバイスまたはデバイス プール レベルでジオロケーション フィルタを設定できます。

論理パーティション ポリシーの設定

論理パーティション ポリシーは、ジオロケーション ID 間に設定されます。ジオロケーション ID は、フィルタ処理されたジオロケーションとデバイス タイプの組み合せになります。フィルタ処理されたジオロケーションを取得するには、デバイスのジオロケーションを呼び出し、デバイスに関連付けられたジオロケーション フィルタを適用します。

ポリシーは、ジオロケーション オブジェクトのセットとデバイス タイプの組み合せ（ソース ジオロケーション ID）として、そのようなもう 1 つの組み合せ（ターゲット ジオロケーション ID）と関係付けて作成されます。関係が一致すると、設定されている「許可」または「拒否」の処理がコール レッグに適用されます。

（注）　ポリシーに設定されているジオロケーション オブジェクトのセットはそれぞれ、1 つのデバイス タイプに関連して考慮されます。たとえば、国 = インド、州 = カルナタカ、市 = バンガロールのようなジオロケーション オブジェクトのセットは、バンガロールの電話機に対する処理に関してはデバイス タイプ Interior に関連付ける必要があり、バンガロールのゲートウェイに対する処理に関してはデバイス タイプ Border に別に関連付ける必要があります。

論理パーティション ポリシーの適用

ユーザの操作によって新しいコール レッグが作成された場合（たとえば、ユーザが第 3 の発信者を既存のコールに参加させる場合）、Unified CM は各参加者ペアのジオロケーション ID と事前に設定されたポリシーのジオロケーション ID を照合します。

（注）　2 つのデバイスのジオロケーション ID が論理パーティションによって評価されている場合、両方のデバイスのデバイス タイプが Interior であれば、ポリシーは適用されません。つまり、同じクラスタ内の IP 電話間のコール、会議、転送などが論理パーティション ポリシーによって拒否されることはありません。

たとえば、インドのバンガロールにある電話機 A と B、およびカナダのオタワにあるゲートウェイ C について考えます。電話機 A から電話機 B にコールします。いずれのデバイスのタイプも Interior であるため、ポリシーは呼び出されません。コールが確立され、次に電話機 A のユーザが会議を起動し、それによってゲートウェイ C が引き込まれます。処理が許可される前に、Unified CM は A と C のジオロケーション ID、および B と C のジオロケーション ID をチェックして、事前に設定されたポリシーとの照合を行います。ポリシーの一致によって処理が拒否された場合、新しいコール レッグは確立できません。

（注）　Unified CM のデフォルト ポリシーは拒否です。つまり、コール レッグを許可するように明示的にポリシーを設定していなければ、コール レッグは拒否されます。

この例では、バンガロールの Interior デバイスがオタワの Border デバイスに接続できるように明示的にポリシーを設定していない限り、コール レッグは拒否されます。

H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング

H.323 プロトコルを使用する Cisco IOS ルータ上でのコール ルーティング ロジックは、ダイヤル ピア コンストラクトに依存しています。ダイヤル ピアは、静的ルートに似たものです。コールの発信地点と終端地点、およびコールがネットワークで通過するパスを定義しています。ダイヤル ピアは、コールの発信元と宛先のエンドポイントを指定するため、およびコール接続の各コール レッグに適用される特性を定義するために使用します。ダイヤル ピアに含まれている属性によって、ダイヤルされるどの番号をルータが収集し、テレフォニー デバイスに転送するかが決まります。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

ダイヤル ピアを使用したコール ルーティングを理解するための鍵の 1 つは、着信コール レッグと発信コール レッグ、つまり着信ダイヤル ピアと発信ダイヤル ピアという概念です。Cisco IOS ルータを経由する各コールは、2 つのコール レッグを持っていると見なされます。1 つはルータに入るもので、1 つはルータから出るものです。ルータに入るコール レッグが *着信コール レッグ*であり、ルータから出るコール レッグが *発信コール レッグ*です。

コール レッグには、主に次の 2 つのタイプがあります。

- ルータを公衆網、アナログ電話機、または PBX に接続する、従来の TDM テレフォニー コール レッグ
- ルータを他のゲートウェイ、ゲートキーパー、または Unified CM に接続する、IP コール レッグ

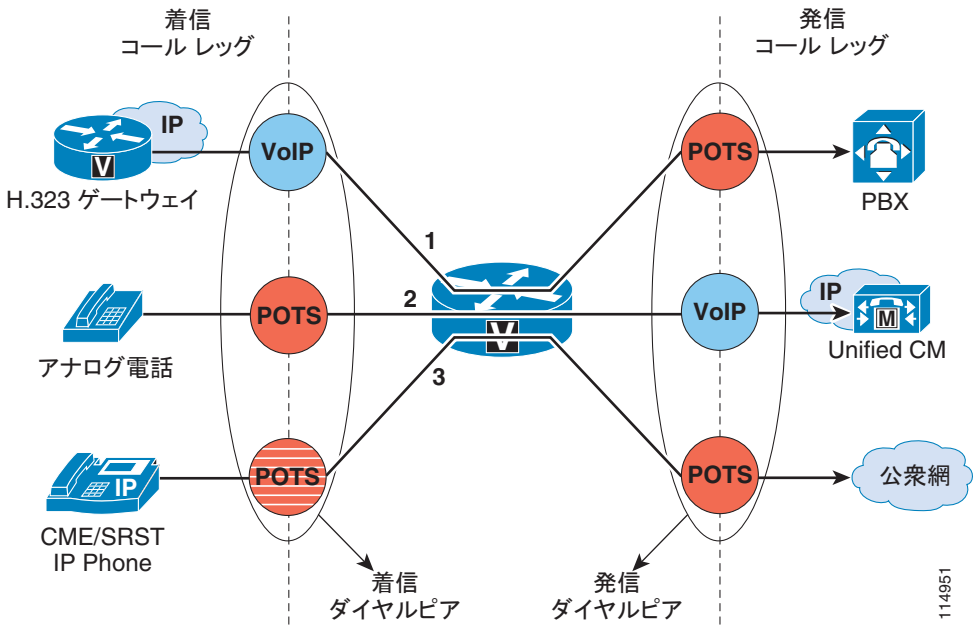
Cisco IOS は、ルータを通過するすべてのコールについて、1 つのダイヤル ピアを各コール レッグに関連付けます。ダイヤル ピアにも、関連付け先となるコール レッグのタイプに応じて、次に示す主に 2 つのタイプがあります。

- 従来の TDM テレフォニー コール レッグに関連付けられる、POTS ダイヤル ピア
- IP コール レッグに関連付けられる、VoIP ダイヤル ピア

図 9-42 では、Cisco IOS ルータを通過する、次の各種コールの例を示しています。

- コール 1 は、IP ネットワークにある別の H.323 ゲートウェイから、ルータに接続されている従来の（たとえば、PRI インターフェイス経由の）PBX までです。このコールに対しては、着信 VoIP ダイヤル ピアと発信 POTS ダイヤル ピアが選択されます。
- コール 2 は、ルータの FXS ポートに接続されているアナログ電話機から、IP ネットワークにある Unified CM クラスタまでです。このコールに対しては、着信 POTS ダイヤル ピアと発信 VoIP ダイヤル ピアがルータによって選択されます。
- コール 3 は、Cisco Unified Communications Manager Express（Unified CME）または SRST の制御する IP Phone から、ルータ上の公衆網インターフェイス（たとえば、PRI インターフェイス）までです。このコールに対しては、自動生成の POTS ダイヤル ピア（ルータ上に設定されている **ephone** に対応します）と発信 POTS ダイヤル ピアが選択されます。

図 9-42　着信ダイヤル ピアと発信ダイヤル ピア



着信コール レッグを着信ダイヤル ピアと対応付けるために、ルータは、セットアップ メッセージ内の情報要素（着信番号/DNIS と発信番号/ANI）が 4 つの設定可能ダイヤル ピア属性と一致するかどうか調べることによって、ダイヤル ピアを選択します。ルータは、これらの項目が一致するかどうかを次の順序で調べます。

1. 着信番号と **incoming called-number**
2. 発信番号と **answer-address**
3. 着信番号と **destination-pattern**
4. 着信音声ポートと設定済み音声ポート

ルータで必要となるのは、これらの条件のいずれか 1 つのみ一致することです。すべての属性をダイヤル ピア内に設定する必要はなく、すべての属性がコール セットアップ情報に一致している必要はありません。ルータがダイヤル ピアを選択するために必要な条件は 1 つのみです。ルータは、1 つのダイヤル ピアが一致するとすぐに検索を停止し、コールは設定済みのダイヤル ピア属性に従ってルーティングされます。一致するダイヤル ピアが他にある場合でも、最初に一致したピアのみが使用されます。

ルータが発信ダイヤル ピアを選択する方法は、着信 POTS ダイヤル ピアに **direct-inward-dial**（DID）が設定されているかどうかによって異なります。

- 着信 POTS ダイヤル ピアに DID が設定されていない場合、ルータは 2 ステージ ダイヤリングを実行し、着信ダイヤル ストリングを 1 桁ずつ収集します。1 つのダイヤル ピアが宛先パターンに一致すると、ルータは一致したダイヤル ピアの設定済み属性を使用して、コールをただちに発信します。
- 着信 POTS ダイヤル ピアに DID が設定されている場合、ルータは着信番号全体を使用して、発信ダイヤル ピアに含まれている宛先パターンに一致するかどうかを調べます。DID を使用する場合は、コールのルーティングに必要な番号がセットアップ メッセージにすべて含まれているため、番号をそれ以上収集する必要がありません。複数のダイヤル ピアがダイヤル ストリングに一致した場合、一致するすべてのダイヤル ピアが*ハント グループ*の形成に使用されます。ルータは、発信コール レッグを確立できるまで、ハント グループに含まれているすべてのダイヤル ピアを使用して確立を試行します。

デフォルトでは、ハント グループ内のダイヤル ピアは、次の基準を使用して、この順序に従って選択されます。

1. 電話番号の最長一致

   この方法では、ダイヤルされた番号と一致している部分が最も長い宛先パターンが選択されます。たとえば、あるダイヤル ピアがダイヤル ストリング 345.... を使用して設定され、別のダイヤル ピアが 3456789 を使用して設定されている場合、ルータはまず 3456789 を選択します。2 つのダイヤル ピアのうち、正確に一致している部分が最も長いためです。

2. 明示的プリファレンス

   この方法では、**preference** ダイヤル ピア コマンドで設定した優先順位を使用します。プリファレンスの数値が小さくなるほど、優先順位が高くなります。最高の優先順位は、プリファレンス順位 0 のダイヤル ピアに与えられます。同じ宛先パターンを持つ複数のダイヤル ピアに対して同じ優先順位が定義されている場合、ダイヤル ピアはランダムに選択されます。

3. ランダム選択

   この方法では、すべての宛先パターンが同等の重みになります。

このデフォルト選択順序を変更することも、**dial-peer hunt** グローバル コンフィギュレーション コマンドを使用して、別のダイヤル ピア ハンティング方法を選択することもできます。この他の選択基準は、*最長待機時間*です。最後に選択された時点から、最も長く待機している宛先パターンを選択します（Unified CM 回線グループの*最長アイドル時間*に相当します）。

Cisco IOS ルータ上で H.323 ダイヤル ピアを設定するときは、次のベスト プラクティスに従ってください。

- 着信公衆網コールが DNIS 情報に基づいて宛先に直接ルーティングされるようにするには、**direct-inward-dial** 属性を使用して、次のようにデフォルト POTS ダイヤル ピアを作成します。

```
dial-peer voice 999 pots
  incoming called-number .
  direct-inward-dial
  port 1/0:23
```

- ルータを Unified CM クラスタに接続されている H.323 ゲートウェイとして使用する場合は、同じ宛先パターンを持ち、2 つの異なる Unified CM サーバを指す VoIP ダイヤル ピアを少なくとも 2 つ設定して、冗長性を実装します。プライマリとセカンダリの Unified CM サーバ間での優先順位を選択するには、**preference** 属性を使用します。次に **preference** 属性の使用例を示します。

```
dial-peer voice 100 voip
 preference 1

!--- Make this the first choice dial peer.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.2

!--- This is the address of the primary Unified CM.

 dtmf-relay h245-alpha


dial-peer voice 101 voip
 preference 2

!--- This  is the second choice.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.3

!--- This is the address of the secondary Unified CM.

 dtmf-relay h245-alpha
```

ゲートキーパーを使用する Cisco IOS でのコール ルーティング

H.323 ゲートキーパーは、H.323 ネットワークにあるエンドポイント（Cisco Unified Communications Manager Express（Unified CME）および Unified CM クラスタ）、H.323 端末、ゲートウェイ、マルチポイント コントロール ユニット（MCU）など）を管理するためのオプション ノードであり、それらのエンドポイントにコール ルーティング機能とコール アドミッション制御機能を提供します。エンドポイントは、H.323 Registration Admission Status（RAS）プロトコルを使用してゲートキーパーと通信します。

エンドポイントは、起動するとゲートキーパーへの登録を試行します。他のエンドポイントとの通信が必要な場合は、E.164 アドレスや電子メール アドレスなど、自身のシンボリック エイリアスを使用して、コールを開始するための許可を要求します。ゲートキーパーは、そのコールを許可してもよいと判断した場合、宛先の IP アドレスを発信元エンドポイントに返します。この IP アドレスは、宛先エンドポイントの実際の IP アドレスではなく、中継アドレスである場合もあります。たとえば、Cisco Unified Border Element や、コール シグナリングをルーティングするゲートキーパーのアドレスです。

H.323 プロトコル、および H.323 エンドポイントとゲートキーパーとのメッセージ交換の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com

Cisco 2600、3600、3700、2800、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール ルーティング機能を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、「ゲートキーパーの冗長性」（P.8-47）を参照してください。コール アドミッション制御に関する考慮事項については、「Cisco IOS ゲートキーパー ゾーン」（P.11-15）を参照してください。

Cisco IOS ゲートキーパーのコール ルーティングは、次のタイプの情報に基づいています。

- 静的に設定されている情報（ゾーン プレフィックスや、デフォルト テクノロジー プレフィックスなど）
- 動的な情報（登録フェーズで H.323 デバイスが提供した E.164 アドレスやテクノロジー プレフィックスなど）
- コールごとの情報（着信番号やテクノロジー プレフィックスなど）

ゾーンは、エンドポイント、ゲートウェイ、MCU などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。

H.323 エンドポイントがゲートキーパーに登録すると、エンドポイントはゾーンに割り当てられます。また、処理できるコールの種類（音声、ビデオ、ファクスなど）を指定するテクノロジー プレフィックスとともに、処理を担当している 1 つまたはそれ以上の E.164 アドレスを登録することもできます。

ゾーンごとに、ゲートキーパー上で 1 つまたはそれ以上の *ゾーン プレフィックス*を設定できます。ゾーン プレフィックスは、番号とワイルドカードを含んだストリングであり、ゲートキーパーがコール ルーティングの判断に使用します。ゾーン プレフィックス ストリングでは、次の文字を使用できます。

- 0 ～ 9 までのすべての数字。それぞれが特定の 1 桁に対応
- ドット（.）ワイルドカード。いずれかの 1 桁の 0 ～ 9 までの数字に対応
- * ワイルドカード。1 またはそれ以上の桁の 0 ～ 9 までの数字に対応

ゲートキーパーのコール ルーティング動作を理解するには、メッセージ解析ロジックについて考えると役立ちます。図 9-43 では、Admission Request（ARQ; アドミッション要求）の解析ロジックを示しています。エンドポイントは、コールを初期化するために、Admission Request（ARQ; アドミッション要求）をゲートキーパーに送信します。ARQ には、宛先つまり着信側の H.323 ID または E.164 アドレスのどちらか、および送信元つまり発信側の E.164 アドレスまたは H.323 ID が含まれています。

ARQ に E.164 アドレスが入っている（Unified CM では、ARQ には常に E.164 アドレスが入っています）場合、ARQ にはテクノロジー プレフィックスが含まれている場合と、含まれていない場合があります。ARQ にテクノロジー プレフィックスが含まれている場合、ゲートキーパーはテクノロジー プレフィックスを着信番号から削除します。ARQ にテクノロジー プレフィックスが含まれていない場合、ゲートキーパーは、デフォルトのテクノロジー プレフィックスが設定されていれば、それを使用します（「集中型ゲートキーパー設定」（P.9-132）の項の **gw-type-prefix** コマンドを参照）。このように取得したテクノロジー プレフィックスは、メモリに格納され、ゲートキーパーはコール ルーティング アルゴリズムに基づく処理を続行します。

次に、ゲートキーパーは、着信番号が設定済みのいずれかのゾーン プレフィックスに一致しないかどうかを調べます。一致する可能性のあるエントリが複数ある場合は、一致する部分の最も長いものが使用されます。一致するゾーン プレフィックスがない場合、未知のプレフィックスを持つコールを受け付けるようにゲートキーパーが設定されているときは、ゲートキーパーは宛先ゾーンが発信元ゾーンと同じであると想定します。

この時点で、ゲートキーパーは選択された宛先ゾーン内を検索して、着信番号に一致する登録済み E.164 アドレスがあるかどうかを調べます。一致が見つかると、コールに関して要求した帯域幅が使用可能になっていて、着信側エンドポイントがゲートキーパーに登録されている場合、ゲートキーパーは Admission Confirm（ACF; アドミッション確認）を送信します。ACF には、宛先エンドポイントの IP アドレスが入っています。帯域幅が使用不能であるか、着信側エンドポイントが登録されない場合、ゲートキーパーは、発信側エンドポイントに Admission Reject（ARJ; アドミッション拒否）を戻します。

一致する E.164 アドレスが宛先ゾーン内に登録されていない場合、ゲートキーパーは、以前に格納したテクノロジー プレフィックスを使用して、そのゾーンに登録されているゲートウェイをコールの宛先として選択します。ゲートキーパーが ACF または ARJ のどちらを発信元エンドポイントに送信するかは、帯域幅の可用性とエンドポイントの登録に関する、上と同じ考慮事項に基づいて決まります。

送信元エンドポイントは、ゲートキーパーから ACF を受信した後、ACF で戻された IP アドレスを使用して、直接セットアップ メッセージを宛先エンドポイントに送信できます。

図 9-43　　ARQ のゲートキーパー アドレス解決

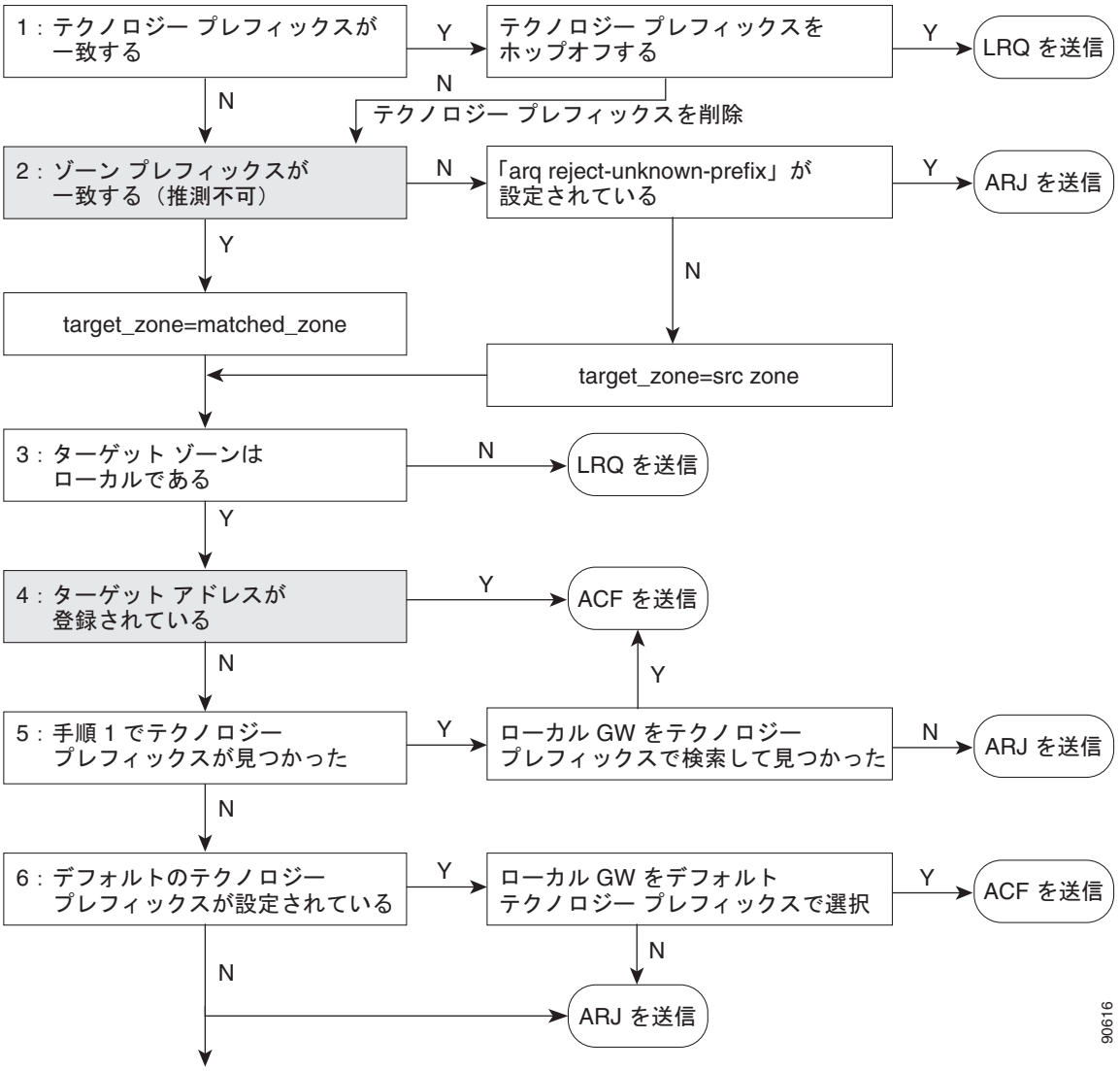
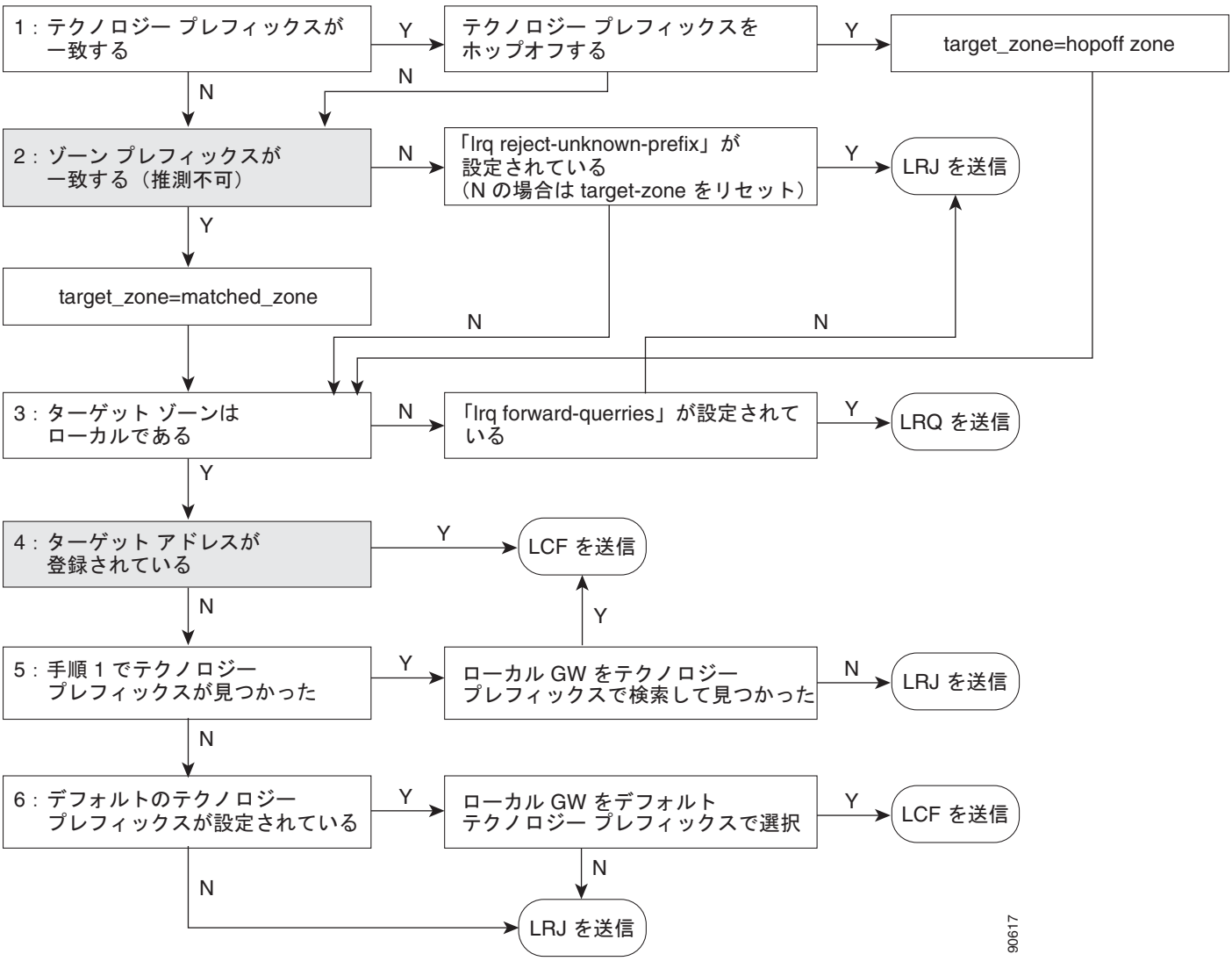


図 9-44 では、Location Request（LRQ; ロケーション要求）の解析ロジックを示しています。LRQ メッセージは、ゲートキーパー間で交換され、ゾーン（リモート ゾーン）間のコールに使用されます。たとえば、ゲートキーパー A が ARQ をローカル ゾーンのゲートウェイから受信し、その ARQ は、リモート ゾーンのデバイスに対するコール アドミッションを要求しているとします。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー B は、自身がゾーン間コール要求を許可するように設定されているかどうか、および要求されたリソースが登録されているかどうかに応じて、この LRQ メッセージに Location Confirm（LCF; ロケーション確認）メッセージまたは Location Reject（LRJ; ロケーション拒否）メッセージで応答します。

図 9-44　　LRQ のゲートキーパー アドレス解決



従来の Cisco IOS ゲートキーパー機能は、*中継ゾーン ゲートキーパー*という概念を通じて、Cisco Unified Border Element に対応するように拡張されました。

中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のクラスタおよび機能はそのまま使用できます。レガシー ゲートキーパーは、着信する LRQ を着信番

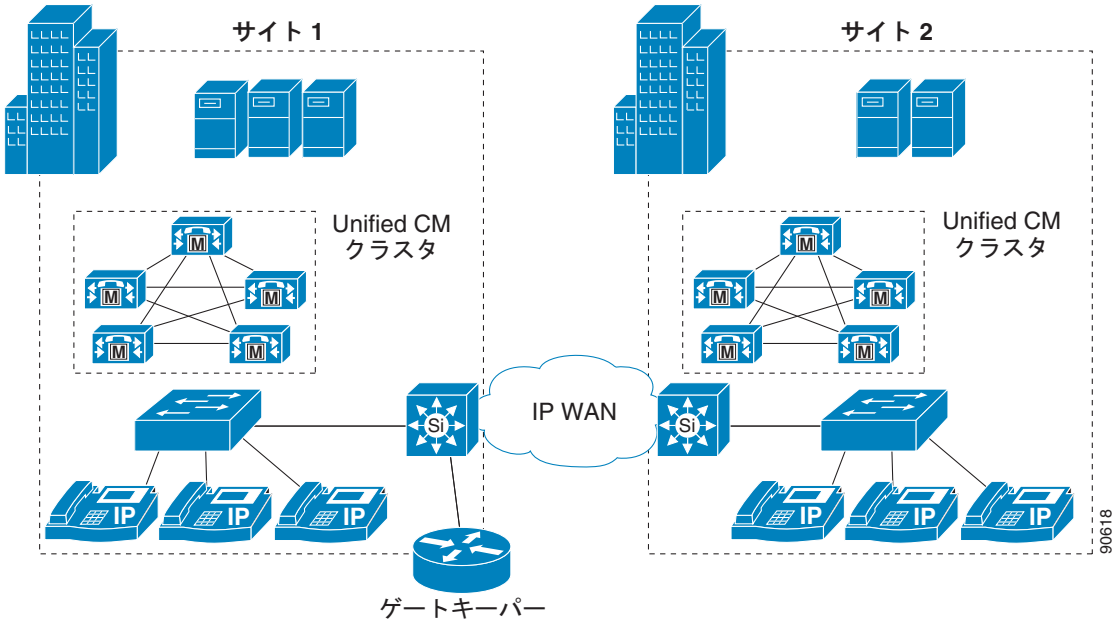
号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれていることを確認します。設定にこれらのいずれかのキーワードが含まれている場合、ゲートキーパーは中継処理をします。含まれていない場合は、従来の処理をします。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの Cisco Unified Border Element を参照している ACF が返され、コールは Cisco Unified Border Element に転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求（LRQ）をリモート ゾーンのゲートキーパーではなく **outvia** ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

集中型ゲートキーパー設定

単一のゲートキーパーは、クラスタ間のコール ルーティング、および最大 100 の Unified CM クラスタに対するコール アドミッション制御をサポートできます。図 9-45 では、2 つの Unified CM クラスタと単一の集中型ゲートキーパーを備えた分散型コール処理環境を示しています。

図 9-45　　2 つのクラスタをサポートする集中型ゲートキーパー



例 9-5 では、図 9-45 のゲートキーパー設定を示しています。

例 9-5　　集中型ゲートキーパーの設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone GK-Site1 160
```

```
bandwidth interzone GK-Site2 160
gw-type-prefix 1#* default-technology
arq reject-unknown-prefix
no shutdown
```

ここでは、図 9-45 について説明します。

- Unified CM トランク登録をサポートするために、各 Unified CM クラスタにはローカル ゾーンが設定されます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することを推奨します。**bandwidth total** コマンドを使用すると、設定内容によっては問題が発生することがあるためです。帯域幅はキロビット/秒（kbps）単位で測定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。

  テクノロジー プレフィックスは、発信されているコールのタイプを示しています。テクノロジー プレフィックスとして使用される個々の値は任意のものであり、ネットワーク管理者が定義します。配置全体で常に同じ値を使用する必要があります。

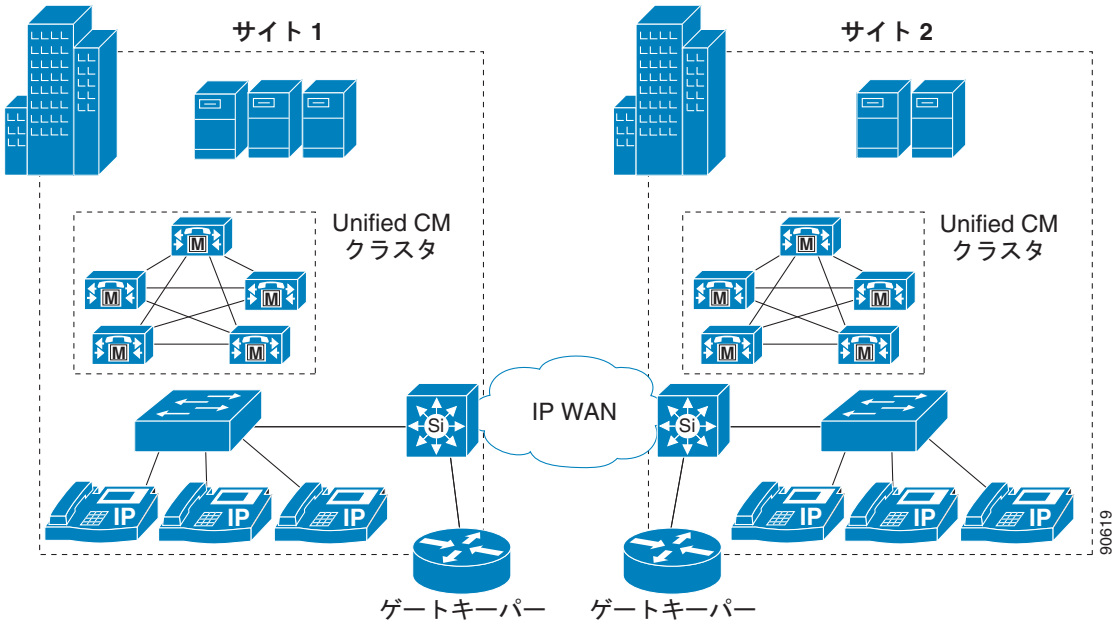
  テクノロジー プレフィックスは、E.164 アドレス（電話番号）のプレフィックスとして送信され、コールが音声であるか、ビデオであるか、その他のタイプであるかを示します。# シンボルは、一般に、プレフィックスと E.164 番号を区別するために使用します。プレフィックスが含まれていない場合、コールのルーティングにはデフォルトのテクノロジー プレフィックスが使用されます。配置全体で 1 つのデフォルト テクノロジー プレフィックスだけが使用される場合があります。

  Cisco IOS ゲートウェイは、プレフィックスが設定されていれば、自動的に発信コールにテクノロジー プレフィックスを追加します。ゲートウェイは、自動的に着信 H.323 コールからプレフィックスを除去します。Unified CM は、ゲートキーパー制御 H.323 トランクの設定ページで指定されているテクノロジー プレフィックスを使用して、ゲートキーパーに登録できます。ただし、このテクノロジー プレフィックスは、ゲートキーパーに向かう発信コールに自動的に追加されることはありません。また、Unified CM に向かう着信コールから自動的に除去されることもありません。トランスレーション パターンとゲートウェイ コンフィギュレーションを使用して着信番号を操作すると、テクノロジー プレフィックスを必要に応じて追加または除去できます。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

分散型ゲートキーパー設定

帯域幅を節約するため、または WAN 障害時に H.323 ゲートウェイにローカル コール ルーティングをサポートするために、ゲートキーパーを分散させることができます。図 9-46 は、2 つのクラスタと 2 つのゲートキーパーを備えた分散型コール処理環境を示しています。

図 9-46　　2 つのクラスタをサポートする分散型ゲートキーパー



例 9-6 では、図 9-46 のサイト 1 に対するゲートキーパー設定を示しています。

例 9-6　　サイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 9-6 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 2 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。

- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

例 9-7 は、図 9-46 のサイト 2 に対するゲートキーパー設定を示しています。

例 9-7　サイト 2 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site2 customer.com 10.1.11.100
 zone remote GK-Site1 customer.com 10.1.10.100
 zone prefix GK-Site2 212.......
 zone prefix GK-Site1 408.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 9-7 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 1 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

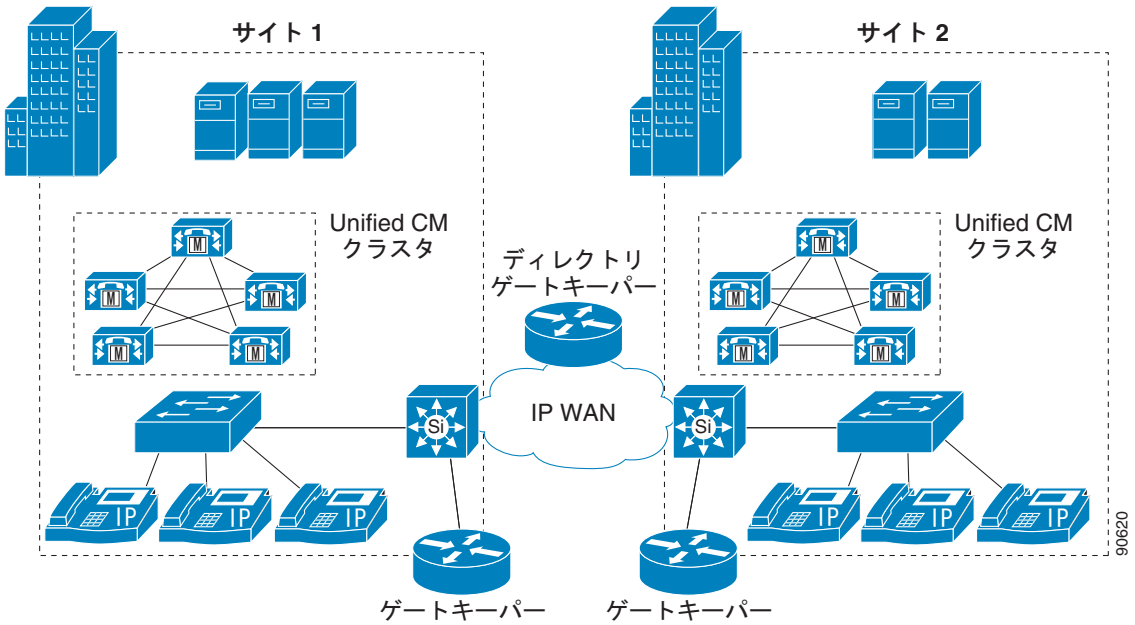
ディレクトリ ゲートキーパーを使用した分散型ゲートキーパー設定

ゲートキーパー ルーティング テーブルを更新するために使用できるゲートキーパー プロトコルがないので、ディレクトリ ゲートキーパーを使用すると、分散型ゲートキーパー設定のスケーラビリティとマネージャビリティの向上に役立ちます。ディレクトリ ゲートキーパーを実装すると、各サイトのゲートキーパー設定が簡単になり、ゾーン間通信の大部分の設定をディレクトリ ゲートキーパーでできるようになります。

ディレクトリ ゲートキーパーがない場合、ゲートキーパーに新しいゾーンを追加するたびに、ネットワーク上のすべてのゲートキーパーに項目を追加する必要があります。しかし、ディレクトリ ゲートキーパーを使用すると、ローカル ゲートキーパーとディレクトリ ゲートキーパーのみで新しいゾーンを追加できます。ローカル ゲートキーパーは、コール要求をローカル側で解決できない場合、ゾーン プレフィックスが一致するディレクトリ ゲートキーパーにその要求を転送します。

図 9-47 では、ローカル コール ルーティング用の分散型ゲートキーパー、およびゲートキーパー間のコール ルーティングをサポートするディレクトリ ゲートキーパーを備えた、Unified CM 分散型コール処理環境を示しています。

図 9-47　ディレクトリ ゲートキーパーを備えた分散ゲートキーパー



例 9-8 では、図 9-47 のサイト 1 に対するゲートキーパー設定を示しています。この例では、サイト 1 とサイト 2 のゲートキーパー設定がほぼ同じなので、ここでは、サイト 1 だけについて説明します。

例 9-8　ディレクトリ ゲートキーパーを使用したサイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote DGK customer.com 10.1.10.101
 zone prefix GK-Site1 408.......
 zone prefix DGK ..........
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 9-8 について説明します。

- ローカル Unified CM クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパー用にリモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ディレクトリ ゲートキーパーのゾーン プレフィックスは、10 個のドットを使用して設定されます。このパターンは、未解決の任意の 10 桁のダイヤル ストリングと一致します。1 つのゾーンに複数のゾーン プレフィックスを設定して、異なる長さのダイヤル ストリングを一致させることができます。ディレクトリ ゲートキーパーのゾーン プレフィックスにもワイルドカード（*）を使用できますが、この方法はコール ルーティングの問題が発生する場合があります。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Unified CM トランクは、1# プレフィックスに登録されるように設定されています。

- **arq reject-unknown-prefix** コマンドは、冗長 Unified CM トランク上にできるコール ルーティング ループを回避します。

例 9-9 では、図 9-47 の例のディレクトリ ゲートキーパー設定を示しています。

例 9-9　　ディレクトリ ゲートキーパー設定

```
gatekeeper
 zone local DGK customer.com 10.1.10.101
 zone remote GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408*
 zone prefix GK-Site2 212*
 lrq forward-queries
 no shutdown
```

ここでは、例 9-9 について説明します。

- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。設定を簡単にするために、ゾーン プレフィックスでワイルドカード（*）が使用されます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスが必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

H.323 ダイヤル ピアを使用する Cisco IOS のコール特権

H.323 を使用する Cisco IOS ベースのシステム（H.323 ゲートウェイ、SRST、および Cisco Unified Communications Manager Express（Unified CME）を含む）にコール特権を実装するには、制限クラス（COR）機能を使用します。この機能は、ネットワークの設計に柔軟性をもたらし、管理者は、すべてのユーザに関して任意のコールをブロックできるようになります（たとえば、米国では 900 番号へのコール）。また、個々の発信者のコール試行に対して、それぞれ別のコール特権を適用できます（一部のユーザには国際通話を許可し、他のユーザには許可しない、など）。

COR 機能の中心となる基本的メカニズムは、着信と発信の *COR リスト*を定義することで成立しています。このリストは既存のダイヤル ピアに関連付けるもので、着信および発信という概念は、Cisco IOS ルータに対してのものです（ダイヤル ピアの場合と同様）。各 COR リストは、メンバーの番号を含めることで定義します。この番号は、Cisco IOS 内に定義済みの単純なタグです。

コールがルータを通過するときには、Cisco IOS ダイヤル ピア ルーティング ロジックに基づいて、着信ダイヤル ピアと発信ダイヤル ピアが選択されます。選択されたダイヤル ピアに COR リストが関連付けられている場合は、コールをルーティングする前に、さらに次のチェックが実行されます。

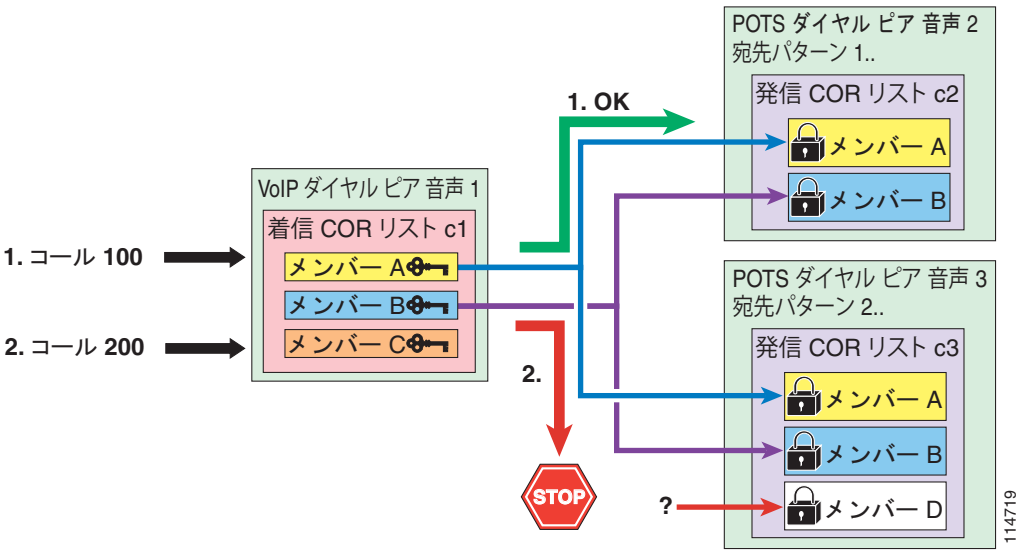
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットである場合、コールは許可されます。
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットでは*ない*場合、コールは拒否されます。

COR リスト ステートメントが一切適用されていないダイヤル ピアが存在する場合は、次のプロパティが適用されます。

- ダイヤル ピア上に着信 COR リストが設定されていない場合は、デフォルトの着信 COR リストが使用されます。デフォルト着信 COR リストは最高の優先順位を持っているため、発信 COR リストの内容にかかわらず、このダイヤル ピアは他のすべてのダイヤル ピアにアクセスできます。
- ダイヤル ピア上に発信 COR リストが設定されていない場合は、デフォルトの発信 COR リストが使用されます。デフォルト発信 COR リストは優先順位が最も低いため、着信 COR リストの内容にかかわらず、他のすべてのダイヤル ピアがこのダイヤル ピアにアクセスできます。

この動作の内容を最もよく表しているのが、図 9-48 に示す例です。この例では、1 つの VoIP ダイヤル ピアと 2 つの POTS ダイヤル ピアが定義されています。

図 9-48　　COR の動作の例



この VoIP ダイヤル ピアは、メンバー A、B、C を持つ着信 COR リスト c1 に関連付けられています。着信 COR リストのメンバーは、「鍵」だと考えることができます。

最初の POTS ダイヤル ピアは、宛先パターン 1.. を持っており、メンバー A と B を持つ発信 COR リスト c2 に関連付けられています。2 番めの POTS ダイヤル ピアは、宛先パターン 2.. を持っており、メンバー A、B、D を持つ発信 COR リスト c3 に関連付けられています。発信 COR リストのメンバーは、「錠」だと考えることができます。

コールが成功するには、発信ダイヤル ピアの発信 COR リストにあるすべての「錠」を開けるための「鍵」を、着信ダイヤル ピアの着信 COR リストがすべて持っている必要があります。

図 9-48 に示した例では、宛先が 100 になっている最初の VoIP コールがルータに受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが最初の POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c2 発信 COR リストの錠（A と B）に必要な鍵をすべて持っているため、コールは成功します。

次に、宛先が 200 になっている別の VoIP コールがルータで受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが 2 番めの POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c3 発信 COR リスト（D）に必要な「鍵」を 1 つ持っていないため、コールは拒否されます。

Cisco IOS で COR 機能を設定するには、次の手順に従います。

ステップ 1　コマンド **dial-peer cor custom** を使用して、COR リスト メンバーとして使用される「タグ」を定義します。

ステップ 2　コマンド **dial-peer cor list** *corlist-name* を使用して、COR リストを定義します。

ステップ 3　COR リストを既存の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けます。このためには、ダイヤル ピアの設定で、コマンド **corlist** {**incoming** | **outgoing**} *corlist-name* を使用します。

Cisco IOS Release 12.2(8)T 以降では、COR 機能を SRST 制御の IP Phone に適用できます。IP Phone は、SRST ルータに対して動的に登録を実行します。このため、SRST では、IP Phone が Cisco Unified CM クラスタへの接続を失うときまで、個々の IP Phone について事前には一切把握していません。したがって、COR 機能の SRST 用の設定は、電話機の DN に基づいています。SRST ルータに登録するとき、IP Phone は自身の DN をルータに通知して、SRST ルータが IP Phone を適切な COR リストに割り当てられるようにします。

SRST によって制御される IP Phone のための COR を設定するには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* {*corlist-number starting-number – ending-number* | **default**} を **call-manager-fallback** コンフィギュレーション モードで使用します。

このコマンドには、次の制限事項があります。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

COR 機能は、Cisco IOS Release 12.2(8)T 以降を使用する Cisco Unified Communications Manager Express（Unified CME）にも配置できます。個々の IP Phone は、Unified CME で具体的に設定されます。したがって、COR リストを IP Phone 自体に直接適用できます。このためには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* を各 IP Phone の **ephone-dn** *dn-tag* コンフィギュレーション モードで使用します。

これらの概念を実際に適用する方法の例については、「H.323 を使用している Cisco IOS でのサービス クラスの構築」（P.9-67）の項を参照してください。

Cisco SRST と Cisco Unified CallManager Express の設定の詳細については、次の Web サイトで入手可能な『*Cisco SRST System Administrator Guide*』および『*Cisco Unified Communications Manager Express System Administrator Guide*』を参照してください。

http://www.cisco.com

H.323 ダイヤル ピアを使用する Cisco IOS での番号操作

H.323 を実行している Cisco IOS ルータでは、番号操作は音声トランスレーション プロファイルを通じて実行されます。このプロファイルは、音声コールの発信番号（ANI）または着信番号（DNIS）の番号を操作するために、またはコールの番号タイプを変更するために使用されるものです。

音声トランスレーション プロファイルは、Cisco IOS Release 12.2(11)T 以降で使用できます。このプロファイルは、コールが着信ダイヤル ピアに対応付けられる前、またはコールが発信ダイヤル ピアによって転送される前に、電話番号を別の番号に変換するために使用します。たとえば、社内で 5 桁の内線番号をダイヤルすると、別のサイトにいる従業員に到達できるとします。コールが他のサイトに公衆

網を通じてルーティングされ、到達する場合は、発信側のゲートウェイで音声トランスレーション プロファイルを使用する必要があります。これによって、5 桁の内線番号が公衆網で認識される 10 桁の形式に変換されます。

音声トランスレーション プロファイルを設定するには、**voice translation-rule** および **voice translation-profile** Cisco IOS コマンドを使用します。これらのコマンドでは、変換の対象となる番号ストリングを正規表現を使用して定義します。次に、この操作を発信番号、着信番号、リダイレクト先着信番号のいずれに関連付けるのかを指定します。音声トランスレーション プロファイルを定義した後に、次の任意の要素に適用できます。

- 特定の音声ポート上で終端する、すべての着信 POTS コール レッグ
- ルータに入るすべての着信 VoIP コール レッグ
- 特定の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けられている発信コール レッグ
- SRST 制御の IP Phone 上で終端する、すべての着信または発信コール レッグ
- SRST 制御のすべての IP Phone によって発信されるコールのための着信コール レッグ

（注） **voice translation-rule** コマンドを使用する音声トランスレーション プロファイルは、以前に **translation-rule** コマンドで提供されていた機能を置き換え、拡張するものです。この新しいコマンドの構文は、以前のコマンドで使用されていた構文とは異なります。詳細については、http://www.cisco.com で入手可能な『*Cisco IOS Voice Command Reference*』（Release 12.2(11)T 以降）の **voice translation-rule** を参照してください。

音声トランスレーション プロファイルの一般的な用途は、IP WAN が使用不可になっていてルータが SRST モードで動作している場合でも、支店サイトからのオンネット サイト間ダイヤリング手順をそのまま維持できるようにすることです。たとえば、中央サイトが San Jose にあり、3 つのリモート サイトが San Francisco、New York、Dallas にある単純な配置について考えます。表 9-10 では、この例の DID 範囲と内部サイト コードを示しています。

表 9-10　変換ルール応用例の DID 範囲とサイト コード

	San Jose	San Francisco	New York	Dallas
DID 範囲	(408) 555-1XXX	(415) 555-1XXX	(212) 555-1XXX	(972) 555-1XXX
サイト コード	1	2	3	4

サイト間のコールは、オンネット アクセス コード 8 の次に 1 桁のサイト コードと着信側の 4 桁内線番号をダイヤルすることによって、通常は IP WAN 経由で発生します。IP WAN がダウンしていて Cisco SRST がアクティブな場合にも、これらのダイヤリング手順を維持できるようにするには、内部の番号を E.164 番号に再変換してから公衆網に送信する必要があります。次に、San Francisco ルータの設定例を示します。

```
voice translation-rule 1
  rule 1 /^81/ /91408555/
  rule 2 /^83/ /91212555/
  rule 3 /^84/ /91972555/

voice translation-profile on-net-xlate
  translate called 1

call-manager-fallback
  translation-profile outgoing on-net-xlate

dial-peer voice 2 pots
  destination-pattern 91[2-9]..[2-9].....
```

```
port 1/0:0
  direct-inward-dial
  forward-digits 11
```

この設定では、San Francisco サイトが SRST モードになっているときにユーザが 831000 をダイヤルすると、ルータは **voice translation-rule 1** の **rule 2** と一致するものと判定し、着信番号を 912125551000 に変換します。この新しい番号が使用され、発信ダイヤル ピア（**dial-peer voice 2**）と一致するものと判定されます。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

Cisco IOS の正規表現構文の詳細については、次の Web サイトで入手可能な『*Cisco IOS Terminal Services Configuration Guide*』の「*Regular Expressions*」を参照してください。

http://www.cisco.com/en/US/docs/ios/termserv/configuration/guide/tsv_reg_express_ps6441_TSD_Products_Configuration_Guide_Chapter.html

Service Advertisement Framework（SAF）Call Control Discovery（CCD）

この項では、Unified CM および関連する Unified Communications サブシステムにおける Service Advertisement Framework（SAF）コール制御ディスカバリ（CCD）サービス設定に関して、いくつかの点に重点を置いて説明します。このテーマの詳細については、「Service Advertisement Framework のコール制御ディスカバリを使用したコール ルーティングおよびダイヤル プラン配信」（P.5-66）の項、および次の URL にある最新バージョンの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Unified CM クラスタは、CCD アドバタイザとしてフレームワークに参加することによって、ホストする DN 範囲に関する情報をネットワークに挿入します。この情報は Service Advertisement Framework フォワーダ（SAF フォワーダ）に送信されます。SAF フォワーダは、新しいルートを取得し、それらをネットワーク内の参加している他の SAF フォワーダや CCD リクエスタと共有します。

Unified CM クラスタは、CCD リクエスタとしてフレームワークに参加することによって、ネットワーク内の他のコール エージェントによってアドバタイズされた DN 範囲を SAF フォワーダから取得します。

SAF フォワーダ

SAF フォワーダは Cisco IOS ルータに設定します。SAF フォワーダには Cisco IOS Release 15.0(1) 以降が必要です。SAF フォワーダの設定の詳細については、次の URL にある『*Cisco IOS Service Advertisement Framework Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html

SAF フォワーダの設定

Unified CM では、SAF セキュリティ プロファイル（[Advanced Features] > [SAF] > [SAF Security Profile]）および SAF フォワーダ（[Advanced Features] > [SAF] > [SAF Forwarder]）の両方を設定する必要があります。

Unified CM の [SAF Security Profile] 設定ページには、[User Name] フィールドと [User Password] フィールドがあります。これらのエントリは、Cisco IOS Command Line Interface（CLI; コマンドライン インターフェイス）での SAF フォワーダ設定と一致する必要があります。

また、[SAF Forwarder] 設定ページで設定された [Unified CM Client Label] は、SAF フォワーダの CLI 設定の external-client 文のいずれかと一致する必要があります。次の例を参考にしてください。

```
  service-family ipv4 autonomous-system 1
  !
  topology base
   external-client sample_client_label
  exit-sf-topology
 exit-service-family
!

service-family external-client listen ipv4 5050
 external-client sample_client_label
  username sample_user_name
  password sample_user_password
  keepalive 10000
!
```

詳細については、次の URL にある『*Cisco IOS Service Advertisement Framework Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html

要求サービス

SAF CCD から取得された DN 範囲は、要求元クラスタの専用の CCD コール ルーティング パーティションに設定されます。取得された DN 範囲は、1 つ以上の CCD トランクに関連付けられています。CCD から取得された DN 範囲へのコールは、要求サービスに関連付けられた CCD トランクから発信されます。CCD トランクと要求サービスの関連付けは、Unified CM の [Call Routing] > [Call Control Discovery] > [Requesting Service] にある [CCD Requesting Service Info] ページの [Selected SAF Trunks] フィールドで行います。

クラスタと SAF フォワーダとの間で交換される CCD レコードには、DN 範囲、DN 範囲をホストするコール エージェント ノードの IP アドレス、コールを公衆網に再ルーティングするときに DN を適合させるための番号操作ルール、およびこの DN 範囲をコールするために必要な IP シグナリング プロトコルに関する情報が含まれています。

たとえば、クラスタ A には DN 範囲 8555XXXX がホストされ、公衆網における対応する DID 範囲は +1415555XXXX であるとします。この DN 範囲の IP コールの受信に指定された CCD トランクに関連付けられているクラスタ A サブスクライバの IP アドレスは 10.1.1.1 です。この DN 範囲に到達するために必要なプロトコルは SIP です。この場合、この DN 範囲に関連付けられた CCD レコードは、次のように表すことができます。

DN 範囲	ToDID	IP	プロトコル
8555XXXX	1:+1415	10.1.1.1	SIP

- DN 範囲

  ユーザが 85551234 にダイヤルすると、8555XXXX に一致し、85551234 へのコールはこのパターンをアドバタイズしたクラスタに発信されます。

- ToDID

  このフィールドは、公衆網経由で DN 範囲に到達するためのルールを表しています。ユーザが 85551234 にダイヤルし、コールが CCD トランク経由でルーティングできない場合、ToDID ルールが適用されて、宛先番号が公衆網に互換性がある形式に変換されます。たとえば、範囲 8555XXXX にルール 1:+1415 が適用されると、左端の 1 桁が削除されて、+1415 が先頭に付加されます。その結果 +14155551234 という番号が生成されます。この番号を使用すると、次の場合に発信側クラスタ内の任意のゲートウェイにコールをルーティングできます。+E.164 形式でコールをルーティングするようにプロビジョニングされており、グローバルな +E.164 形式の番号を公衆網キャリアで受け付けられるローカル形式に適合させるための適切な着信側トランスフォーメーション パターンでゲートウェイがプロビジョニングされている場合です。

- IP

  宛先 DN をホストするコール エージェント ノードの IP アドレスは、発信側クラスタ内で関連する CCD トランク経由でコールを発信する場合に使用されます。

- プロトコル

  この場合、DN 範囲をホストするコール エージェントによってアドバタイズされるプロトコルは SIP です。H.323 が使用されることもあります。

特定のクラスタでどのような SAF CCD レコードが検出されたかを表示するには、Cisco Unified CM Real-Time Monitoring Tool（RTMT）を使用します。このツールでは、検出された DN 範囲、および SAF フォワーダとクラスタとの関連付けに関する情報が提供されます。

Unified CMBE 3000 のダイヤル プランに関する考慮事項

Cisco Unified Communications Manager Business Edition（CMBE）3000 では、ドロワー ユーザ インターフェイス（GUI）とともに非常に単純化されたフロント エンドが提供されます。サイト プロファイルや使用プロファイルなどの新しいコンセプトが導入されました。回線/デバイス アプローチとコーリング サーチ スペースを使用するダイヤル プランの基本的なコンセプトは同じですが、Unified CMBE 3000 ではサイトとプロファイルのコンセプトを使用してダイヤル プランが実装されます。次のように、デバイス レベルのコール特権はサイトによって定義され、回線レベルのコール特権に対する制限は使用プロファイルによって定義されます。

- サイト

  サイトは、電話機、ユーザ、ゲートウェイなどを含むエンドポイントの地理的なグループを表します。サイトには特権が与えられ、そのサイトの各ユーザが使用できるコール特権の最大レベルが定義されます。これは、各ユーザがこれらの特権を持つのではなく、特権がコールを発信する各ロケーションの機能を制御することを意味します。たとえば、国際番号をダイヤルするコール特権を持つロケーションがあるとしても、これは必ずしもこのサイトの各ユーザが国際コールを発信できることを意味しません。

- 使用プロファイル

  使用プロファイルを使用すると、システム管理者は電話機のほとんどのユーザ設定を一箇所で行うことができます。管理者は、既存の使用プロファイルを編集したり、既存の使用プロファイルを複製して新しいプロファイルを作成したり、完全に新しい使用プロファイルを追加したりできます。各使用プロファイルは一意の名前を持ちます。使用プロファイルの設定後に、システム管理者は使用プロファイルをユーザまたは配置に割り当て、ユーザ プロファイルの設定を個々のユーザまたは全体の部門に属する電話機に適用できます。

使用プロファイルでは、割り込みや Cisco Extension Mobility などの電話機機能、電話機ハードウェア機能、電話機に表示できる電話機アプリケーション、電話機に表示されるボタンと機能ボタンの順序を制御する電話機ボタン テンプレートなどのユーザのコール特権を設定できます。

（注）　Cisco Unified Communications Manager Business Edition 3000 は、最大 10 個の使用プロファイルをサポートします。

サイト特権と使用コール特権の組み合わせにより、ユーザが番号をダイヤルする実際の機能が定義されます。たとえば、サイトにはコールの最大レベルとして国際コールをダイヤルする特権を割り当てることができます。この場合、ユーザは国際コール、長距離コール、およびローカル コールを含む任意の番号をダイヤルできます。ただし、ユーザが、ダイヤル特権をローカル コールだけに制限する使用プロファイルに割り当てられている場合、サイトが国際コールをダイヤルする特権を持っていても、そのユーザはローカル コールだけをダイヤルできます。

別の例として、ユーザが、国際コールをダイヤルするコール特権を持つ使用プロファイルとサイトに割り当てられているとします。このユーザが、サイト レベル特権がローカル コールへのダイヤルだけに制限された別のサイトに移動した場合、このユーザはローカル コール以外にダイヤルすることはできません。これは、現在のサイト レベル コール特権により許可されないためです。

実際には、サイト レベル コール特権と使用プロファイル コール特権を下げることによって、ユーザのコール特権が決まります。

変換ルール

変換ルールにより、Cisco Unified CMBE 3000 はシステムの一部である着信電話番号を操作し、コールのルーティング前に内線に変換できます。システムに着信したコールと IP 電話機により生成されたコールは設定された変換ルールに基づいて照合され、番号が一致すると、変換が実行されます。

（注）　Unified CMBE 3000 では、変換ルールでのワイルド カードの使用はサポートされていません。

論理パーティション

各電話機は、電話機で設定された IP アドレスに基づいてサイトに関連付けられます。各サイトは 1 つまたは複数のサブネットにマップされます。電話機の IP アドレスがこれらいずれかのサブネット内に存在する場合、電話機はサブネットがマップされたサイトに属します。電話機がシステム定義されていない IP アドレスを取得した場合は、電話機は中央サイトの一部であると見なされます。ただし、テレワーカー サイトが設定されている場合は、設定された IP アドレスが設定されたいずれかのサブネット内に存在しない電話機がテレワーカー電話機と見なされます。

設定されたサイトは論理パーティションをサポートします。サイトの設定時に、管理者は PSTN 特権を設定する必要があります。中央サイト PSTN へのアクセスが設定されていない場合、リモート サイトのユーザは PSTN コール レグが関係する会話に参加できません。また、リモート サイト電話機は PSTN コールを開始することができません。

CHAPTER 10

緊急サービス

音声システムを適切に配置するには、緊急サービスが非常に重要です。この章では、緊急コールの計画に不可欠な次の主要な設計上の考慮事項について説明します。

この章では、カナダおよび米国で配置されている 911 緊急ネットワークに固有の情報について説明します。ここで説明する概念の多くは、他の地域にも適応できます。緊急コール機能の適切な実装については、ローカル テレフォニー ネットワーク プロバイダーにご相談ください。

米国の一部の州では、Multi-Line Telephone System（MLTS）のユーザに必要な 911 機能を対象にした法律がすでに制定されています。また、National Emergency Number Association（NENA）が『*NENA Technical Requirements Document on Model Legislation E9-1-1 for Multi-Line Telephone Systems*』を制作しています。これは、次のサイトからオンラインで入手できます。

http://www.nena.org/

さらに、Federal Communications Commission（FCC; 米国連邦通信委員会）も、タイトル 47、パート 68、セクション 319 に対して新しいセクション案を作成しました。これは、次のサイトで入手可能です。

http://www.apcointl.org/about/pbx/worddocs/mltspart68.doc

この章は、北米在住の公衆網ユーザに使用可能な汎用 911 機能について十分に理解している読者を対象にしています。このテーマの詳細については、次の URL にある NENA Web サイトを参照してください。

http://www.nena.org/

この章の新規情報

表 10-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 10-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
911 緊急サービスのアーキテクチャ コンポーネント	「911 緊急サービスのアーキテクチャ」（P.10-2）	2011 年 3 月 31 日
Cisco Emergency Responder のキャパシティ プランニング	「Cisco ER クラスタリングのキャパシティ プランニング」（P.10-9）	2011 年 3 月 31 日
Cisco Emergency Responder のハイ アベイラビリティ要件	「緊急サービスのハイ アベイラビリティ」（P.10-9）	2011 年 3 月 31 日
Cisco Emergency Responder を WAN で配置する場合の要件	「Cisco Emergency Responder の WAN 配置」（P.10-22）	2011 年 3 月 31 日

911 緊急サービスのアーキテクチャ

この項では、Multi-Line Telephone Systems（MLTS）における緊急コールの機能要件の一部について説明します。ここでの緊急コールとは、北米の Public Switched Telephone Network（PSTN; 公衆電話交換網）によって提供される 911 コールのことです。

緊急サービスのアーキテクチャは、通常次の要素から構成されます。

- 緊急事態にある発信者は、固定回線、携帯電話機、または音声コールを行うことができる任意のデバイスから緊急サービスをダイヤルできる必要があります。
- 緊急サービス コール ハンドラが緊急要求に応答し、警察、消防、医療などの必要なサービスを派遣できる必要があります。
- コール ハンドラは、支援を提供するために緊急事態にある発信者のロケーションを特定できる必要があります。
- 発信者のロケーションに最も近い緊急サービス コール ハンドラにコールをルーティングするには、緊急サービス ネットワークが必要です。

次の項では、911 緊急サービス アーキテクチャの重要なアーキテクチャ コンポーネントのいくつかについて説明します。

Public Safety Answering Point（PSAP）

Public Safety Answering Point（PSAP）は、911 コールに応答して、適切な緊急対応（警察、消防署、救急チームの派遣など）を手配する機関です。911 コールを発信する電話機の物理的なロケーションは、そのコールに応答する適切な PSAP を決定する基本要素です。一般に、各建物を、1 つのローカル PSAP が担当します。

所定のロケーションを担当する PSAP を確認するには、地域の防火管理者や警察署などの地域の公衆安全情報サービス機関に問い合せてください。また、通常、地域通信事業者のディレクトリにも、所定地域内の 911 コールを処理する機関がリストされています。

標準的な状況

- 1 つの番地に対して、1 つの PSAP だけが指定されます。
- 1 つの番地の 911 コールはすべて、同じ PSAP にルーティングされます。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP の管轄になります。
- 一部の 911 コールをオンネット ロケーション（キャンパスのセキュリティ、建物のセキュリティ）にルーティングする必要があります。

選択ルータ

選択ルータは、発信者の地理的な場所と Automatic Number Identification（ANI; 自動番号識別）に基づいたコール送信のために適切な PSAP を決定する緊急サービス ネットワークのノードです。通常、Local Exchange Carrier（LEC; 地域通信事業者）が選択ルータを稼動します。したがって、発信者がそのロケーションに基づいて適切な選択ルータにルーティングされるようエンタープライズ IP テレフォニー ネットワークが設計されている必要があります。

自動ロケーション識別データベース

発信者のロケーション情報は、911 サービス インフラストラクチャの重要な部分です。Automatic Location Identifier（ALI; 自動ロケーション識別）データベースには LEC により提供された特定の地理的なロケーションに関する情報が保持されます。各 911 コールに対して、PSAP は ALI データベースを検索し、発信番号の ANI に基づいて発信者のロケーションを取得します。ALI データベースでは、アドレスが Master Street Address Guide（MSAG）形式で保存されます。ALI データベースは、ローカル緊急サービス管理側の代わりに、契約を締結したサード パーティ（通常は現在の Local Exchange Carrier（LEC; 地域通信事業者））によって保守されます。

Private Switch ALI

Private Switch ALI（PS/ALI）は、MLTS オペレータが各テレフォニー エンドポイントに詳細なアドレスとロケーション情報を提供できるようにする 911 緊急応答システムの拡張機能です。このサービスにより、顧客が生成したアドレス テーブルを ALI データベースにロードできるようになります。この結果、MLTS システムの各ステーションの電話番号から 911 にコールされた場合に、MLTS システムの各ステーションを一意に識別できるようになります。スイッチング システムにより生成されたステーション固有またはロケーション固有の Automatic Number Identification（ANI; 自動番号識別）は、発信者の正確なロケーションを特定するために直接 E911 システムに渡すことができます。次に、PSAP オペレータは、正確な住所、建物、階、部屋、またはパーティションに緊急対応人員を派遣できます。この結果、作業が簡略化され、精度が高まります。

911 ネットワーク サービス プロバイダー

担当 PSAP を確認したあと、各 PSAP が接続されている 911 ネットワーク サービス プロバイダーも特定する必要があります。通常、PSAP は公衆網から 911 コールを受信すると想定されますが、実際はそうではありません。実際は、911 コールは、地域の重要な専用ネットワークを経由して伝送され、各 PSAP は 1 つ以上のこうした地域ネットワークに接続されます。大半の場合、既存の Local Exchange Carrier（LEC; 地域通信事業者）が PSAP の 911 ネットワーク サービス プロバイダーです。例外として、軍事施設、大学構内、国立や州立の公園、または公衆安全の責任が地方自治体の管轄外であるロケーション、もしくは公共の地域通信事業者以外のエンティティによってプライベート ネットワークが運営されているロケーションがあります。

所定の PSAP の 911 ネットワーク サービス プロバイダーについて疑問がある場合は、その PSAP に直接連絡して、情報を確認してください。

標準的な状況

- 所定の番地に対する 911 ネットワーク サービス プロバイダーは、既存の Local Exchange Carrier（LEC; 地域通信事業者）です。電話会社 X がサービスを提供するロケーションの場合、対応する PSAP も、電話会社 X からサービスが提供されます。
- すべての 911 コールは、オフネット ロケーションに直接ルーティングされるか、オンネット ロケーションに直接ルーティングされます。

例外的な状況

- MLTS インターフェイスから公衆網へ接続するために使用する Local Exchange Carrier（LEC; 地域通信事業者）と、PSAP に対して 911 ネットワーク サービス プロバイダーの役目をする LEC が*異なる*場合があります（たとえば、電話システムは電話会社 X からサービスを受け、PSAP は電話会社 Y に接続されている場合です）。この状況では、LEC 間の特別な調整、または電話システムと PSAP の 911 ネットワーク サービス プロバイダー間に特別な専用トランクが必要な場合があります。
- 一部の LEC は、ネットワーク上で 911 コールを受け入れることができません。この場合、LEC を変更するか、911 コールを適切な PSAP にルーティングできる LEC に接続されたトランク（911 コール ルーティング専用）を確立するかの 2 つのオプションしかありません。
- 一部（または全部）の 911 コールをオンネット ロケーション（キャンパスのセキュリティや建物のセキュリティなど）にルーティングする必要があります。各電話機の 911 コールの宛先が正しく計画され、文書化されていれば、この状況には、設計および実装の段階で簡単に対応できます。

適切な 911 ネットワークへのインターフェイス ポイント

大規模なテレフォニー システムでは、911 接続に多数のインターフェイス ポイントが必要になる場合があります。一般に、複数の E911 選択ルータが LEC の管轄地区内で使用されます。これらのルータは、通常、相互接続*されません*。

たとえば、大規模なキャンパスを備えた企業に、次のような状況があるとします。

- 建物 A は San Francisco にある。
- 建物 B は San Jose にある。
- San Francisco 警察と San Jose 警察が、該当する PSAP である。
- San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーのサービスを利用している。
- しかし、San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーが運営する異なる E911 選択ルータのサービスを受けている。

このタイプの状況では、2 つの別々のインターフェイス ポイント（E911 選択ルータごとに 1 つずつ）が必要です。E911 選択ルータの管轄地区に関する情報は、一般に、担当 LEC が保持しています。また、その LEC の地域アカウント担当者が、企業カスタマーに関連情報を提供できる必要があります。多くの LEC は、911 問題を担当する専門家のサービスも用意しています。この専門家は、911 アクセス サービスの適切なマッピングについてアカウント担当者と協議できます。

標準的な状況

- 単一サイト配置またはキャンパス配置では、通常、911 コール用に 1 つだけの PSAP があります。
- 1 つの PSAP だけへのアクセスが必要であれば、必要なインターフェイス ポイントは 1 つだけです。複数の PSAP へのアクセスが必要な場合でも、同じ集中インターフェイスを介して、同じ E911 選択ルータから到達可能です。集中型コール処理で企業の支店サイトが WAN を介して接続されており、Survivable Remote Site Telephony（SRST）操作がアクティブであるときに WAN 障害が発生した場合の 911 分離を防止するため、911 へのローカル（つまり、各支店内の）アクセスを各ロケーションに指定することを推奨します。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP 管轄になります。*また、*
- 一部の 911 コールは、異なるインターフェイス ポイントを通じて、異なる E911 選択ルータにルーティングされる必要があります。

（注） PSAP と E911 選択ルータの地理的な管轄地区の設定に必要な情報は、オンライン、または各種の Competitive Local Exchange Carrier（CLEC; 競争的地域通信事業者）の Web サイトから部分的に情報を入手できます（たとえば、https://clec.att.com/clec/hb/shell.cfm?section=782 には、California および Nevada の AT&T がカバーする管轄地区についての貴重なデータが提供されています）。しかし、911 コール ルーティングを設計および実装する前に、該当するインターフェイス ポイントの適切な情報を LEC から入手しておくことを強く推奨します。

インターフェイス タイプ

ネットワークへの 911 コールの発信に使用されるインターフェイスは、音声通信の提供に加えて、発信側についての識別データも提供する必要があります。

Automatic Number Identification（ANI; 自動番号識別）は、ネットワークが適切な宛先へ 911 コールをルーティングするために使用する、発信側の北米番号計画の番号を参照します。この番号は、PSAP がコールの Automatic Location Identification（ALI; 自動ロケーション識別）を検索するためにも使用されます。

911 コールは、ソースルートされます。つまり、911 コールは発信番号に応じてルーティングされます。別々のロケーションからすべて同じ番号（911）をダイヤルする場合でも、ANI によって表される起点ロケーションに基づいて、別々の PSAP に到達します。

911 コール機能は、次のいずれかのインターフェイス タイプを使用して実装できます。

- 動的 ANI 割り当て
- 静的 ANI 割り当て

動的 ANI 割り当ては、（複数の ANI をサポートするので）スケーラビリティに優れていますが、小規模のシステム配置には適していません。これに対し、静的 ANI 割り当ては、最小のシステムから最大のシステムまで、より広範囲にわたる環境で使用できます。

動的 ANI（トランク接続）

動的 ANI では、システムの 1 つのインターフェイスを、911 ネットワークにアクセスする多数の電話機が共用します。また、ネットワークに送信される ANI がコールごとに異なっていることが必要な場合があります。

動的 ANI インターフェイスには、次の 2 つの主なタイプがあります。

- Integrated Services Digital Network Primary Rate Interface（ISDN-PRI、または単に PRI）
- Centralized Automatic Message Accounting（CAMA）

PRI

このタイプのインターフェイスは、通常、テレフォニー システムを公衆網 Class 5 スイッチに接続します。Calling Party Number（CPN; 発番号）は、発信側の E.164 番号を識別するためにコールのセットアップ時に使用されます。

911 にコールする場合、LEC によって CPN を扱う方法が異なります。Class 5 スイッチ機能の制限、または LEC や地方自治体の方針によっては、CPN が 911 コール ルーティング用の ANI として使用されない場合があります。この場合、CPN の代わりに Listed Directory Number（LDN）または Bill-To Number（BTN; 請求先番号）を ANI の目的で使用するように、ネットワークをプログラムできます。

CPN が ANI に使用されない場合、PRI インターフェイスから発信する 911 コールはすべて、911 ネットワークには同じように見えます。これらの 911 コールはすべて、同じ ANI を持ち、同じ宛先（適切な宛先でない場合があります）にルーティングされるためです。

一部の LEC は、911 コールの CPN が PRI インターフェイスを通過するようにする機能を備えています。この機能を使用すると、コールのセットアップ時に Class 5 スイッチに提示された CPN は、コールをルーティングするために ANI として使用されます。この機能の名称は、LEC によって異なります（たとえば、SBC は California でこの機能を Inform 911 と呼びます）。

（注） CPN は、ルーティング可能な北米番号計画の番号である*必要があります*。つまり、CPN は、関連した E911 選択ルータのルーティング データベースに入力されている必要があります。

（注） Direct Inward Dial（DID; ダイヤルイン方式）の電話機の場合、DID 番号は、911 の目的で ANI として使用できますが、これは、911 サービス プロバイダーのネットワーク内で、緊急サービス番号に適切に関連付けられている場合だけです。DID 以外の電話機の場合は、別の番号を使用してください（詳細については、「緊急ロケーション識別番号のマッピング」（P.10-11）を参照してください）。

多くの Class 5 スイッチは、複数のエリア コードをサポートしないトランクを通じて、E911 選択ルータに接続されています。このような場合、PRI が 911 コールの伝送に使用されるとき、Class 5 スイッチと同じ Numbering Plan Area（NPA; 番号計画エリア）のある CPN（または ANI）を持つ 911 コールだけが、適切にルーティングされます。

例

MLTS が、エリア コード 514（NPA = 514）の Class 5 スイッチに接続されるとします。MLTS が PRI トランク上で 911 コールを送信し、CPN が **450**.555.1212 である場合、Class 5 スイッチは、（正しい **450**.555.1212 ではなく）ANI **514**.555.1212 として E911 選択ルータにそのコールを送信するため、不適切なルーティングと ALI ルックアップが発生します。

PRI を 911 インターフェイスとして適切に使用するには、システムの設計担当者が、CPN が ANI に使用されることを確認し、リンク上で受け入れ可能な番号の範囲（NPA NXX TNTN の形式）を適切に指定する必要があります。たとえば、PRI リンクが、範囲 514 XXX XXXX 内の ANI 番号を受け入れるように指定されている場合、NPA = 514 の発番号を持つコールだけが適切にルーティングされます。

CAMA

Centralized Automatic Message Accounting（CAMA）トランクも、MLTS がコールを 911 ネットワークに送信することを可能にします。PRI 方式との相違点は、次のとおりです。

- CAMA トランクは、E911 選択ルータに直接接続されます。E911 選択ルータと MLTS ゲートウェイ ポイント間の距離をカバーするために、マイレージ追加料金が適用される場合があります。
- CAMA トランクは、911 コールだけをサポートします。CAMA トランクの設置と操作に関連した資産コストと運営コストは、911 トラフィックのサポートだけに使用されます。
- MLTS 業界の CAMA トランクは、固定エリア コードに制限されることがあります。このエリア コードは、一般に、リンク プロトコルで暗黙的に示されます（つまり、明示的に送信されません）。接続には、すべてのコールが同じ固定エリア コードを共用するため、7 桁または 8 桁だけが ANI として送信されます。

静的 ANI（回線接続）

静的 ANI は、公衆網との回線（トランクではなく）接続をサポートし、発信側の電話機の CPN に関係なく、回線の ANI が、その回線で発信されるすべての 911 コールに関連付けられます。Plain Old Telephone Service（POTS; 一般電話サービス）回線が、この目的に使用されます。

POTS 回線は、最も単純で、かつ広くサポートされている公衆網インターフェイスの 1 つです。POTS 回線は、通常、911 コールを受け入れるように設定されています。さらに、既存の E911 インフラストラクチャは、POTS 回線からの 911 コールを適切にサポートします。

POTS には、次の特徴があります。

- POTS 回線に関連する運用コストが低くなります。
- POTS 回線に、電源障害に備えたバックアップ回線の役割を持たせることができます。
- POTS 回線番号を、ALI データベースに入力されるコールバック番号として使用できます。
- POTS 回線は、公衆網へのローカル PRI、または CAMA アクセスに見合うユーザ密度を持たないロケーションに対して、最低コストで最適な 911 サポートを実現します。
- 公衆網の敷設に伴い、POTS 回線は広く普及しています。

このタイプのインターフェイスを介した 911 発信コールはすべて、E911 ネットワークによって同じものとして扱われます。ANI は単なる POTS 回線番号の可能性があるため、E911 ネットワークに提示される ANI を Cisco Unified Communications Manager が制御できるようにするツール（たとえば、発信者番号トランスフォーメーション マスクなど）は、無関係です。

Cisco Emergency Responder

IP テレフォニー テクノロジーの主な利点の 1 つは、移動、追加、および変更の管理が容易であることです。ユーザが介入することなく自動的に 911 情報を更新する移動、追加、および変更をサポートするために、シスコは Cisco Emergency Responder（Cisco ER）と呼ばれる製品を開発しました。

Cisco ER は、次の主な機能を備えています。

- 検出された電話機の物理ロケーションに基づいて、電話機を Emergency Response Location（ERL; 緊急応答ロケーション）に動的に関連付けます。
- コールバックのために Emergency Location Identification Number（ELIN; 緊急ロケーション識別番号）を発信側電話機に動的に関連付けます。上記の項で説明されている ER 以外のシナリオと異なり、Cisco ER は、911 コールを発信した電話機にコールバックできるようにします。
- 緊急コールが進行中であることを知らせるために、指定された通話者へのオンサイト通知が可能です（ポケットベル、Web ページ、または電話を使用）。ポケットベルと Web ページによる通知には、発信者の名前と電話番号、ERL、およびそのコールに関連した日時の詳細が含まれます。電話による通知では、緊急コールの発信番号に関する情報が提供されます。

ERL と ELIN の詳細については、「緊急応答ロケーションのマッピング」（P.10-10）と「緊急ロケーション識別番号のマッピング」（P.10-11）を参照してください。Cisco ER の詳細については、「Cisco Emergency Responder の設計に関する考慮事項」（P.10-15）と、次の Web サイトで入手可能な Cisco ER 製品のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

Cisco ER の主な機能は、電話機が 911 コールを発信したネットワーク ポート（ファスト イーサネット スイッチ ポートなどのレイヤ 2 ポート）の検出による、電話機のロケーションの検出に依存します。この検出メカニズムは、主に次の 2 つの前提事項に依存します。

- 企業の有線インフラストラクチャが十分に確立され、散発的な変更が行われないこと。
- Cisco ER が、このインフラストラクチャをブラウズできること。つまり、Cisco ER は、敷設されたネットワーク インフラストラクチャとの Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）セッションを確立でき、接続された電話機を検出するためにネットワーク ポートをスキャンできること。

Cisco ER はコールの発信ポートを検出すると、そのコールを、そのポートのロケーション用として事前に確立された ERL に関連付けます。このプロセスは、ロケーションに事前に確立された ELIN との関連付けと、発信 ERL に基づく、E911 インフラストラクチャの適切な出口点の選択も行います。

また、Cisco ER は、IP サブネットに対して ERL を設定し、IP アドレス別に IP 電話機のロケーションを割り当てる機能を提供します。この機能は、接続されたスイッチ ポートで Cisco ER が見つけることができない、Cisco Unified CM に登録されたワイヤレス IP 電話機、IP ソフトフォン、およびサードパーティの SIP 電話機を見つけるために使用できます。また、この機能は、有線のシスコ製 IP 電話機に対して接続されたスイッチ ポート ロケーションの代わりに使用したり、これらのスイッチ ポート ロケーションに追加して使用したりできます。IP 電話機に対して接続されたスイッチ ポートと IP サブネット ロケーションの両方が利用可能である場合、Cisco ER は接続されたスイッチ ポートを優先して利用します。これは、接続されたスイッチ ポートは通常 IP サブネット ロケーションよりも具体的であるためです。接続されたスイッチ ポートの検出で遅延やエラーが発生した場合であっても適切な ERL が割り当てられるように、接続されたスイッチ ポートと IP サブネット ロケーションの両方を使用することを推奨します。

Cisco ER では、1 つの ERL に対して 2 つ以上の ELIN を使用できます。この機能拡張の目的は、次の例に示されているように、同じ期間内に 1 つの ERL から複数の 911 コールが発信される特定のケースに対応することです。

例 1

- 電話機 A と電話機 B はどちらも ERL X 内に存在し、ERL X は ELIN X に関連付けられています。
- 電話機 A は 13:00 に 911 にコールします。ELIN X は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、コールを解除します。その後、13:15 に電話機 B が 911 にコールします。再び ELIN X が、コールを PSAP X にルーティングするために使用されます。

- PSAP X は、電話機 B からコールを解除したあと、電話機 A の最初のコールに関連する詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X にダイヤルしますが、（目的の電話機 A ではなく）電話機 B につながります。

この状況を回避するために、Cisco ER では、各 ERL に ELIN のプールを定義できます。このプールにより、後続のコールごとに別個の ELIN をラウンドロビン方式で使用できます。この例で ERL X に対して 2 つの ELIN を定義すると、例 2 で説明する状況になります。

例 2

- 電話機 A と電話機 B はどちらも ERL X 内に存在し、ERL X は ELIN X1 と ELIN X2 の両方に関連付けられています。
- 電話機 A は 13:00 に 911 にコールします。ELIN X1 は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、コールを解除します。その後、13:15 に電話機 B が 911 にコールし、このコールを PSAP X にルーティングするために ELIN X2 が使用されます。
- PSAP X は、電話機 B からコールを解除したあと、電話機 A の最初のコールに関連する詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X1 にダイヤルし、電話機 A につながります。

3 番めの 911 コールが発信されたが ERL に 2 つの ELIN しかない場合、コールバック機能が、最後の 2 人の発信者にしか正しく到達できません。

緊急サービスのハイ アベイラビリティ

最も危機的な状況であってもユーザが緊急サービスを利用できることは非常に重要です。したがって、企業で緊急サービスを配置する場合は、ハイ アベイラビリティの計画を慎重に行う必要があります。

Cisco Emergency Responder は、アクティブ/スタンバイ モードで最大 2 台のサーバを使用するクラスタリングをサポートします。データは、プライマリ Cisco ER サーバとセカンダリ Cisco ER サーバ間で同期されます。プライマリ サーバが利用できない場合にコールがセカンダリ サーバにルーティングされるようにするために、システム管理者は特定のプロビジョニング ガイドラインに従って、CTI ルート ポイントと、Cisco Unified CM でこれらの CTI ルートポイントに関連付けられた DN を設定する必要があります。設定の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

両方の Cisco ER サーバが利用できない場合は、Local Route Group（LRG; ローカル ルート グループ）を使用して適切な ELIN/ERL（Cisco ER が提供したものよりも具体的でない可能性があります）を持つ適切な PSAP にコールをルーティングできます。また、別の方法として、コールを内部セキュリティ オフィスにルーティングして発信者のロケーションを決定できます。いずれの場合であっても、このプロビジョニングは Cisco Unified CM で実行する必要があります。

Cisco ER の冗長性以外に、911 緊急サービスをルーティングし、単一障害点を回避できるように Cisco Unified CM の冗長性とゲートウェイ/トランクの冗長性も考慮する必要があります。

Cisco ER クラスタリングのキャパシティ プランニング

Cisco ER クラスタでは、ホーム Cisco ER グループのトラッキング ドメイン外部でローミングする電話機の数が、スケーラビリティ ファクタとなります。このような電話機の数は、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Network Hardware and Software Requirements*」に記載されている制限内に収める必要があります。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Cisco MCS 7845 サーバ プラットフォームを使用すると、Cisco ER クラスタで最大 3000 台のローミング電話機をサポートできます。この制限を超える必要のある配置（たとえば、複数の Unified CM クラスタを含む大規模なキャンパス配置）では、IP サブネットによって電話機の移動をトラッキングできます。各 Cisco ER グループで IP サブネットを定義し、Cisco ER グループごとに各 ERL を 1 つの ELIN に割り当てることによって、実質的にローミング電話機をなくすことができます。これは、キャンパス内のすべての電話機が、それぞれの Cisco ER グループのトラッキング ドメインに含まれるためです。

適切なサイジングを確実に行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用してください。このツールは、シスコのパートナーと従業員だけが利用できます（http://tools.cisco.com/cucst で適切なログインが必要）。このサイジング ツールにアクセスできない場合は、シスコ アカウント チームまたはパートナー インテグレータと協力してシステムのサイジングを適切に行ってください。

911 緊急サービスの設計に関する考慮事項

Multi-Line Telephone System（MLTS）配置の 911 緊急サービスを計画している場合は、最初に電話サービスが必要なすべての物理ロケーションを確立します。これらのロケーションは、次のように分類できます。

- 単一ビル配置：すべてのユーザは同じ建物に存在しています。
- 単一キャンパス配置：ユーザは近距離にある建物のグループに存在しています。
- マルチサイト配置：ユーザは地理的に広い範囲に分散しており、WAN 接続を介してテレフォニー コール処理サイトにリンクされています。

これらのロケーション（つまり、配置のタイプ）は、911 サービスの設計と実装に使用される基準に影響を与えます。次の各項で、主要な基準を、それぞれの一般的な状況および例外的な状況とともに説明します。これらの基準を分析し、適用する際には、ネットワーク内の電話機ロケーションによって受ける影響を考慮してください。

緊急応答ロケーションのマッピング

NENA は、企業テレフォニー システムで 911 を管理する規則を制定する際に、州および連邦機関が使用すべき法律モデルを提案しています。NENA 提案の概念の 1 つは、次のように定義される Emergency Response Location（ERL; 緊急応答ロケーション）の概念です。

> *911 緊急応答チームの派遣先ロケーション：このロケーションは、緊急応答チームがそのロケーション内で発信者の位置をすばやく確認するための妥当な機会を提供できる、明確なものでなければならない。*

この要件は、各電話機のロケーションを個々に識別するのではなく、電話機を「ゾーン」（ERL）にグループ化することを見込んでいます。ERL の最大サイズは、この法律の地域ごとの実施に応じて異なる可能性がありますが、ここでは説明の基準として 7000 平方フィートを使用します（ここで説明する概念は、任意の州または地域で許可される最大 ERL サイズとは無関係です）。

Emergency Location Identification Number（ELIN; 緊急ロケーション識別番号）が、各 ERL に関連付けられます。ELIN は、E911 ネットワーク内でコールのルーティングに使用される完全修飾 E.164 番号です。関連した ERL から発信するすべての 911 コールで、ELIN が E911 ネットワークに送信されます。このプロセスは、911 の目的で、複数の電話機を同じ完全修飾 E.164 番号に関連付けることを可能にし、DID 電話機と非 DID 電話機にも同様に適用できます。

（注）　このマニュアルは、法律の実際の要件を提示しようとするものではありません。ここで提示する情報や例は、説明だけを目的としています。システムの設計担当者の責任において、適用されるローカル要件を確認してください。

たとえば、ある建物の床面積が 70,000 平方フィートであり、100 台の電話機があるとします。911 機能を計画する際に、この建物を 7000 平方フィートごとの 10 個のゾーン（ERL）に分割し、そこに置かれた各電話機を ERL に関連付けることができます。911 コールが発信されると、関連した ELIN を PSAP に送信することによって、ERL（複数の電話機に対して同一）が識別されます。この例のように、電話機が均等に分散されている場合、10 台の電話機を持つ各グループには、同じ ERL があり、したがって同じ ELIN を持ちます。

各種法律により、最小台数の電話機（たとえば 49）と最低床面積（たとえば、40,000 平方フィート）が定義されます。この数を下回ると、MLTS 911 の要件は適用されません。しかし、法律が企業の 911 機能を要求しない場合であっても、911 機能をプロビジョニングすることが常に最善の方法です。

緊急ロケーション識別番号のマッピング

一般に、Emergency Location Identification Number（ELIN; 緊急ロケーション識別番号）と呼ばれる 1 つの完全修飾 E.164 番号を、各 ERL に関連付ける必要があります（ただし、Cisco Emergency Responder を使用する場合は、ERL ごとに複数の ELIN を設定できます）。ELIN は、E911 インフラストラクチャ全体でコールをルーティングするために使用され、ALI データベースへのインデックスとして PSAP が使用します。

ELIN は次の要件を満たす必要があります。

- ELIN は、E911 インフラストラクチャ全体でルーティング可能である必要があります（「インターフェイス タイプ」（P.10-5）の項の例を参照）。ELIN がルーティング不能である場合、関連した ERL からの 911 コールは、E911 選択ルータでプログラムされたデフォルト ルーティングに応じて処理されます。
- 企業の ERL-to-ELIN マッピングが定義されたあとは、LEC を使用して、対応する ALI レコードを設定する必要があります。その結果、PSAP にサービスを提供する ANI と ALI データベース レコードを正確に更新できます。

ELIN マッピング プロセスは、所定の ERL に対する E911 インフラストラクチャとのインターフェイスのタイプに応じて、次のいずれかを選択できます。

- 動的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は MLTS によって制御されます。MLTS のテレフォニー ルーティング テーブルは、発信側電話機の ERL に基づいて、正しい ELIN をコールに関連付けます。Cisco Unified Communications Manager では、トランスフォーメーション マスクを使用して、911 へのコールの発番号を変更できます。たとえば、所定の ERL 内にあるすべての電話機が、トランスレーション パターン（911）を含み、かつ電話機の CPN をそのロケーションの ELIN に置き換える発信者番号トランスフォーメーション マスクも含むパーティションをリストする同じコーリング サーチ スペースを共有できます。

- 静的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は公衆網によって制御されます。これは、インターフェイスが POTS 回線である場合に該当します。ELIN は POTS 回線の電話番号であり、電話機の発信者識別番号をさらに操作することはできません。

PSAP コールバック

PSAP は、最初の会話の完了後、発信者に到達できることが必要な場合があります。PSAP がコールバックできるかどうかは、PSAP が最初の着信コールとともに受信する情報によって決まります。

この情報は、次の 2 段階のプロセスによって PSAP に送信されます。

1. 最初に、Automatic Number Identification（ANI; 自動番号識別）が PSAP に送信されます。ANI は、コールをルーティングするために使用される E.164 番号です。この説明では、PSAP で受信された ANI は、MLTS が送信した ELIN を指しています。
2. PSAP は ANI を使用して、データベースを照会し、Automatic Location Identification（ALI; 自動ロケーション識別）を取得します。ALI は、次のような情報を PSAP 担当者に知らせます。
   - 発信者名。
   - 住所。
   - 該当する公衆安全機関。
   - コールバック情報を組み込むことができる、その他のオプション情報。たとえば、救援活動の調整に役立てるために、企業のセキュリティ サービスの電話番号がリストされています。

標準的な状況

- ANI 情報が PSAP コールバックに使用されます。ここでは、ELIN がダイヤル可能番号であると想定します。
- ELIN は、MLTS に関連した公衆網番号です。公衆網から ELIN にコールすると、そのコールは、MLTS によって制御されるインターフェイス上で終端します。
- システム内の任意の ELIN に発信されたコールが、関連した ERL のすぐ近くにある電話機（または複数の電話機）を鳴らすように、コール ルーティングをプログラムするのは、MLTS システム管理者の責任です。
- ERL-to-ELIN マッピングが設定されたあと、修正が必要なのは、企業の物理的な状況に変更があった場合だけです。電話機が単に追加、移動、またはシステムから削除された場合、ERL-to-ELIN マッピングと、それに関連する ANI/ALI データベース レコードは変更する必要はありません。

例外的な状況

- 発信 ERL のすぐ近くへのコールバックを、オンサイト緊急デスクへのコールバックのルーティングと組み合せる（または置き換える）ことができます。これは、PSAP が最初の発信者を呼び出し、緊急事態に対してただちに支援を要請するときに役立ちます。
- たとえば、エリア コードの分割、公衆安全業務の新しい配分を必要とする地方自治体業務の変更、新しい建物の追加、または 911 の目的でコールの望ましいルーティングに影響を与えるその他の変更により、企業の状況が変わる場合があります。こうした状況では、企業の ERL-to-ELIN マッピングおよび ANI/ALI データベース レコードの変更が必要です。

ダイヤル プランに関する考慮事項

アクセス コード（たとえば、9 など）を使用するかどうかにかかわらず、システムが緊急コールを認識しやすいようにダイヤル プランを設定することが必要です。北米の緊急ストリングは、通常、911 です。ストリング 911 と 9911 の両方を認識するようにシステムを設定することを強く推奨します。

また、緊急ルート パターンに Urgent Priority のマークを明示的に付けて、Unified CM が、コールのルーティング前に、桁間タイムアウト（Timer T.302）を待機*しない*ようにすることも強く推奨します。

これ以外の緊急コール ストリングを、システム上で並行してサポートできます。テレフォニー システム ユーザには、選択した緊急コール ストリングを想定した訓練を行うことを強く推奨します。

また、ユーザが誤って緊急ストリングをダイヤルした場合に適切な対応ができるように訓練することも必要です。北米では、アクセス コード 9 を使用して長距離番号にアクセスしようとするユーザが、誤って 911 をダイヤルする可能性があります。このような場合、ユーザは、緊急事態ではないため、緊急人員を派遣する必要がないことを確認するために、回線を保持する必要があります。Cisco ER のオンサイト通知機能では、誤って発信されたコールを含め、911 に発信されたすべてのコールの詳細なアカウントを提供することによって、そのような疑わしい 911 コールの起点にある電話機を識別できます。

マルチサイト配置では、ダイヤル プラン設定により、緊急コールがサイトに対してローカルな PSTN ゲートウェイを介して常にルーティングされ、緊急コールが該当する地域で最も近い PSAP にルーティングされるようにする必要があります。これを実現するメカニズムの 1 つとして、Cisco Unified CM のローカル ルート グループ機能を使用することがあります。

また、マルチサイト配置では、緊急番号が、常に到達可能であり、実装された Class of Service（CoS; サービス クラス）に関係なくモビリティ ユーザ（拡張モビリティおよびデバイス モビリティ）のためにローカル PSTN ゲートウェイを介してルーティングされることが非常に重要です。サイト/デバイス方法が使用される場合は、緊急コールをルーティングするためにデバイスの Calling Search Space（CSS; コーリング サーチ スペース）を使用できます。

シスコは、Cisco Emergency Responder で発信側変更を有効にすることを推奨しています。この機能が有効な場合は、発番号が Cisco ER によって緊急コールを表す ELIN で置き換えられます。発信側変更が有効でない場合は、DID が PSAP に送信されます。または、発信側が ELIN で置き換えられるように Cisco Unified CM を設定する必要があります。

（注）　手動で設定された電話機を除いて、Cisco Emergency Responder では E.164 番号がサポートされています。手動で設定された電話機の場合、シスコは Cisco Unified CM 上の電話機を、先頭の「+」がない E.164 番号を使用して設定することを推奨します。

ゲートウェイに関する考慮事項

システムの緊急コールを処理するゲートウェイを選択する際には、次の要素を考慮してください。

- 「ゲートウェイの配置」（P.10-13）
- 「ゲートウェイのブロック」（P.10-14）
- 「応答監視」（P.10-14）
- 「応答監視」（P.10-14）

ゲートウェイの配置

Local Exchange Carrier（LEC; 地域通信事業者）ネットワーク内で、911 コールは、コールの起点に基づいて、ローカル側で有効なインフラストラクチャ上でルーティングされます。サービスを提供する Class 5 スイッチは、ロケーションに関連した PSAP に直接接続されるか、E911 選択ルータに接続されます。この選択ルータ自体は、その地域に有効な PSAP 群に接続されます。

シスコの IP ベースの企業テレフォニー アーキテクチャでは、リモート側に置かれているゲートウェイに、オンネットでコールをルーティングすることが可能です。たとえば、San Francisco に置かれている電話機は、IP ネットワークを介して、San Jose にあるゲートウェイにコールを伝送してから、LEC のネットワークに送信できます。

911 コールの場合、緊急コールが適切なローカル PSAP にルーティングされるように、LEC ネットワークへの出口点を選択することが重要です。上記の例では、San Francisco の電話機からの 911 コールが、San Jose のゲートウェイにルーティングされてしまうと、San Francisco の PSAP に到達できま

せん。これは、そのコールを受信する San Jose の LEC スイッチには、San Francisco PSAP にサービスを提供する E911 選択ルータへのリンクがないためです。さらに、San Jose 地域の 911 インフラストラクチャは、San Francisco の発番号に基づいてコールをルーティングすることができません。

このため、911 コールは、発信側電話機と物理的に同じ場所にあるゲートウェイにルーティングしてください。共通ゲートウェイを使用して、複数のロケーションからの 911 コールを集約できるかどうかは、LEC に問い合せてください。所定の地域の 911 ネットワークが、911 コールに中央ゲートウェイを使用しやすい場合でも、911 コール ルーティングが WAN 障害中の影響を受けないように、発信側電話機と同じ場所にあるゲートウェイを使用することが望ましいことに注意してください。

ゲートウェイのブロック

911 コールが「全トランク使用中」状況にならないようにする必要があります。911 コールを接続する必要がある場合、トランキング リソースの不足により他のタイプのコールがブロックされる場合でも、911 コールは処理可能にしておく必要があります。このような状況に備えて、明示トランク グループを 911 コール専用にできます。

緊急コールを独占的に緊急トランク グループにルーティングするのが、好ましい方法です。もう 1 つの方法は、通常の公衆網コールと同じトランク グループに緊急コールを送信し（インターフェイスが許可する場合）、専用緊急トランク グループへの代替パスを用意するものです。後者の方法では、最大限の柔軟性が得られます。

たとえば、緊急コールを PRI トランク グループに向け、オーバーフロー状態になったときに備えて POTS 回線への代替パス（緊急コール専用に予約済み）を指定できます。代替トランク グループに 2 つの POTS 回線を入れる場合、メインのトランク グループで許可されたすべてのコール以外に、少なくとも 2 つの 911 コールを同時にルーティングできることを保証します。

優先ゲートウェイが使用不能になった場合、代替ゲートウェイが使用されるように、緊急コールを代替番号にオーバーフローできます。たとえば、北米で 911 にダイヤルされたコールは、E.164（911 以外）ローカル緊急番号にオーバーフローできます。この方法は、北米の 911 ネットワーク インフラストラクチャを利用しません（つまり、選択ルーティング、ANI、または ALI サービスを使用しません）。この方法は、該当する公衆安全機関によって受け入れられる場合にかぎり、ネットワーク リソースの不足による緊急コールのブロックを回避する最後の手段としてだけ使用してください。

応答監視

通常の状態では、緊急番号に発信されたコールは、PSAP との接続後、応答監視を返す必要があります。応答監視は、他のコールと同じように、オンネット発信者と、LEC ネットワークへの出口インターフェイスとの間の全二重音声接続をトリガーできます。

一部の北米 LEC では、「無料」コールを行う場合、応答監視が返されないことがあります。これは、一部のフリーダイヤル番号（たとえば、800 番など）にも該当します。例外的な状況では、緊急コールは「無料」コールと見なされるため、PSAP との接続後、応答監視が返されないことがあります。この状況は、911 テスト コールを発信するだけで検出できます。PSAP との接続後、音声が存在する場合、コール タイマーが発信コールの所要時間を記録します。コール タイマーがない場合は、応答監視が返されなかった可能性があります。応答監視が返されない場合、LEC に連絡して、この状況を報告することを強く推奨します。望ましい機能ではない可能性があります。

この状況が Local Exchange Carrier（LEC; 地域通信事業者）によって修正できない場合、LEC ネットワークにコールが発信されるときに応答監視を必要とし*ない*ように出口ゲートウェイを設定することを推奨します。また、応答監視が返されない場合でも、プログレス インジケータ トーン、代行受信メッセージ、および PSAP との通信が可能であるように、両方向で音声をカットスルーすることも推奨します。

デフォルトでは、Cisco IOS ベースの H.323 ゲートウェイは、両方向で音声を接続するために、応答監視を受信する必要があります。これらのゲートウェイ上で応答監視の必要をなくすには、次のコマンドを使用してください。

- **progress_ind alert enable 8**

  このコマンドは、アラートの受信時にプログレス インジケータ 8（インバンド情報が使用可能）を受信することに相当します。このコマンドを使用すると、ゲートウェイの POTS 側が、コールの起点方向の音声を接続できます。

- **voice rtp send-recv**

  このコマンドは、宛先スイッチから Connect メッセージを受信する前に、逆方向と順方向の両方の音声カットスルーを可能にします。このコマンドは、すべての Voice over IP（VoIP）コール（使用可能である場合）に影響を与えます。

応答監視が提供されない場合は、Call Detail Record（CDR; コール詳細レコード）に 911 コールの接続時間または期間が正確に反映されません。その結果、コール レポーティング システムが、911 コール関連の統計情報を正しく表すことができない場合があります。

いかなる場合でも、すべてのコール パスからの 911 コール機能をテストし、PSAP との接続後、応答監視が返されることを確認することを強く推奨します。

Cisco Emergency Responder の設計に関する考慮事項

デバイス モビリティにより、緊急コールに特別な設計上の考慮事項が生じます。Cisco Emergency Responder（Cisco ER）は、デバイスの動的な物理ロケーションに基づいて、デバイス モビリティをトラッキングし、システムによる緊急コールのルーティングを適合させるために使用できます。

コール アドミッション制御ロケーション間のデバイス モビリティ

集中型コール処理配置では、Cisco ER は IP 電話機の移動を検出し、移動した IP 電話機を適切な ERL に自動的に再び割り当てることができます。ただし、移動した電話機に対する Cisco Unified CM のロケーションベースのコール アドミッション制御は、新しいロケーションの電話機の WAN 帯域幅使用量を正しく把握できず、WAN 帯域幅リソースのオーバーサブスクリプションやアンダーサブスクリプションが発生する可能性があります。たとえば、電話機を支店 A から支店 B に物理的に移動したにもかかわらず、電話機のコール アドミッション制御ロケーションが同じままである（たとえば、Location_A など）場合、Location_A に使用可能な帯域幅がすべて他のコールで使用中であれば、その電話機から 911 に発信するコールは、コール アドミッション制御拒否によりブロックされる可能性があります。このようなコールのブロックを回避するために、デバイスのロケーションとリージョン パラメータを使用するよう手動で設定する必要がある場合があります。

Cisco Unified CM デバイス モビリティを使用すると、新しい物理ロケーションを反映するよう Unified CM で電話機の設定（コーリング サーチ スペースとロケーション情報を含む）を自動的に更新できます。デバイス モビリティを使用しない場合は、Cisco Unified CM で手動で設定を変更する必要があることがあります。

デフォルトの緊急応答ロケーション

Cisco ER は、電話機の物理的なロケーションを直接判別できない場合、コールにデフォルトの Emergency Response Location（ERL; 緊急応答ロケーション）を割り当てます。デフォルトの ERL は、こうしたすべてのコールを特定の PSAP に導きます。この状態が発生した場合、コールの送信先について共通の推奨事項はありませんが、通常、中央に置かれ、最大の公衆安全管轄権を提示する PSAP を選択するのが望ましい方法です。また、デフォルト ERL の Emergency Location Identification Numbers（ELIN; 緊急ロケーション識別番号）の ALI レコードに、企業の緊急番号の連絡先情報を取

り込み、発信者のロケーションの不確実性についての情報を提供することも推奨します。さらに、緊急コールのデフォルト ルーティングが発生したというマークを ALI レコードに付けることも推奨します。また、別の方法として、コールを内部セキュリティ オフィスにルーティングして発信者のロケーションを決定できます。

Cisco Emergency Responder および Extension Mobility

Cisco ER は、Cisco Unified CM クラスタ内で Extension Mobility をサポートします。また、両方の Cisco Unified CM クラスタが、共通の Cisco ER サーバまたはグループによってサポートされるか、Cisco ER クラスタとして設定された 2 つの Cisco ER サーバまたはグループによってサポートされる場合、Cisco ER は、Extension Mobility Cross-Cluster（EMCC）もサポートします。いずれの場合でも、Cisco Unified CM クラスタが、911 コールに対する EMCC に関連付けられた付加 Calling Search Space（CSS; コーリング サーチ スペース）を使用するよう設定せず、両方の Cisco Unified CM クラスタですべての 911 コールに対して Cisco ER を使用するよう設定する必要があります。

ソフト クライアント

Cisco IP Communicator などのソフト クライアントが企業内で使用される場合、Cisco ER は、デバイス モビリティをサポートできます。ただし、企業の境界外でソフト クライアントが使用される場合（たとえば、ホーム オフィスやホテルからの VPN アクセスなど）、Cisco ER は、発信者のロケーションを判別できません。さらに、Cisco のシステムで、発信者のロケーションに該当する PSAP にコールを送信できるように、適切な位置にゲートウェイが配置されている可能性はほとんどありません。

ソフト クライアントに 911 コールの使用を許可するか、許可しないかは、企業ポリシーの問題です。インターネット上でローミングする可能性があるソフト クライアントに対して、企業のポリシーとして 911 コールを許可しないことを推奨します。それにもかかわらず、このようなユーザが 911 をコールした場合、ベストエフォート型のシステム応答では、オンサイト保安部隊、またはシステムのメインサイトに近い大規模 PSAP のどちらかに、コールをルーティングします。

次のパラグラフは、ソフト クライアント ユーザに対して緊急コール機能が保証されていないことを警告するために、ユーザに発行される通知の例を示しています。

> *緊急コールは、設定されているサイト（オフィスなど）に設置されている電話機から発信する必要があります。地域保安当局は、設定されたサイトから移動された電話機からの緊急コールには応答しない可能性があります。設定済みのサイトから離れているときに、この電話機を緊急コールに使用する必要がある場合は、応答した公共安全機関に、現在のロケーションに関する具体的な情報を伝えられるように準備してください。旅行または在宅勤務時の緊急コールには、サイトに対してローカル側で設定されている電話機（たとえば、ホテルの電話機や自宅の電話機など）を使用してください。*

また、Cisco ER は Intrado V9-1-1（米国でほとんどすべての PSAP に到達できる緊急コール配信サービス）との統合をサポートします。Cisco ER と Intrado V9-1-1 の組み合わせにより、企業の外部の IP 電話機とソフトフォンは Cisco ER で提供された Web ページを介してロケーションを提供および更新できます。オフプレミス ロケーションからの緊急コールは、発信者のロケーションのために Intrado によって適切な PSAP に配信されます。

テスト コール

企業テレフォニー システムでは、911 コール機能のテストは、初期インストール後だけでなく、予防手段として定期的に実施することを推奨します。

テストを実施する際は、次の推奨事項を参考にしてください。

- PSAP に連絡して、テスト前に許可を要請し、テスト実施者の連絡先情報を伝えます。

- 各コール発信時に、実際の緊急事態 *ではなく*、単なるテストであることを伝えます。
- 通話者の画面上に表示される ANI と ALI を確認します。
- コールがルーティングされた先の PSAP を確認します。
- IP Phone 上のコール所要時間タイマーを調べることによって、応答監視が受信されたことを確認します。アクティブ コール タイマーは、応答監視が正しく機能していることを示します。

共用ディレクトリ番号への PSAP コールバック

Cisco ER は、Emergency Location Identification Numbers（ELIN; 緊急ロケーション識別番号）に対する着信コールのルーティングを処理します。911 コールの発信元の回線が、共用ディレクトリ番号である場合、PSAP コールバックにより、すべての共用ディレクトリ番号アピアランスが鳴ります。その後、共用アピアランスのいずれかがコールに応答できます。これは、911 コールが発信された電話機とはかぎりません。

Cisco Emergency Responder の配置モデル

複数の Unified CM クラスタに基づく企業テレフォニー システムは、Cisco Emergency Responder（Cisco ER）の機能のメリットを受けられます。

ここで使用する用語の詳細、および次の説明を理解するために必要な背景情報については、『*Cisco Emergency Responder Administration Guide*』を参照してください。「*Planning for Cisco Emergency Responder*」の章は特に重要です。このマニュアルは、次の Web サイトで入手できます。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

（注）　Cisco Emergency Responder は、Cisco Unified Communication Manager Express（Unified CME）または Survivable Remote Mode Telephony（SRST）をサポートしません。SRST 配置の場合は、サイト公開番号を使用して 911 コールを PSTN にルーティングするよう適切なダイヤルピアを設定してください。

単一の Cisco ER グループ

単一の Emergency Responder グループを配置して、複数の Unified CM クラスタからの緊急コールを処理できます。この設計の目標は、どの電話機の緊急コールも、その Cisco ER グループにルーティングされるようにすることです。その Cisco ER グループが ELIN を割り当て、電話機のロケーションに基づいてコールを適切なゲートウェイにルーティングします。

単一の Cisco ER グループを使用する 1 つの利点は、すべての ERL と ELIN が単一のシステムに設定されることです。単一の Cisco ER グループがシステムのすべてのアクセス スイッチのポーリングを担当しているため、どのクラスタに登録されている電話機でも、そのグループによって位置が確認されます。図 10-1 は、2 つの Unified CM クラスタとインターフェイスする単一の Cisco ER グループを示しています。

図 10-1　2 つの Unified CM クラスタに接続されている単一の Cisco ER グループ

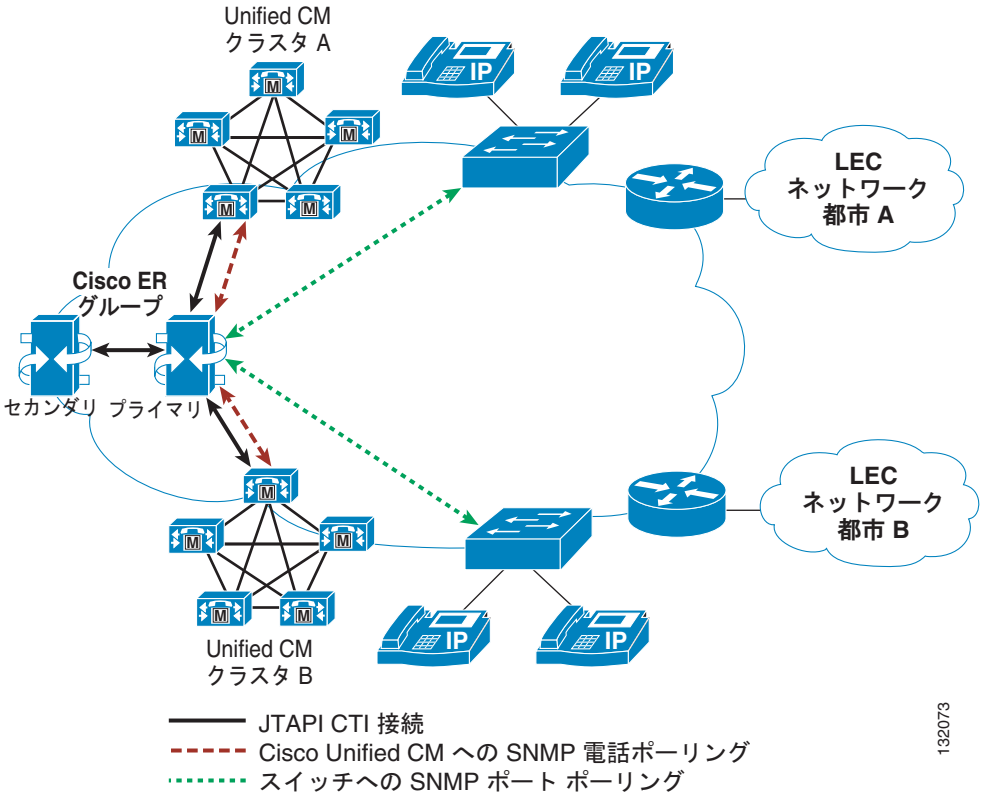


図 10-1 の単一の Cisco ER グループは、次のコンポーネントとインターフェイスします。

- SNMP を介して各 Unified CM クラスタとインターフェイスし、それぞれに設定されている電話機に関する情報を収集する。
- SNMP を介して企業のすべてのスイッチとインターフェイスし、どのスイッチに接続されているどのクラスタの電話機でも、その位置を確認できるようにする。電話機のロケーションが IP サブネットに基づいて識別される場合、この接続は不要です。IP サブネットベースの ERL を設定する方法の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Configuring Cisco Emergency Responder」の章を参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html
- JTAPI を介して各 Unified CM クラスタとインターフェイスし、911 をダイヤルするどの電話機にも必要なコール処理を可能にする必要があります。そのコール処理とは、発信側電話機の ERL の識別、ELIN の割り当て、（発信側電話機のロケーションに基づく）適切なゲートウェイへのコール リダイレクション、PSAP コールバック機能の処理などです。

Cisco Emergency Responder によって使用される JTAPI インターフェイスのバージョンは、Cisco Emergency Responder が接続される Unified CM ソフトウェアのバージョンによって決まります。システムの初期化時に、Cisco ER は Unified CM クラスタに問い合せ、適切な JTAPI Telephony Service Provider（TSP; テレフォニー サービス プロバイダー）をロードします。Cisco ER サーバ上には 1 つのバージョンの JTAPI TSP しか存在できないため、単一の Cisco ER グループがインターフェイスするすべての Unified CM クラスタが、同じバージョンの Unified CM ソフトウェアを実行する*必要があります*。

配置によっては、このソフトウェア バージョン要件によって問題が生じる場合があります。たとえば、Unified CM のアップグレード中は、クラスタが異なると、実行されているソフトウェアのバージョンが異なり、一部のクラスタが、Cisco ER サーバ上で実行されているバージョンと互換性のないバージョンの JTAPI を実行していることがあります。このような場合、Cisco ER グループの JTAPI バージョンとは異なるバージョンを実行しているクラスタからの緊急コールは、緊急番号の CTI ルート ポイントの Call Forward Busy 設定によって提供されるコール トリートメントを受けられます。

複数の Unified CM クラスタに対して単一の Cisco ER グループが適切であるかどうかを検討する場合は、次のガイドラインを適用してください。

- Unified CM のアップグレードは、緊急コールの数ができるだけ少ない許容可能なメンテナンス時間帯（たとえば、営業時間後や、システムの使用量が最小限のとき）に行う。
- クラスタの数とサイズから判断して、ソフトウェアのアップグレード中に異なるバージョンの JTAPI が使用される時間を最小限に抑えることができると思われる場合にだけ、単一の Cisco ER グループを使用する。

たとえば、8 台のサーバで構成される 1 つの大規模なクラスタと、2 台のサーバで構成される 1 つの小規模なクラスタを同時に配置し、単一の Cisco ER グループとともに使用するとします。この場合、大規模なクラスタを最初にアップグレードすることを推奨します。これにより、アップグレードのメンテナンス時間帯に Cisco ER サービスを使用できないユーザ（小規模なクラスタからサービスを受けるユーザ）の数を最小限に抑えられます。さらに、小規模なクラスタのユーザは、Cisco ER に到達できない間、実際には、緊急コールの一時スタティック ルーティングによって適切にサービスを受けられます。これは、そのユーザが、その時間中に発信されるすべての非 ER コールに割り当てられている単一の ERL/ELIN によって識別されることが可能なためです。

複数の Cisco ER グループ

マルチクラスタ システムをサポートするために、複数の Cisco ER グループを配置することもできます。この場合は、各 ER グループが次のコンポーネントとインターフェイスします。

- Unified CM クラスタ。次の方式を使用します。
  - SNMP：クラスタに設定されている電話機に関する情報を収集します。
  - JTAPI：適切なゲートウェイへの、またはローミング電話機の場合は適切な Unified CM クラスタへの、コール リダイレクションに関連するコール処理を可能にします。
- その Cisco ER グループの Unified CM に関連付けられているほとんどの電話機の接続先となるアクセス スイッチ（SNMP を使用）。

この方法を使用すると、Unified CM クラスタが、異なるバージョンのソフトウェアを実行できます。これは、各クラスタが、別の Cisco ER グループとインターフェイスするためです。

電話機がネットワーク上のさまざまな場所をローミングし、Cisco ER がその電話機をトラッキングできるようにするには、Cisco ER グループを 1 つの Cisco ER クラスタに設定する必要があります。Cisco ER クラスタおよびグループの詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Planning for Cisco Emergency Responder*」の章を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

図 10-2 は、Cisco ER クラスタリングの背後にある基本的な概念を表すトポロジの例を示しています。

図 10-2　　複数の Cisco ER グループ

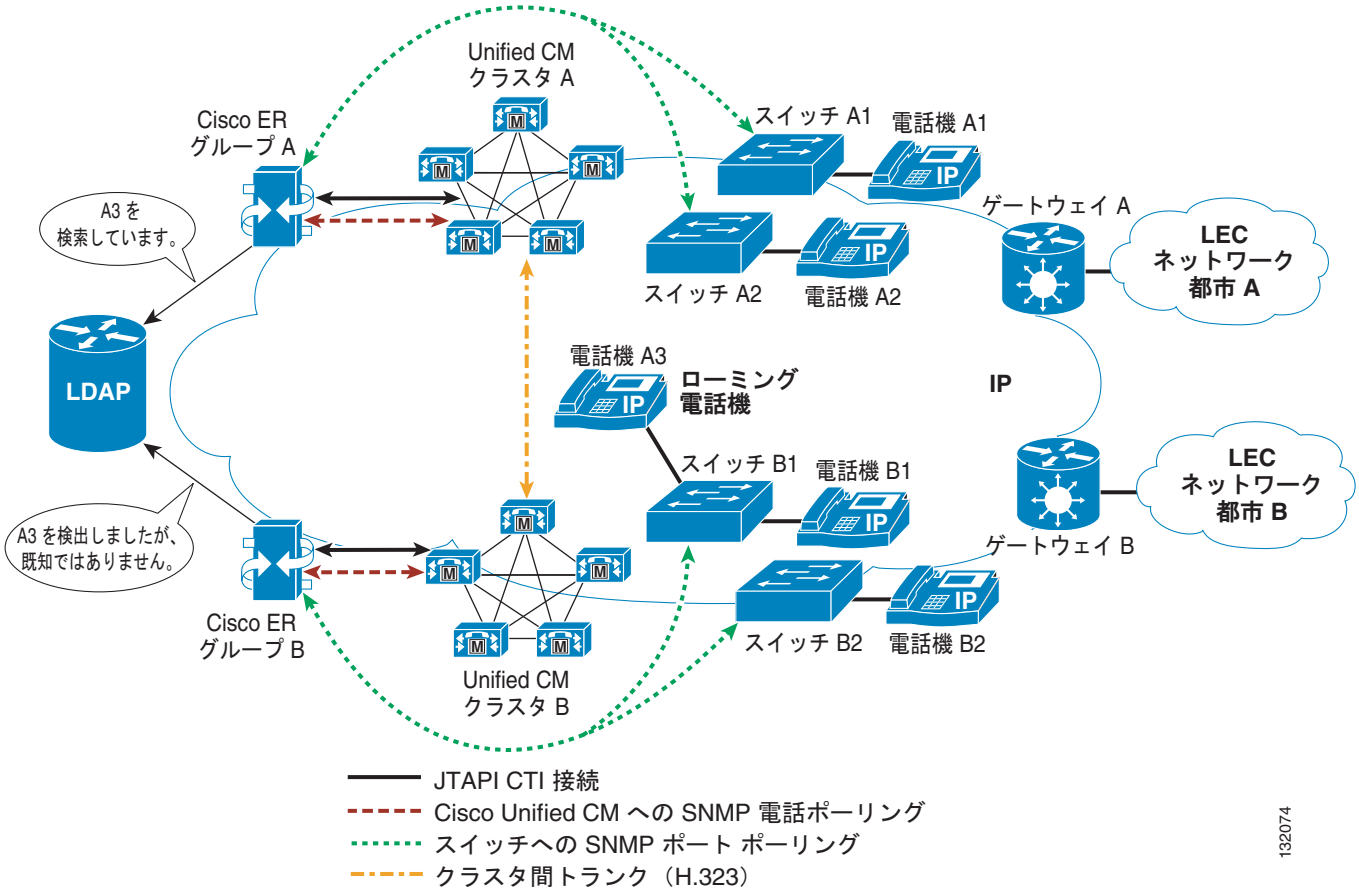


図 10-2 は、次のトポロジを示しています。

- Cisco ER グループ A は、Unified CM クラスタ A とインターフェイスして、スイッチ A1 および A2 にアクセスする。このグループは、Unified CM クラスタ A に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。
- 同様に、Cisco ER グループ B は、Unified CM クラスタ B とインターフェイスして、スイッチ B1 および B2 にアクセスする。このグループは、Unified CM クラスタ B に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。

（注） Emergency Responder の場合は、ER クラスタ内のすべての ER グループで同じバージョンのソフトウェアを実行する必要があります。

Cisco ER グループのトラッキング ドメイン内の電話機移動

電話機が、同じホーム Cisco ER グループによって制御されるアクセス スイッチ間を移動する場合、その電話機の緊急コール処理は、単一の Unified CM クラスタを使用する配置で行われる処理と同じです。たとえば、アクセス スイッチ A1 と A2 の間を移動する電話機は、Unified CM クラスタ A に登録されたままで、移動前も移動後もその電話機のロケーションは Cisco ER グループ A によって決定されます。Unified CM クラスタ A による電話機検出と、スイッチ A2 による電話機のロケーション特定の両方で、電話機は引き続き Cisco ER グループ A の完全な制御下にあります。したがって、電話機は位置未確認の電話機と見なされません。

Cisco ER クラスタのさまざまなトラッキング ドメイン間の電話機移動

Cisco ER クラスタは、実質的に、ロケーション情報を共有する Cisco ER グループの集まりです。各グループは、アクセス スイッチ上または IP サブネット内で検出するすべての電話機のロケーションを共有します。

また、Cisco ER グループは、Cisco ER グループのトラッキング ドメイン内（スイッチまたは IP サブネット内）で位置を確認できないが、そのグループに関連付けられている Unified CM クラスタに登録されていることがわかっている電話機に関する情報も共有します。このような電話機は、*位置未確認*と見なされます。

異なる Cisco ER グループによってモニタされるアクセス スイッチ間を電話機がローミングする場合、それらのグループは、電話機のロケーションに関する情報を交換できるように、1 つの Cisco ER クラスタに設定される必要があります。たとえば、Unified CM クラスタ A に登録されている電話機 A3 が、Cisco ER グループ B によって制御されるアクセス スイッチに接続されているとします。Cisco ER グループ A は、電話機 A3 が Unified CM クラスタ A に登録されていることを認識しますが、サイト A のどのスイッチでも電話機 A3 の位置を確認することはできません。したがって、電話機 A3 は Cisco ER グループ A によって*位置未確認*と見なされます。

これに対し、Cisco ER グループ B は、モニタ対象のスイッチの 1 つで、電話機 A3 の存在を検出します。電話機 A3 は、Unified CM クラスタ B に登録されていないため、*不明*な電話機として Cisco ER LDAP データベースを介してアドバタイズされます。

2 つの Cisco ER グループは、LDAP データベースを介して通信しているため、Cisco ER グループ B の*不明*な電話機 A3 が Cisco ER グループ A の*位置未確認*の電話機 A3 と同じであることがわかります。

Cisco ER グループ A の [Unlocated Phone] ページには、この電話機のホスト名が、リモート Cisco ER グループ（この場合は Cisco ER グループ B）とともに表示されます。

Cisco ER クラスタ内の緊急コール ルーティング

Cisco ER クラスタリングは、1 つの Unified CM クラスタと 1 つの Cisco ER で構成されるペア間で緊急コールをリダイレクトできるようにするルート パターンにも依存します。詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「*Creating Route Patterns for Inter-Cisco Emergency Responder-Group Communications*」の項を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

電話機 A3 が緊急コールを発信した場合、コール シグナリング フローは次のようになります。

1. 電話機 A3 が、処理のために緊急コール ストリングを Unified CM クラスタ A に送信します。
2. Unified CM クラスタ A が、リダイレクションのためにコールを Cisco ER グループ A に送信します。
3. Cisco ER グループ A が、電話機 A3 の位置を Cisco ER グループ B のトラッキング ドメイン内であると確認し、Unified CM クラスタ B を指すルート パターンにコールをリダイレクトします。
4. Unified CM クラスタ A がコールを Unified CM クラスタ B に送信します。
5. Unified CM クラスタ B が、リダイレクションのためにコールを Cisco ER グループ B に送信します。
6. Cisco ER グループ B が、電話機 A3 のロケーションに関連付けられている ERL と ELIN を識別し、コールを Unified CM クラスタ B にリダイレクトします。発信番号は、電話機 A3 の ERL に関連付けられている ELIN に変換されます。着信番号は、コールを適切なゲートウェイにルーティングするように変更されます。
7. Unified CM クラスタ B が、Cisco ER グループ B から入手した新しい着信番号情報に従ってコールをルーティングします。
8. Unified CM クラスタ B が、ゲートウェイを通じてコールを緊急公衆網ネットワークに送信します。

Cisco Emergency Responder の WAN 配置

Cisco Emergency Responder Group は Cisco Unified CM クラスタからリモートで（つまり、WAN を介して）見つけることができます。また、プライマリ Cisco ER サーバおよびセカンダリ Cisco ER サーバを WAN を介して地理的に離れたサイトに配置することもできます。このような配置の場合、推奨される Round-Trip Time（RTT; ラウンド トリップ時間）は 40 msec 以下であり、Cisco ER サーバ間で必要な最小帯域幅は 1.544 Mbps です。

ALI フォーマット

マルチクラスタ構成では、単一の Cisco ER グループに定義されている ERL と ELIN の物理ロケーションが、複数の電話会社の管轄地区にまたがることがあります。これにより、複数の LEC 用のレコードを含む共通ファイルから、さまざまな電話会社用のレコードを抽出する必要が生じることがあります。

Cisco ER は、この情報を、National Emergency Number Association（NENA）2.0、2.1、および 3.0 フォーマットに準拠する ALI レコードでエクスポートします。ただし、多くのサービス プロバイダーは NENA 規格を使用しません。そのような場合は、Cisco ER によって生成された ALI レコードが、サービス プロバイダーによって指定されたフォーマットに準拠するように、ALI Formatting Tool（AFT）を使用してそのレコードを変更できます。これにより、サービス プロバイダーは、再フォーマットされたファイルを使用して、ALI データベースを更新できます。

ALI Formatting Tool（AFT）では、次の機能を実行できます。

- レコードを選択し、ALI フィールドの値を更新する。AFT では、ALI フィールドを編集し、さまざまなサービス プロバイダーの要件を満たすようにカスタマイズできます。これにより、サービス プロバイダーは、再フォーマットされた ALI ファイルを読み取り、そのファイルを使用して ELIN レコードを更新できます。
- 複数の ALI レコードに対するバルク更新を実行する。バルク更新機能を使用すると、選択したすべてのレコード、1 つのエリア コード、または 1 つのエリア コードと 1 つのシティ コードに対して共通の変更を適用できます。
- エリア コード、シティ コード、または 4 桁のディレクトリ番号に基づいて ALI レコードを選択してエクスポートする。たとえば、あるエリア コードのすべての ALI レコードを選択してエクスポートすることにより、各サービス プロバイダーのすべての ELIN レコードにすばやくアクセスできるため、複数のサービス プロバイダーを簡単にサポートできます。

AFT の柔軟性を利用して、単一の Cisco ER グループが、複数の ALI データベース フォーマットで ALI レコードをエクスポートできます。Cisco ER グループがサービスを提供する Unified CM クラスタが 2 つの LEC の管轄地区内にあるサイトを持つ場合、基本的な方法は次のとおりです。

1. Cisco Emergency Responder からの ALI レコード ファイル出力を標準の NENA フォーマットで入手します。このファイルには、複数の LEC 用のレコードが含まれています。
2. 必要な ALI フォーマットごとに元のファイルの 1 つのコピーを作成します（LEC ごとに 1 つのコピー）。
3. 最初の LEC（たとえば、LEC-A）の AFT を使用して、NENA フォーマットのファイルのコピーをロードし、他の LEC に関連付けられているすべての ELIN のレコードを削除します。削除する情報は、通常、NPA（またはエリア コード）によって識別できます。
4. 結果として生成されたファイルを、LEC-A に必要な ALI フォーマットで保存し、適宜ファイル名を付けます。
5. 各 LEC に対してステップ 3 と 4 を繰り返します。

ALI Formatting Tools の詳細については、次の Web サイトで入手可能なオンライン マニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

この URL にリストされていない LEC の場合、スプレッドシート プログラムや標準のテキスト エディタなど、標準のテキスト ファイル編集ツールを使用して Unified CM からの出力をフォーマットできます。

CHAPTER 11

コール アドミッション制御

コール アドミッション制御機能は、すべての IP テレフォニー システム（特に IP WAN 経由で接続された複数のサイトで構成されるシステム）に不可欠なコンポーネントです。コール アドミッション制御の機能と必要性をわかりやすく説明するために、図 11-1 の例について考えます。

図 11-1　　コール アドミッション制御が必要な理由

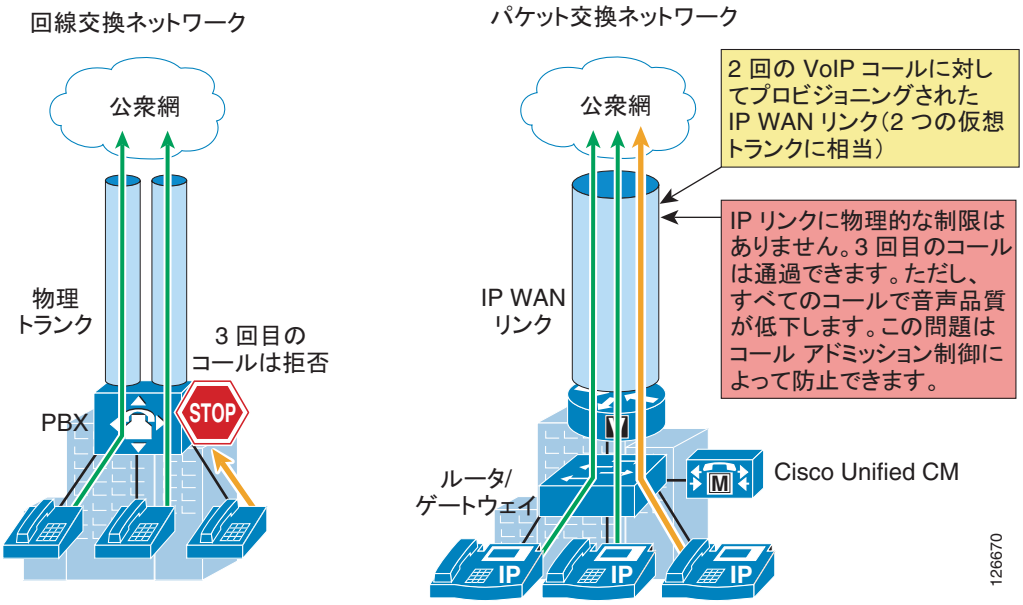


図 11-1 の左側で示すように、従来の TDM ベースの PBX は、回線交換ネットワークの一部として動作します。このネットワークでは、回線はコールがセットアップされるたびに確立されます。このため、レガシー PBX が公衆網または他の PBX に接続されている場合は、一定数の物理トランクを設定する必要があります。公衆網または他の PBX 宛てのコールをセットアップする必要があるとき、PBX は、使用可能なトランクの中からトランクを選択します。使用可能なトランクがない場合、コールは PBX によって拒否され、発信者にはネットワーク ビジー信号が聞こえます。

次に、図 11-1 の右側に示している IP テレフォニー システムについて考えます。このシステムは、パケット交換ネットワーク（IP ネットワーク）を基盤としているため、IP テレフォニー コールをセットアップするために回線を確立する必要はありません。サンプリング音声を含んでいる IP パケットが、他のタイプのデータ パケットとともに、IP ネットワーク経由でルーティングされるだけです。音声パケットは、Quality of Service（QoS）を使用してデータ パケットと区別されますが、帯域幅リソースは、特に IP WAN リンクでは無限ではありません。このため、ネットワークの管理者が、一定量の「優先」帯域幅を各 IP WAN リンク上の音声トラフィック専用として割り当ててください。ただし、設定した帯域幅がすべて使用される状態になった場合は、IP テレフォニー システムで以後のコールを拒

否して、IP WAN リンク上のプライオリティ キューのオーバーサブスクリプションを防止する必要があります。オーバーサブスクリプションが発生すると、すべての音声コールで品質が低下します。この機能はコール アドミッション制御と呼ばれ、IP WAN を利用したマルチサイト配置で良好な音声品質を保証するために不可欠なものです。

エンド ユーザ環境の満足度を維持するには、コール アドミッション制御機能を常にコール セットアップ段階で実行する必要があります。このようにすることで、ネットワーク リソースを使用できない場合に、エンド ユーザにメッセージを表示したり、異なるネットワーク（公衆網などの）を通じてコールを再ルーティングしたりすることができるようになります。

この章では、次の主要トピックについて説明します。

- 「コール アドミッション制御の設計上の推奨事項」（P.11-94）

  この項では、この章で説明する原理とメカニズムにすでに精通している読者向けに、コール アドミッション制御に関する主なベスト プラクティス、推奨事項、および注意事項の概要を示します。

- 「コール アドミッション制御の原理」（P.11-3）

  この項では、IP ベースのテレフォニー システムにおけるコール アドミッション制御の 2 つの基本的な方法である、トポロジ対応とトポロジ非対応のコール アドミッション制御について説明します。

- 「コール アドミッション制御のアーキテクチャ」（P.11-12）

  この項では、Cisco Unified Communications システムのさまざまなコンポーネント、たとえば Cisco Unified Communications Manager ロケーション、Cisco IOS ゲートキーパー、RSVP、RSVP SIP プレコンディションなどで使用できるコール アドミッション制御メカニズムについて説明します。

- 「コール アドミッション制御の設計上の考慮事項」（P.11-69）

  この項では、上の項で説明したメカニズムを適用し、組み合せる方法について、IP WAN のトポロジ（単純なハブアンドスポーク、2 層ハブアンドスポーク、MPLS、またはその他のトポロジ）に基づいて、および採用する Cisco Unified Communications Manager 配置モデルに基づいて示します。

この章の新規情報

表 11-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 11-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Unified Border Element および RSVP SIP プレコンディション	「Cisco Unified Border Element および RSVP SIP プレコンディション」（P.11-65）	2010 年 11 月 15 日
Cisco IOS における RSVP コール アドミッション制御機能の拡張	「Cisco IOS の機能」（P.11-29）	2010 年 11 月 15 日
クラスタ間のエクステンション モビリティ	「クラスタ間のエクステンション モビリティのアーキテクチャおよび考慮事項」（P.11-59）	2010 年 4 月 2 日
相互運用性	「Unified CM の相互運用性と機能の考慮事項」（P.11-61）	2010 年 4 月 2 日
リソース予約プロトコル（RSVP）	「リソース予約プロトコル（RSVP）を使用した Unified Communications アーキテクチャ」（P.11-17）	2010 年 4 月 2 日

表 11-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報 （続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
RSVP のアプリケーション ID	「RSVP アプリケーション ID と Unified CM」（P.11-47）	2010 年 4 月 2 日
Service Advertisement Framework（SAF）および Call Control Discovery（CCD）	「Service Advertisement Framework（SAF）および Call Control Discovery（CCD）」（P.11-66）	2010 年 4 月 2 日
SIP プレコンディション	「RSVP SIP プレコンディション」（P.11-49）	2010 年 4 月 2 日

コール アドミッション制御の原理

すでに述べたように、コール アドミッション制御は、IP ベースのテレフォニー システムのコール処理エージェントの機能です。したがって理論上は、IP ベースのテレフォニー システムと同じ数のコール アドミッション制御メカニズムが存在する可能性があります。しかし、ほとんどの既存のコール アドミッション制御メカニズムは、次の 2 つの主なカテゴリのいずれかになります。

- トポロジ非対応コール アドミッション制御：コール処理エージェント内の静的設定に基づくもの
- トポロジ対応コール アドミッション制御：使用可能なリソースに関するコール処理エージェントとネットワーク間の通信に基づくもの

次の項では、トポロジ非対応コール アドミッション制御の原理とその制限について分析し、次にトポロジ対応コール アドミッション制御の原理を示します。

トポロジ非対応コール アドミッション制御

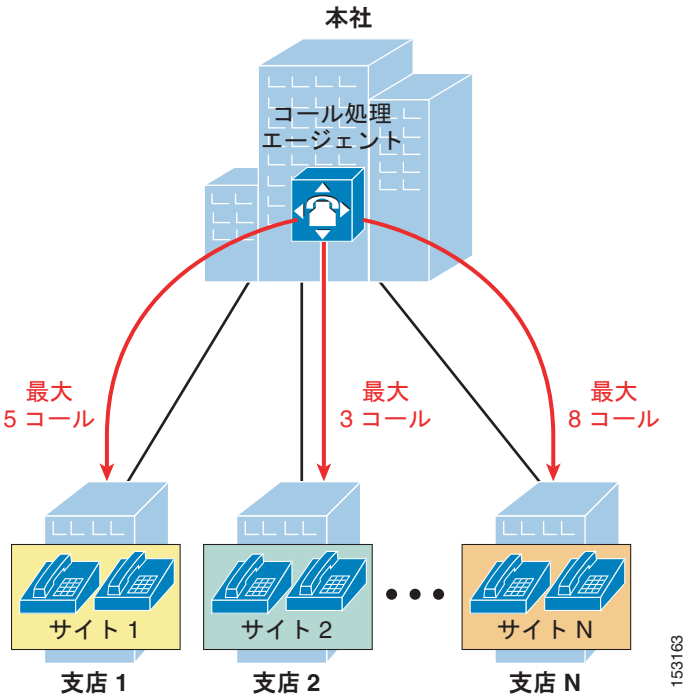
トポロジ非対応コール アドミッション制御とは、IP WAN で接続されたリモート サイトとの間の同時コール数を制限することを目的とし、コール処理エージェントまたは IP ベースの PBX 内の静的設定に基づくメカニズムです。

図 11-2 に示すように、このようなメカニズムのほとんどは、一般に企業 IP WAN に接続される地理上の支店に対応する、論理的な「サイト」エンティティの定義に依存しています。

各支店にあるすべてのデバイスを対応するサイト エンティティに割り当てた後に、管理者がそのサイトを宛先または発信元とするコールの許容最大数（または帯域幅の最大量）を設定するのが一般的です。

新しいコールの確立が必要になるたびに、コール処理エージェントは発信エンドポイントおよび終端エンドポイントが属するサイトをチェックし、（関係する両サイトのコール数または帯域幅の量に関して）コールに利用できるリソースがあるかどうか確認します。チェックが成功した場合、そのコールは確立され、両サイトのカウンタが減少します。チェックに失敗した場合、コール処理エージェントは事前に設定されたポリシーに基づいてコールの処理方法を決定できます。たとえば、発信者のデバイスにネットワーク ビジー信号を送信したり、公衆網接続を通じて再ルーティングを試行します。

図 11-2　トポロジ非対応コール アドミッション制御の原理



トポロジ非対応のコール アドミッション制御メカニズムは静的設定に依存しているため、一般に比較的単純な IP WAN トポロジのネットワークだけに配置できます。実際、このようなメカニズムのほとんどでは、図 11-3 に示すような単純なハブアンドスポーク トポロジまたは単純な MPLS ベースのトポロジ（MPLS サービスがサービス プロバイダーによって提供される場合）が必要です。

図 11-3　トポロジ非対応コール アドミッション制御に適したドメイン

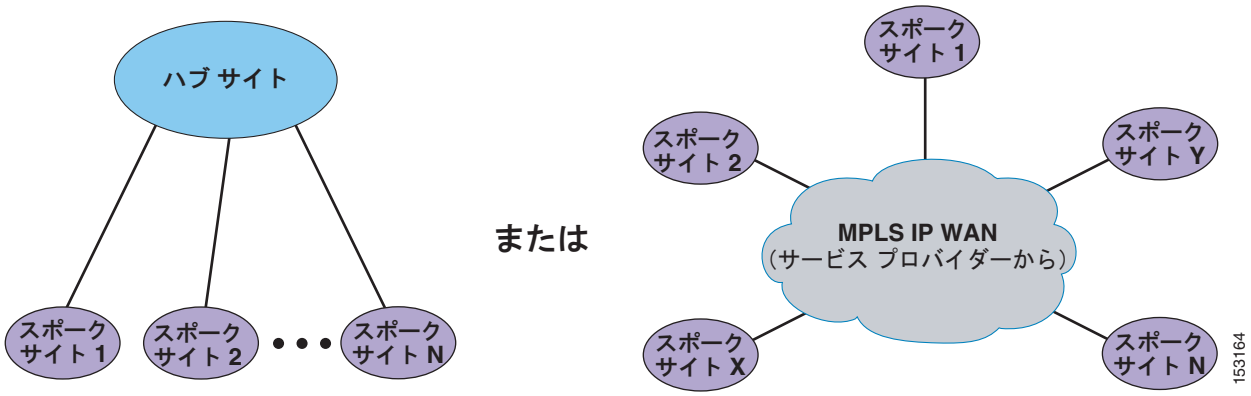


図 11-3 に示すようなハブアンドスポーク ネットワークまたは MPLS ベースのネットワークで、各スポーク サイトはコール処理エージェント内の「サイト」に割り当てられ、その「サイト」のコール数または帯域幅の量は、そのスポークを IP WAN に接続する IP WAN リンク上の音声またはビデオ（あるいはその両方）に利用可能な帯域幅と一致するように設定されます。

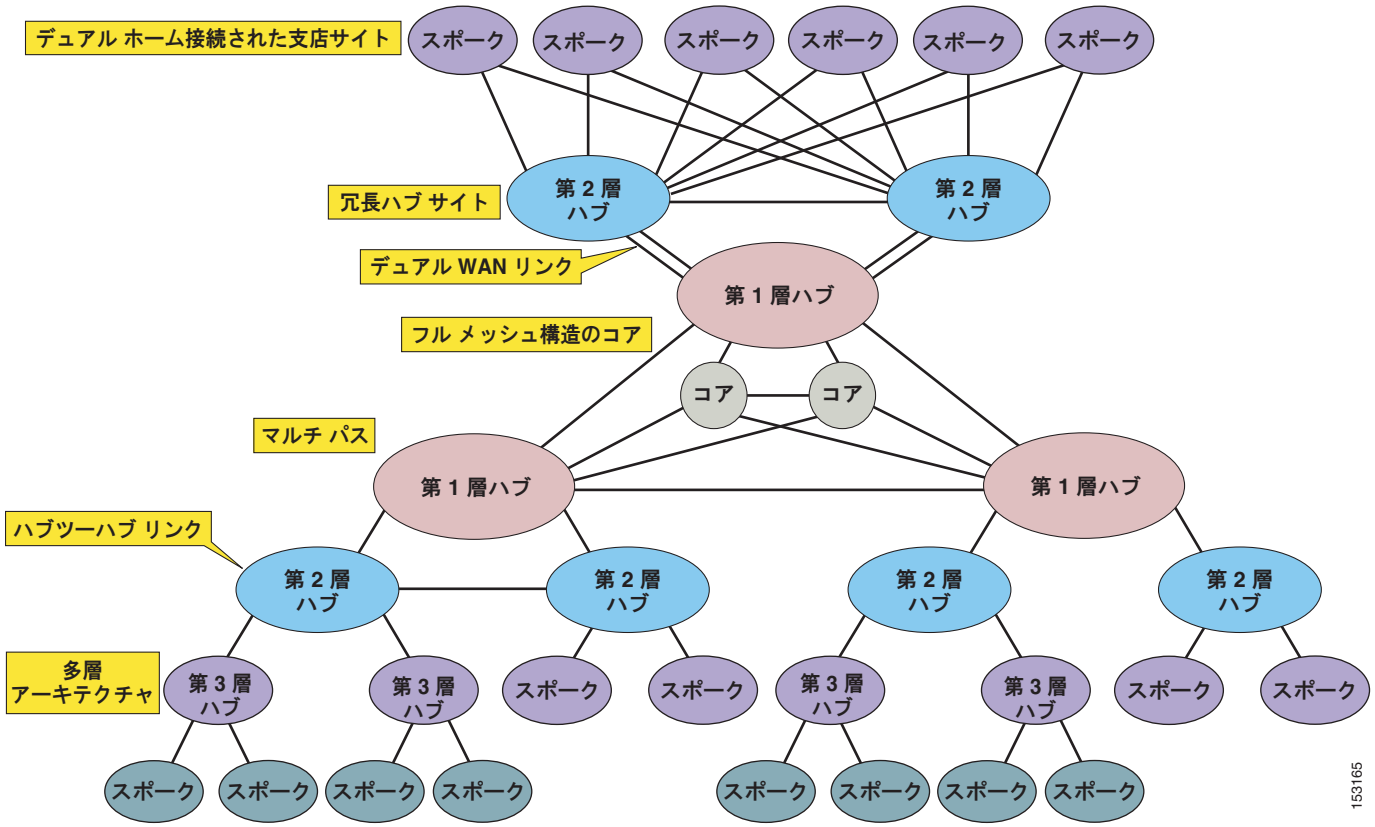
スポーク サイトからハブ サイトへの冗長リンクと、2 つのスポーク サイトを直接接続するリンクがないことに注意してください。次の項では、トポロジ非対応コール アドミッション制御で、このようなリンクが問題を発生させる理由について説明します。

トポロジ非対応コール アドミッション制御の制限

現在の企業ネットワークでは、ハイ アベイラビリティは共通の要件であり、そのために IP WAN ネットワーク接続に冗長性が求められることがあります。

代表的な企業ネットワークにおける IP WAN トポロジについて考えると、純粋なハブアンドスポークトポロジの前提を複雑にする数多くの特性があることがわかります。図 11-4 は、このようなネットワーク特性のいくつかを 1 つの図にまとめたものです。すべての特性が一度に現れるのは大規模な企業ネットワークだけですが、多くの IP WAN ネットワークでも最低 1 つの特性が存在していることがよくあります。

図 11-4　代表的な企業ネットワークのトポロジ特性



「コール アドミッション制御の設計上の考慮事項」（P.11-69）の項で説明するように、複雑なネットワーク トポロジにトポロジ非対応コール アドミッション制御メカニズムを適用できる場合がありますが、この方法を利用できる場合と、実現できる動作に関して制限があります。たとえば、冗長性がネットワーク要件となっている IP WAN を通じてハブ サイトに接続される支店サイトの単純なケースについて考えます。一般的に、冗長性は次のいずれかの方法で実現できます。

- IP WAN へのプライマリ リンクとバックアップ リンクを備えた 1 台のルータ
- ロード バランシング設定で 2 つのアクティブな WAN リンクを備えた 1 台のルータ
- それぞれが IP WAN に接続され、ロード バランシングされたルーティングを行う 2 つのルータ プラットフォーム

図 11-5 の例では、プライマリ リンクとバックアップ リンクを備えた 1 台のルータの場合と、2 つのアクティブなロード バランシング リンクを備えた 1 台のルータの場合に、トポロジ非対応コール アドミッション制御メカニズムを適用しようとしています（2 つのルータ プラットフォームの場合のコール アドミッション制御に対する影響は、後者の例と同じです）。

図 11-5　デュアル リンクが存在する場合のトポロジ非対応コール アドミッション制御

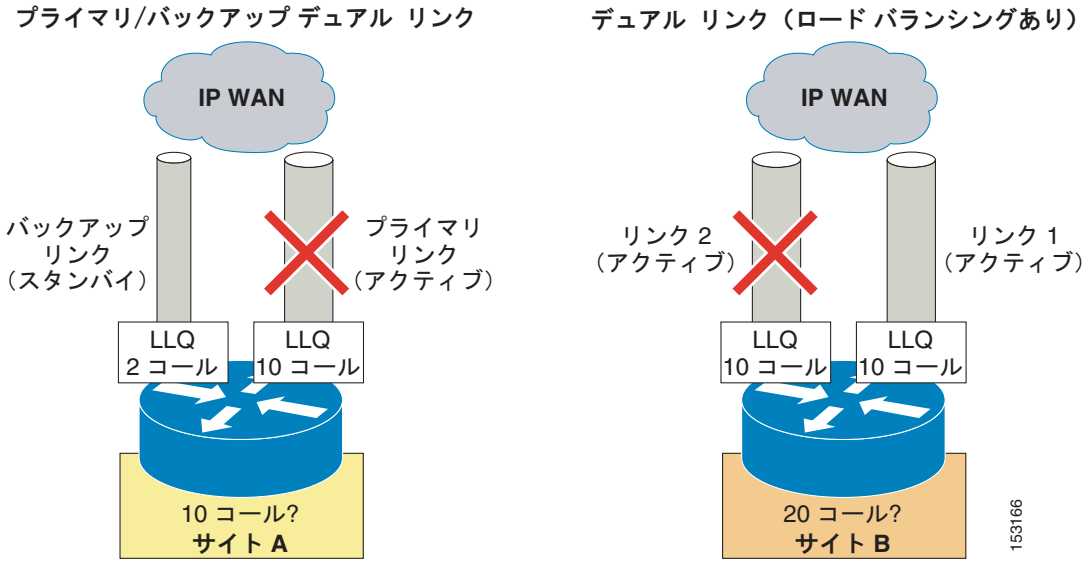


図 11-5 の最初の例で、支店 A は通常、最大 10 の同時コールが可能になるよう、Low Latency Queuing（LLQ; 低遅延キューイング）帯域幅がプロビジョニングされたプライマリ リンクを通じて、IP WAN に接続されます。このプライマリ リンクに障害が発生した場合、小さい方のバックアップ リンクがアクティブになり、IP WAN への接続を維持します。ただし、このバックアップ リンクの LLQ 帯域幅は、最大 2 つの同時コールだけが可能なようにプロビジョニングされています。

この支店にトポロジ非対応コール アドミッション制御メカニズムを配置するには、コール処理エージェントで「サイト」A を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。サイト A の最大値として 10 コールを使用する場合、プライマリ リンクの障害時にバックアップ リンクにオーバーランが発生し、すべてのアクティブなコールで音声の品質が低下する可能性があります。これに対して、最大値を 2 コールにした場合、プライマリ リンクがアクティブなときは、残りの 8 コールに対してプロビジョニングされた帯域幅を使用できません。

次に、IP WAN に接続する 2 つのアクティブなリンクを備えた支店 B について考えます。各リンクは、最大 10 の同時コールが可能なようにプロビジョニングされ、ルーティング プロトコルは各リンク間のロード バランシングを自動的に実行します。この支店にトポロジ非対応コール アドミッション制御メカニズムを配置する場合、コール処理エージェントで「サイト」B を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。支店 A の場合と同様に、2 つのリンクの容量を増強し、サイト B の最大値として 20 コールを使用する場合、一方のリンクの障害時に、もう一方のリンクで LLQ のオーバーランが発生する可能性があります。たとえば、リンク #2 に障害が発生した場合、サイト B を宛先または発信元とする 20 の同時コールが引き続き可能です。これらのコールは、すべてリンク #1 を通じてルーティングされるようになるため、オーバーランが発生し、すべてのコールで音声品質が低下します。これに対して、最大 10 の同時コールでサイト B を設定した場合、（両方のリンクが動作している）通常の条件では、使用可能な LLQ 帯域幅が十分に活用されなくなります。

上記の 2 つの単純な例は、実際の企業ネットワークでの IP WAN 帯域幅のプロビジョニングが非常に複雑で、コール処理エージェント内の静的に設定されたエントリにまとめられない場合があることを示しています。このようなネットワークでトポロジ非対応コール アドミッション制御を配置すると、管理者は推測をしたり、回避策を取ったり、最適ではないネットワーク リソースの使用を許容したりする必要があります。

単純なハブアンドスポークに従わないネットワーク トポロジが存在する場合にコール アドミッション制御を提供する最適な方法は、次の項で説明するようにトポロジ対応コール アドミッション制御を実装することです。

（注）　一部の IP テレフォニー システムは、ネットワークで検知された輻輳に基づくフィードバック メカニズムで、従来のトポロジ非対応コール アドミッション制御を拡張します。これにより、音声品質が低下した場合、コールが強制的に公衆網経由になります。コール処理エージェントはコールの確立後に実行されることと、輻輳が発生している正確な場所を認識しないという理由から、この方法はまだ真のトポロジ対応コール アドミッション制御と同等ではありません。この章の最初に述べたように、効果的に運用するには、コールをセットアップする前にコール アドミッション制御を実行する必要があります。

トポロジ対応コール アドミッション制御

トポロジ対応コール アドミッション制御とは、IP WAN リンクを通じた同時コール数を制限することを目的とするメカニズムであり、任意のネットワーク トポロジに適用でき、またトポロジの変更にも動的に適応できます。

このような目的を達成するには、トポロジ対応コール アドミッション制御は、コール処理エージェント（または IP ベースの PBX）とネットワーク間のネットワーク リソースの可用性に関するリアルタイム通信を利用する必要があります。ネットワークは分散エンティティであるため、リアルタイムの通信にはシグナリング プロトコルが必要です。

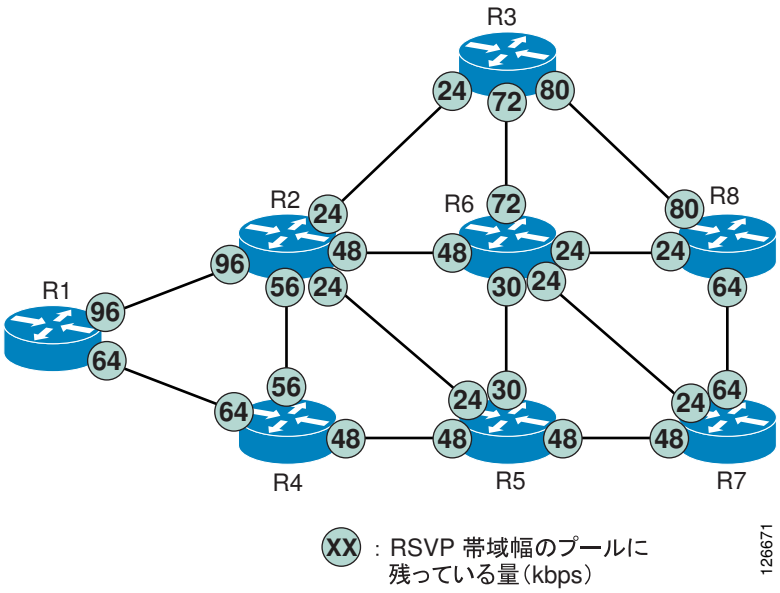
Resource Reservation Protocol（RSVP; リソース予約プロトコル）は、アプリケーションが IP ネットワークを通じて動的に帯域幅を予約できるようにするための、業界初のシグナリング プロトコルです。RSVP を使用すると、アプリケーションはネットワークを通じたデータ フロー（音声コールなど）のために一定の帯域幅を要求し、実際のリソースの可用性に基づいて予約結果の通知を受け取ることができます。

音声コールまたはビデオ コールのためのコール アドミッション制御の特定のケースで、IP ベースの PBX は、2 つのリモート サイト間でコール セットアップ プロセスを RSVP 予約と同期し、予約の結果に基づいてルーティングの決定を行います。分散型ネットワークに対応し、動的に機能する性質を持っているため、RSVP はあらゆるネットワーク トポロジにわたって帯域幅を予約できます。つまり、本格的なトポロジ対応コール アドミッション制御メカニズムを提供します。

RSVP がネットワークで帯域幅予約を実行する方法の基本的な原理を理解するために、図 11-6 に示す簡単な例について考えます。この例では、メッセージ交換とプロトコルの動作自体については説明しません。機能によってもたらされる結果を中心に説明します。RSVP メッセージ交換の詳細については、「RSVP の原理」（P.11-18）を参照してください。

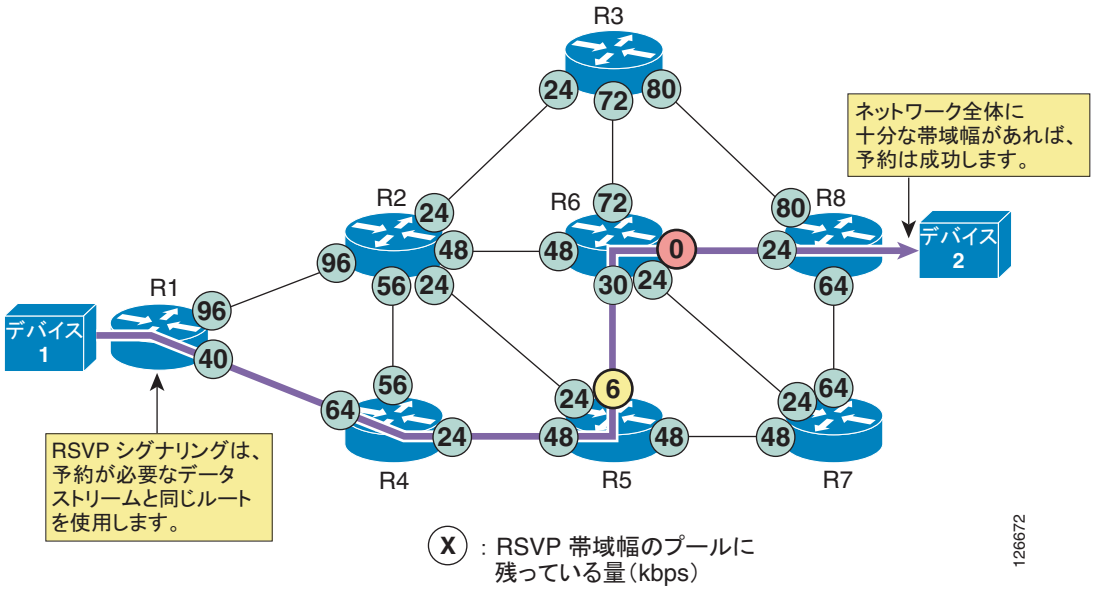
図 11-6 に示すネットワークの各ルータ インターフェイスで、RSVP が有効になっているとします。円で囲まれた数値は、各インターフェイス上に残っている使用可能な RSVP 帯域幅の量を表しています。

図 11-6　RSVP の原理を示すためのサンプル ネットワーク



ここで、RSVP 対応のアプリケーションが、2 つのデバイス間でのデータ ストリーム用に一定の帯域幅を予約するとします。このシナリオを図 11-7 に示します。この図では、デバイス 1 からデバイス 2 への個々のデータ ストリームで、24 Kbps の帯域幅を要求することを示しています。

図 11-7　予約が成功する RSVP シグナリング

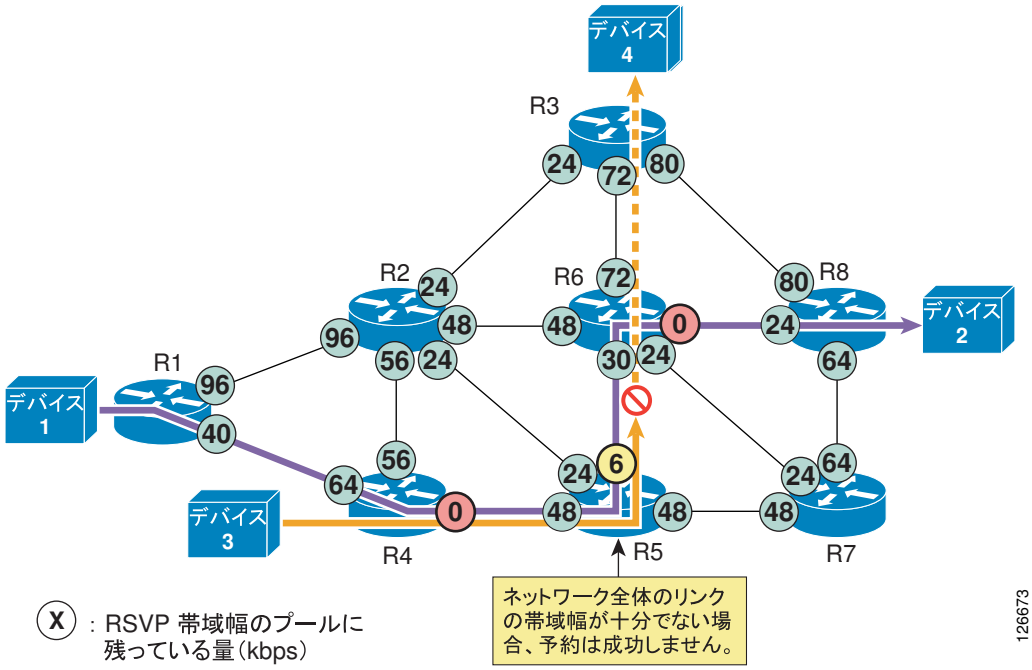


ここでは、図 11-7 について説明します。

- RSVP は、自身ではルーティングを実行しません。代わりに、下位レイヤで機能しているルーティング プロトコルを使用して、予約要求の宛先を決定します。トポロジの変更に対応するためにルーティングのパスが変化すると、RSVP は、自身の予約を予約が存在する新しいパスに合せて調整します。
- RSVP プロトコルは、デバイス 1 からデバイス 2 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 11-7 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- 使用可能な帯域幅がすべての発信側インターフェイスで十分にあり、この新しいデータ ストリームを受け付けることができる場合は、予約が成功し、アプリケーションに通知されます。
- RSVP 予約は単方向です。この例では、予約はデバイス 1 からデバイス 2 に向かって確立され、逆方向については確立されません。音声会議やビデオ会議などの双方向アプリケーションがある場合は、各方向について 1 つずつ、2 つの予約を確立する必要があります。
- RSVP は、RSVP をサポートしないルータ ノードでは透過的に動作します。RSVP に対応しないルータがパスに存在していても、それらのルータは単に RSVP メッセージを無視して、他の IP パケットと同様に渡すだけであり、予約を確立することは可能です（プロトコルのメッセージと動作の詳細については、「RSVP の原理」（P.11-18）を参照してください）。ただし、エンドツーエンドでの QoS を確保するには、この RSVP 非対応のルータが制御するリンク上で、帯域幅の輻輳が発生しないようにする必要があります。

デバイス 1 とデバイス 2 の間で予約が正常に確立された後に、別のアプリケーションがデバイス 3 とデバイス 4 の間で 24 Kbps の予約を要求したとします（図 11-8 を参照）。

図 11-8　予約が成功しない RSVP シグナリング



ここでは、図 11-8 について説明します。

- RSVP プロトコルは、デバイス 3 からデバイス 4 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 11-8 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- この例では、R6 に対する R5 の発信側インターフェイス上に、この新しいデータ ストリームを受け付けるための使用可能な帯域幅が十分にありません。このため、予約は失敗し、アプリケーションに通知されます。パスに含まれている各発信側インターフェイス上の使用可能な RSVP 帯域幅は、以前の値に戻されます。
- 次にどのように処理するかは、アプリケーションが決定します。データの転送を放棄することも、何らかの方法で QoS 保証のないベストエフォート型トラフィックとして送信することもできます。

ここで、前の項で紹介した二重接続される支店 A および B の例に、RSVP に基づくトポロジ対応コール アドミッション制御方法を適用できます。

図 11-9 に示すように、支店 A には 10 コール用にプロビジョニングされた LLQ を備えるプライマリ リンクと、2 つのコールだけを許容するバックアップ リンクがあります。この方法で RSVP は、RSVP 帯域幅が LLQ 帯域幅と一致するように、両方のルータ インターフェイスで設定されます。支店 A は、他の支店を宛先または発信元とするすべてのコールの RSVP 予約を要求するために、コール処理エージェント内でも設定されます。これで、コールは、ルーティング プロトコルによって決定されるパスに自動的に従う RSVP 予約の結果に基づいて、許可または拒否されるようになります。通常の条件下では（プライマリ リンクがアクティブな場合）、最大 10 コールが許容されます。プライマリ リンクの障害時には、最大 2 コールだけが許容されます。

ポリシーは、一般にコール アドミッション制御に障害が発生した場合の動作を決定するために、コール処理エージェント内で設定できます。たとえば、コールを拒否したり、公衆網を通じて再ルーティングしたり、異なる DSCP マーキングでのベストエフォート コールとして IP WAN を通じて送信したりできます。

図 11-9　　デュアル リンクのトポロジ対応コール アドミッション制御

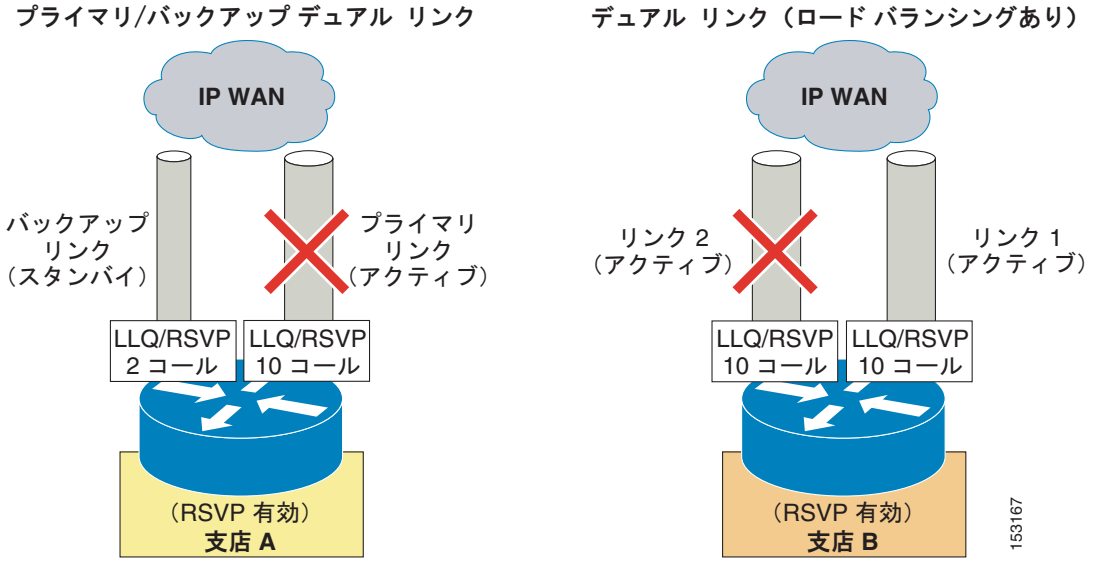


図 11-9 の右側に示すように、2 つのロード バランシング リンクを通じて IP WAN に接続される支店 B にも、同様の考慮事項が該当します。RSVP は、LLQ 設定と一致する帯域幅の値（この場合は、10 コールに対して十分な帯域幅）で、2 つのルータ インターフェイスのそれぞれで有効になります。支店 B は、他の支店との間のコール用に RSVP 予約を要求するため、コール処理エージェント内でも設定

されます。このときも、コールはルーティング プロトコルが決定するパスに沿って、使用可能な実際の帯域幅に基づいて許可または拒否されるようになります。したがって、2 つのリンクを通じた完全に均等なロード バランシングの場合、（両方のリンクが動作している）通常の条件下で最大 20 コールを許容できます。2 つのリンクのいずれかに障害が発生した場合は、最大 10 コールだけが許容されます。

10 を超えるコールがアクティブなときに 2 つのリンクのいずれかに障害が発生した場合、一部のコールは新しいパスでの予約の再確立に失敗します。この時点で、コール処理エージェントは通知を受け、設定されたポリシーに基づいて対応できます（追加のコールをドロップしたり、ベストエフォート コールとして再マーキングします）。

要するに、トポロジ対応コール アドミッション制御によって、管理者は任意のネットワーク トポロジでコール品質を保護し、トポロジの変更に自動的に適応し、すべての状況の下でネットワーク リソースを最適に使用できます。

MPLS ネットワークの特別な考慮事項

コール アドミッション制御の点から見ると、ネットワークの「ハブ」での RSVP のサポートに関して、MPLS に基づくネットワークは従来のレイヤ 2 WAN サービスに基づくネットワークとは異なっています。従来のレイヤ 2 WAN は、ほとんどの場合、RSVP への参加を有効にできる企業管理のルータから構成されます。MPLS ネットワークではネットワーク全体（クラウド）が「ハブ サイト」であるため、RSVP を有効にするための企業管理のハブ ロケーションは存在しません（詳細については、「単純な MPLS トポロジ」（P.11-77）を参照してください）。したがって、MPLS 環境でトポロジ対応コール アドミッション制御を提供するには、RSVP のサポート用にネットワークの Customer Edge（CE）デバイスを設定する必要があります。

RSVP は CE で有効にする必要があるため、この機器の制御は重要です。この機器が企業で管理されていない場合、サービス プロバイダーに問い合せて、WAN インターフェイスで RSVP が有効になっているかどうか、およびその実装で RSVP アプリケーション ID などの高度な機能がサポートされるかどうかを確認する必要があります。

RSVP メッセージは、RSVP 非対応 MPLS クラウドを透過的に通過するため、エンドツーエンドの RSVP 機能で問題は生じません。CE の WAN インターフェイスで RSVP を設定すると、そのプライオリティ キューにオーバーランが発生しなくなります。RSVP 予約は単方向であるため、RSVP が MPLS クラウドで有効になっていない場合、Provider Edge（PE）ルータでプライオリティ キューを保護するには、次の規則に従う必要があります。

- メディア ストリームを両方向で同じサイズにする。
- メディアを対称的にルーティングする。

RSVP PATH メッセージは、通過する RSVP 対応ルータの出口 IP アドレスを記録します。PATH メッセージの情報は、RSVP RESV メッセージを同じルートで返信するために使用されます。このメカニズムのため、CE と PE 間の WAN リンクにルーティング可能な IP アドレスがないと、RSVP 予約は失敗します。

MPLS ネットワークがこれらの規則に従っていない場合は、RSVP を実装する前にシスコのアカウント チームにお問い合せください。

コール アドミッション制御のアーキテクチャ

Cisco Unified Communications システムには、コール アドミッション制御機能を実行する複数のメカニズムがあります。この項では、次のカテゴリに従って、すべてのメカニズムの設計と設定のガイドラインについて説明します。

- トポロジ非対応メカニズム
  - 「Unified CM の静的ロケーション」（P.11-12）
  - 「Cisco IOS ゲートキーパー ゾーン」（P.11-15）
- トポロジ対応メカニズム
  - 「Unified CM の RSVP 対応ロケーション」（P.11-38）
  - 「RSVP SIP プレコンディション」（P.11-49）

Unified CM の静的ロケーション

Unified CM では、集中型コール処理配置において、コール アドミッション制御を実装するために、*静的ロケーション*と呼ばれている単純なメカニズムを取り入れています。Unified CM でデバイスを設定するときは、そのデバイスをロケーションに割り当てることができます。各ロケーションとの間のコールに対しては、特定の帯域幅が割り当てられます。Unified CM で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。Unified CM は、デバイスの物理的なロケーションを認識しません。このため、デバイスをある物理ロケーションから別のロケーションに移動する場合は、システム管理者がロケーション設定を手動でアップデートして、Unified CM がそのデバイスの帯域幅割り当てを正しく計算できるようにする必要があります。各デバイスは、デフォルトでは Hub_None ロケーションに配置されます。ロケーション Hub_None は、デフォルトで設定される特別なロケーションで、無制限の音声およびビデオの帯域幅が割り当てられます。ロケーション Hub_None は削除できません。支店ロケーションにあるデバイスが Hub_None ロケーションに設定されている場合、その支店デバイスが宛先または発信元となっている電話コールはすべて、コール アドミッション制御の対象となりません。

Unified CM では、各ロケーションに対して音声およびビデオの帯域幅プールを定義できます。ロケーションの音声帯域幅とビデオ帯域幅が [Unlimited] に設定されている場合、そのロケーションでは帯域幅を無限に使用できるため、そのロケーションが宛先または発信元となる音声コールとビデオ コールは、Unified CM ではすべて許可されます。帯域幅の値が有限のキロビット/秒（Kbps）に設定されている場合は、アクティブになっているすべてのコールで使用されている合計帯域幅が、その設定値以下になっている場合に限り、Unified CM は、そのロケーションで入出力されるコールを許可します。ロケーションのビデオ帯域幅を [None] に設定した場合、このロケーションが宛先または発信元となるすべてのビデオ コールは拒否されます。ただし、このロケーションの内部でやり取りされるビデオ コールには影響しません。

ビデオ コールの場合、ビデオ ロケーションの帯域幅については、コールのビデオ部分と音声部分の両方を考慮に入れる必要があります。したがって、ビデオ コールの場合、帯域幅が音声帯域幅プールから差し引かれることは一切ありません。

ロケーションでメンバーシップを指定できるデバイスには、次のものがあります。

- IP Phone
- CTI ポート
- H.323 クライアント
- CTI ルート ポイント
- カンファレンス ブリッジ

- Music On Hold（MoH; 保留音）サーバ
- ゲートウェイ
- トランク

静的ロケーションのコール アドミッション制御メカニズムでは、通話中のコール タイプ変更も考慮に入れる必要があります。たとえば、サイト間でビデオ コールを確立する場合、Unified CM は、それぞれのロケーションから適切なビデオ帯域幅を差し引きます。このビデオ コールが、ビデオ非対応のデバイスに転送する過程で音声専用コールに変更された場合、Unified CM は割り当てた帯域幅をビデオ プールに戻し、適切な帯域幅を音声プールから割り当てます。音声からビデオに変更されるコールについては、これとは逆の帯域幅割り当て変更が発生します。

表 11-2 に、さまざまなコールのタイプ（ビット レート）において静的ロケーション アルゴリズムが要求する帯域幅を示します。音声コールでは、Unified CM は、メディア ビット レートにレイヤ 3 オーバーヘッドを加えて計算します。たとえば、G.711 音声コールは、ロケーションの音声帯域幅プールから割り当てられた 80 kbps を消費します。ビデオ コールでは、Unified CM は、音声ストリームとビデオ ストリームの両方に対して、メディア ビット レートだけを計算します。たとえば、384 kbps の速度のビデオ コールに対して、Unified CM はビデオ帯域幅プールから 384 kbps を割り当てます。

表 11-2　静的ロケーション アルゴリズムが要求する帯域幅

コールのビット レート	静的ロケーションの帯域幅の値
G.711 音声コール（64 Kbps）	80 kbps
G.729 音声コール（8 Kbps）	24 kbps
128 Kbps ビデオ コール	128 kbps
384 Kbps ビデオ コール	384 kbps
512 Kbps ビデオ コール	512 kbps
768 Kbps ビデオ コール	768 kbps

コーデックおよび静的ロケーション帯域幅値のリストについては、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』の「*Call Admission Control*」の項の帯域幅計算情報を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

たとえば、使用可能な音声帯域幅 256 Kbps およびビデオ帯域幅 384 Kbps を指定した、支店 1 のロケーションの設定があるとします。この場合、支店 1 は最高 3 つの G.711 音声コール（コールごとに 80 Kbps）、または 10 個の G.729 音声コール（コールごとに 24 Kbps）、または両方のコールの組み合せ（256 Kbps を超えないこと）をサポートできます。このロケーションでは、使用されているビデオ コーデックおよび音声コーデックに応じて、さまざまな数のビデオ コールをサポートすることもできます（たとえば、384 kbps の帯域幅を要求する 1 つのビデオ コール、またはそれぞれ 128 kbps の帯域幅を要求する 3 つのビデオ コールをサポートできます）。

（注） コール アドミッション制御は、同じロケーション内のデバイス間のコールには適用されません。

あるロケーションから他のロケーションにコールが発信されると、Unified CM は、両方のロケーションから適切な帯域幅を差し引きます。たとえば、2 つのロケーション間の G.729 コールによって、Unified CM は、両方のロケーションで使用可能な帯域幅から 24 kbps を差し引きます。コールが完了すると、Unified CM は、帯域幅を差し引かれたロケーションに帯域幅を戻します。いずれかの支店ロケーションで十分な帯域幅がない場合、コールは Unified CM によって拒否され、発信者はネットワーク ビジー トーンを受け取ります。発信側デバイスが、ディスプレイを備えた IP Phone である場合、そのデバイスには、「Not Enough Bandwidth」というメッセージも表示されます。

サイト間コールがコール アドミッション制御によって拒否された場合、Unified CM は Automated Alternate Routing（AAR）機能を使用して、公衆網接続を通じて宛先にコールを自動的に再ルーティングできます。AAR 機能の詳細については、「Automated Alternate Routing」（P.9-103）を参照してください。

（注）　AAR が呼び出されるのは、帯域幅が不足しているために、ロケーション ベースのコール アドミッション制御によってコールが拒否される場合だけです。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Unified CM に登録されない状態になった場合には、AAR は呼び出されません。このような場合、コールは着信側デバイスの [Call Forward No Answer] フィールドで指定されている宛先に転送されます。

ロケーションおよびリージョンの設定

ロケーションは、リージョンとともに、ネットワーク リンクの特性を定義します。リージョンではリンクで使用する圧縮またはビット レートのタイプ（8 kbps または G.729、64 kbps または G.722/G.711 など）を定義し、ロケーションではリンクに使用できる帯域幅の容量を定義します。システム内の各デバイスを（デバイス プールを使用して）リージョンに割り当て、（デバイス プールまたはデバイス自体に直接設定した値を使用して）ロケーションに割り当てます。

Unified CM では、*ロケーション*を設定することにより、次の要素を定義できます。

- 物理的なロケーション（支社など）。
- WAN 内のロケーションとの間でやり取りされる音声コールおよび FAX コールに利用できる帯域幅。Unified CM では、ロケーションベースのコール アドミッション制御にこの帯域幅値が使用されます。
- WAN 内のロケーションとの間でやり取りされるコールに利用できるビデオ帯域幅。Unified CM では、ロケーションベースのコール アドミッション制御にこの帯域幅値が使用されます。
- ロケーション間の RSVP コール アドミッション制御の設定（可能な設定は、[No Reservation]、[Optional]、[Optional (Video Desired)]、[Mandatory]、および [Mandatory (Video Desired)] です）。

Unified CM では、*リージョン*を設定することにより、次の要素を定義できます。

- リージョン内コールに使用する最大オーディオ ビット レート設定（Max Audio Bit Rate）
- リージョン間コールに使用する最大オーディオ ビット レート設定（Max Audio Bit Rate）
- リージョン内コールおよびリージョン間コールに使用するビデオ コールの最大ビット レート設定（音声を含む）（Max Video Call Bit Rate（Includes Audio））
- リージョン間コールのリンク損失タイプ（可能なリンク損失タイプは [Low Loss] および [Lossy] です）。

Unified CM によるロケーションおよびリージョンのサポート

Cisco Unified Communications Manager は、Cisco MCS-7845 サーバで 2000 のロケーションと 2000 のリージョンをサポートします。最大 2000 のロケーションおよびリージョンを配置するには、[Clusterwide Parameters] >（[System] > [Location and Region]）および [Clusterwide Parameters] >（[System] > [RSVP]）の設定メニューで次のサービス パラメータを設定する必要があります。

- Default Intraregion Max Audio Bit Rate
- Default Interregion Max Audio Bit Rate
- Default Intraregion Max Video Call Bit Rate (Includes Audio)

- Default Interregion Max Video Call Bit Rate (Includes Audio)
- Default Intraregion and Interregion Link Loss Type

リージョンを追加するときは、[Max Audio Bit Rate] と [Max Video Call Bit Rate] の値として [Use System Default] を選択してください。RSVP コール アドミッション制御を使用している場合は、[RSVP Setting] パラメータにも [Use System Default] を選択します。

個々のリージョンおよびロケーションについてこれらの値をデフォルトから変更すると、サーバの初期化とパブリッシャのアップグレードにかかる時間に影響します。合計 2000 のリージョンと 2000 のロケーションを使用する場合、そのうち最大 200 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。合計 1000 以下のリージョンおよびロケーションを使用する場合、そのうち最大 500 のリージョンおよびロケーションでデフォルト以外の値を使用するように変更できます。表 11-3 は、これらの制限を要約したものです。

表 11-3　デフォルト以外の値を使用できるリージョンおよびロケーションの数

デフォルト以外の値を使用するリージョンおよびロケーションの数	リージョンの最大数	ロケーションの最大数
0 ～ 200	2000	2000
200 ～ 500	1000	1000

（注） [Max Audio Bit Rate] は、音声コールと FAX コールの両方に使用されます。リージョン間コーデックとして G.729 を使用する場合、FAX コールには T.38 FAX リレーを使用してください。WAN で FAX パススルーを使用する場合は、[Interregion Max Audio Bit Rate] をデフォルト値から 64 kbps（G.722 または G.711）に変更するか、デフォルト値でない 64 kbps（G.722 または G.711）ビット レートを使用する各ロケーションに FAX マシンのリージョンを追加します（表 11-3 内の制限に従います）。

（注） 使用している MCS モデルに関係なく、多数のリモート サイトを包含する設計には、Unified CM クラスタのスケーラビリティ（リージョン、ロケーション、ゲートウェイ、メディア リソースなど）に影響する可能性ある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニアが常に Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、それらの設計をすべて検証する必要があります。サイジング ツールを使用して、設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定します。

Cisco IOS ゲートキーパー ゾーン

Cisco IOS ゲートキーパーは、Cisco Unified CM、Cisco Unified Communications Manager Express（Unified CME）、レガシー PBX に接続されている H.323 ゲートウェイなどのデバイス間で、コール ルーティングとコール アドミッション制御を提供できます。H.323 Registration Admission Status（RAS）プロトコルを使用してこれらのデバイスと通信し、コールをネットワークにルーティングします。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、単純なハブアンドスポーク トポロジに制限されます。トポロジの詳細な例については、「コール アドミッション制御の設計上の考慮事項」（P.11-69）の項を参照してください。

使用可能な Cisco IOS ゲートキーパー プラットフォームおよび各プラットフォームでサポートされている機能のリストを見るには、次の Web サイトで入手可能な『*Cisco IOS H323 Gatekeeper Data Sheet*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4139/data_sheet_c78_561921.html

Cisco IOS ゲートキーパーのコール アドミッション制御機能は、ゲートキーパーの ゾーンの概念に基づいています。ゾーンは、エンドポイント、ゲートウェイ、マルチポイント コントロール ユニット（MCU）などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。ローカル ゾーンは、当該のゲートキーパーがアクティブに処理しているゾーンです。つまり、このゾーンに割り当てられている H.323 デバイスは、すべて当該ゲートキーパーに登録されます。

複数のゲートキーパーを同一ネットワークに配置している場合、ゾーンがローカル ゾーンとして設定されるのは、1 つのゲートキーパー上のみです。他のゲートキーパーでは、このゾーンはリモート ゾーンとして設定されます。この設定によって、あるゾーンが宛先になっているコールを、そのゾーンを「所有」しているゲートキーパー（つまり、そのゾーンがローカル ゾーンとして設定されているゲートキーパー）に転送するようにゲートキーパーに指示しています。

ゲートキーパーの設定の詳細については、次の Web サイトから入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/voice/h323/configuration/guide/15_0/vh_15_0_book.html

すべてのアクティブなコールに対してゲートキーパーによって差し引かれる帯域幅の値は、レイヤ 2、IP、および RTP のオーバーヘッドを除いた、コールのビット レートの倍です。たとえば、64 Kbps を使用する G.711 音声コールは、ゲートキーパーでは 128 Kbps と認識され、384 Kbps のビデオ コールは 768 Kbps と認識されます。表 11-4 に、一般に利用されているいくつかのコール ビット レートにおいて、ゲートキーパーが使用する帯域幅の値を示します。

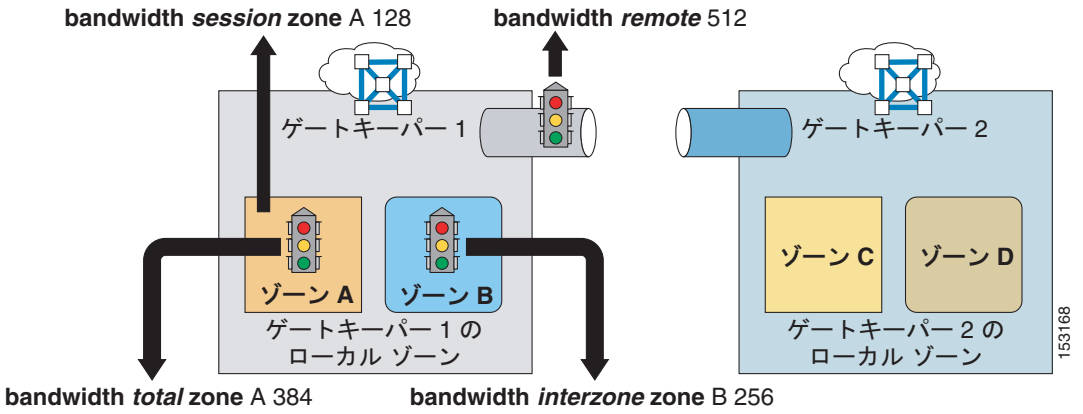
表 11-4　さまざまなコール ビット レートにおけるゲートキーパーの帯域幅設定

コールのビット レート	ゲートキーパーの帯域幅の値
G.711 音声コール（64 Kbps）	128 kbps
G.729 音声コール（8 Kbps）	16 kbps
128 Kbps ビデオ コール	256 kbps
384 Kbps ビデオ コール	768 kbps
512 Kbps ビデオ コール	1024 kbps
768 Kbps ビデオ コール	1536 kbps

（注） コール ARQ（アドミッション要求）に対する帯域幅計算には、RTP ヘッダー圧縮（cRTP）やその他のトランスポートのオーバーヘッドは含まれません。インターフェイス キューのプロビジョニング方法の詳細については、「帯域幅のプロビジョニング」（P.3-47）を参照してください。

実際のネットワークでの **bandwidth** コマンドの利用方法を深く理解するために、図 11-10 に示す例について考えます。

図 11-10　Cisco IOS ゲートキーパーの bandwidth コマンドの例



すべてのコールが G.711 コーデックを使用する音声専用コールであるとすると、図 11-10 に示すコンフィギュレーション コマンドについて、次のことがいえます。

- 1 回のコールに対してゾーン A で任意のデバイスによって要求される帯域幅の最大量は、128 kbps です。つまり、64 kbps よりも高いビット レートのコーデックを使おうとするコールは拒否されます。
- ゾーン A のデバイスに関係するすべてのコール（ゾーン内、またはその他のゾーンとの間）で使用される帯域幅の最大量は、384 kbps です。つまり、ゾーン A のデバイスに関係する最大 3 つのアクティブなコールが存在できます。
- ゾーン B のデバイスとその他のゾーンのデバイス間のすべてのコールによって使用される帯域幅の最大量は、256 kbps です。つまり、ゾーン B のデバイスと、ゾーン A、C、および D のデバイスの間には、最大 2 つのアクティブなコールが存在できます。
- ゲートキーパー GK 1 で登録されたデバイスと、その他のゲートキーパーで登録されたデバイスとの間のすべてのコールで使用される帯域幅の最大量は、512 kbps です。つまり、ゾーン A およびゾーン B のデバイスと、ゾーン C および ゾーン D のデバイスの間には、最大 4 つのアクティブなコールが存在できます。

リソース予約プロトコル（RSVP）を使用した Unified Communications アーキテクチャ

ここでは、Resource Reservation Protocol（RSVP; リソース予約プロトコル）をコール アドミッション制御メカニズムとして実装するさまざまな Unified Communications アーキテクチャを取り上げます。RSVP の紹介とプロトコル アーキテクチャの概要、RSVP とサービス品質の概念、アプリケーション ID、およびインフラストラクチャ設計上の考慮事項と推奨事項の概要から始めます。

次に、単一クラスタ Unified CM 環境での Unified CM RSVP 対応ロケーションについて説明します。具体的には、関与するコンポーネントとそのコンポーネントのプロビジョニング、Unified CM による RSVP ポリシーとアプリケーション ID の使用、および静的ロケーションに基づいてコール アドミッション制御から移行するための推奨戦略を取り上げます。

続いて、分散型コール処理アーキテクチャについて説明します。RSVP SIP プレコンディションの説明から始まり、その機能の概要と、その機能が Unified CM、Unified CME、SIP-TDM Cisco IOS ゲートウェイなどさまざまな呼制御アプリケーション間で RSVP レイヤおよび呼制御レイヤを同期する仕組みについて説明します。次に、機能の注意事項や設計の推奨事項と考慮事項を含め、RSVP SIP プレコンディションに関して各呼制御アプリケーションを詳しく説明します。

リソース予約プロトコル（RSVP）

リソース予約プロトコル（RSVP）は、異種ネットワークにわたってエンドツーエンドの QoS を動的にセットアップするための、実質上最初の業界標準プロトコルです。RSVP は IP を基盤として機能し、IETF によって RFC 2205 で最初に導入されました。RSVP を使用すると、アプリケーションがネットワーク帯域幅を動的に予約できます。RSVP を使用すると、ネットワークを流れるデータ フローに関して、アプリケーションが一定レベルの QoS を要求できます。分散型ネットワークに対応し、動的に機能する性質を持っているため、RSVP はあらゆるネットワーク トポロジにわたって帯域幅を予約できます。つまり、音声コールとビデオ コールにトポロジ対応コール アドミッション制御を提供できます。

この項では、RSVP プロトコルの原理と、このプロトコルと WAN インフラストラクチャとの対話を中心に、特に QoS について説明します。RSVP に基づくコール アドミッション制御の目的とメカニズムについては、この章の他の項で説明します。

この項では、次のトピックを扱います。

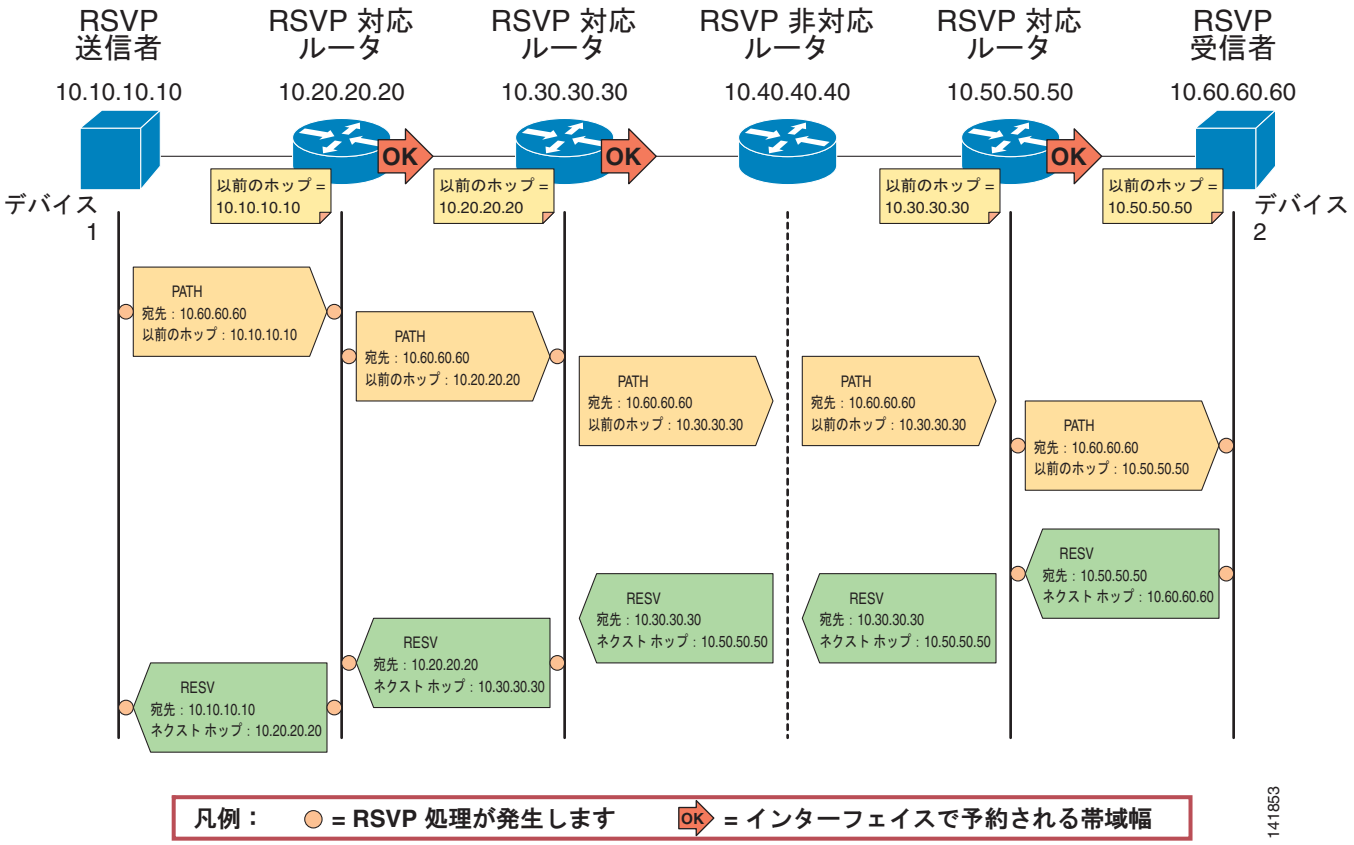
RSVP の原理

RSVP は、ネットワーク全体で、指定されたデータ フローのリソース予約を行います。RSVP 予約は単方向です。このため、2 つの RTP ストリームを含む単一の音声コールでは、各 RTP ストリームに 1 つずつの 2 つの RSVP 予約が生成されます。リソース予約は、データ フローの発信元デバイスと宛先デバイス間でシグナリング メッセージを交換することで作成され、メッセージはパスに沿って介在するルータにより処理されます。RSVP シグナリング メッセージは、IP ヘッダーのプロトコル番号が 46 に設定されている IP パケットで、既存のルーティング プロトコルに従ってネットワーク内でルーティングされます。

パス上のすべてのルータで RSVP をサポートする必要はありません。このプロトコルは、RSVP に対応していないノードでは透過的に動作するように設計されています。各 RSVP 対応ルータで、RSVP プロセスがシグナリング メッセージを代行受信し、帯域幅リソースを「予約」するために、データ フローに含まれるルータの発信側インターフェイスの QoS マネージャと対話します。パスの任意の場所で、使用可能なリソースがそのデータ フローには不十分な場合、ルータは予約要求を発信したアプリケーションに、失敗を示す信号を返します。

RSVP シグナリングの原理は、図 11-11 に示す例で説明できます。この図では、デバイス 1（IP アドレス 10.10.10.10）からデバイス 2（IP アドレス 10.60.60.60）に流れるデータ ストリーム用に、アプリケーションがネットワーク リソースを予約しようとします。

図 11-11　RSVP Path と Resv メッセージ フローの例



次の手順では、図 11-11 の例に示すように、単一データ フローとしての RSVP シグナリング プロセスついて説明します。

1. デバイス 1 にあるアプリケーションが Path という RSVP メッセージを発信します。このメッセージは、予約を要求するデータ フローと同じ宛先 IP アドレス（10.60.60.60）に送信され、IP ヘッダーの「router alert」オプションがオンにされて送信されます。Path メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。宛先 IP アドレス、プロトコル番号、および UDP/TCP ポートで構成され、RSVP 対応ルータでデータ フローを識別するために使用します。
   - 「sender T-Spec」（トラフィック仕様）オブジェクト。予約が要求されたデータ フローの特性を示します。T-Spec は基本的に、特定のコーデックを使用するコール フローに必要な最大 IP 帯域幅を定義します。T-Spec は通常、データ フローの平均ビット レート、ピーク レート、およびバースト サイズの値を使用して定義されます。T-Spec については、この章の後半で詳しく説明します。
   - 「P Hop」（以前のホップ）オブジェクト。Path メッセージを最後に処理したルータ インターフェイスの IP アドレスが含まれます。この例では、P Hop は最初にデバイス 1 で 10.10.10.10 に設定されます。
2. 「router alert」オプションによって、Path メッセージは RSVP 対応ルータ（図 11-11 の 10.20.20.20）の CPU が代行受信し、RSVP プロセスに送信されます。RSVP は、このデータ フローのパス状態を作成し、Path メッセージに含まれる session オブジェクト、sender Tspec オブジェクト、および P Hop オブジェクトの値を格納します。次に、P Hop 値を発信インターフェイスの IP アドレス（この例では 10.20.20.20）で置き換えて、メッセージをダウンストリームに転送します。

3. 同様に、次の RSVP 対応ルータ（図 11-11 の 10.30.30.30）の CPU が Path メッセージを代行受信します。パス状態を作成し、P Hop 値を 10.30.30.30 に変更した後、このルータもメッセージをダウンストリームに転送します。
4. 次に、Path メッセージは、RSVP 非対応ルータ（図 11-11 の 10.40.40.40）に到達します。このルータでは RSVP が有効でないため、このメッセージは他の IP パケットと同様に、追加の処理やメッセージ オブジェクトの内容の変更は行われずに、既存のルーティング プロトコルに従ってルーティングされます。
5. その結果、Path メッセージは RSVP 対応ルータ（10.50.50.50）に転送され、ここでメッセージが処理され、対応するパス状態が作成され、メッセージがダウンストリームに転送されます。このルータで記録される P Hop には、ネットワーク パスの最後の RSVP 対応ルータの IP アドレス（この例では 10.30.30.30）がまだ含まれていることに注意してください。
6. デバイス 2 の RSVP 受信側は、P Hop 値が 10.50.50.50 の Path メッセージを受信します。ここで、Resv というメッセージを発信することによって、実際の予約が開始されます。このため、RSVP は受信側開始プロトコルと呼ばれます。Resv メッセージは、セッションのデータ フローの逆方向のパスに従って、予約要求を受信側から送信側にホップごとに伝達します。各ホップでの Resv メッセージの IP 宛先アドレスは、パス状態から取得した直前のホップ ノードの IP アドレスです。したがって、この例では、デバイス 2 は宛先 IP アドレスが 10.50.50.50 の Resv メッセージを送信します。Resv メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。データ フローの識別に使用します。
   - 「N Hop」（次のホップ）オブジェクト。メッセージを生成したノードの IP アドレスが含まれます。この例では、N Hop は最初にデバイス 2 で 10.60.60.60 に設定されます。
7. 10.50.50.50 の RSVP 対応ルータがこのデータ フローの Resv メッセージを受信すると、受信した session オブジェクトを使用してパス状態情報と照合され、次の基準に基づいて予約要求を受け入れることができるかどうかが確認されます。
   - ポリシー制御：このユーザやアプリケーションが、この予約要求を行えるかどうか。
   - アドミッション制御：関連する発信インターフェイスに、この予約要求を満たせるだけの帯域幅リソースがあるかどうか。
8. この例では、10.50.50.50 でポリシー制御とアドミッション制御の両方が成功したとします。つまり、このセッションのパス状態の Tspec で提供される帯域幅は、発信インターフェイス（データ フローと同じ方向で、デバイス 1 からデバイス 2）で予約され、対応する「予約状態」が作成されるものとします。次に、10.50.50.50 のルータは、このセッションの P Hop に格納されている宛先 IP アドレス（10.30.30.30）にユニキャスト IP パケットとして送信することによって、Resv メッセージをアップストリームに送信できます。N Hop オブジェクトも、値 10.50.50.50 に更新されます。
9. 次に、Resv メッセージは、10.40.40.40 の RSVP 非対応ルータを通過します。ここでは、他の IP パケットと同様に、宛先 10.30.30.30 にルーティングされます。このメカニズムによって、RSVP シグナリングは、RSVP に対応していないノードが含まれる異種ネットワークで機能します。
10. 10.30.30.30 の RSVP 対応ルータは、Resv メッセージを受信し、ステップ 7 および 8 で説明したメカニズムに従って処理します。このホップでも、ポリシー制御およびアドミッション制御が成功したとします。帯域幅が発信インターフェイスで予約され、Resv メッセージが前のホップ（この例では 10.20.20.20）に送信されます。
11. 10.20.20.20 のルータで同様の処理が行われた後、Resv は最終的に RSVP 送信側のデバイス 1 に到達します。これによって、要求元のアプリケーションに対して、エンドツーエンド予約が確立され、ネットワークのすべての RSVP 対応ルータで、帯域幅がこのデータ フロー用に確保されたことが示されます。

この例では、2 つの主な RSVP シグナリング メッセージである Path と Resv がネットワークを通過し、予約を確立する方法を示しました。RSVP 標準では、エラー状態、予約失敗、およびリソースの解放を扱うその他のメッセージがいくつか定義されています。特に、ResvErr メッセージは、要求されたリソースがネットワーク上のいずれかでポリシー制御またはアドミッション制御によって予約できなかっ

たことを示すために使用されます。たとえば、図 11-11 のノード 10.50.50.50 でアドミッション制御が失敗した場合、このノードは失敗の原因を示す ResvErr メッセージをデバイス 2 に送信して、アプリケーションがこの通知を受け取ります。

もう 1 つの RSVP プロトコルの重要な点として、ソフト状態アプローチの採用があります。これは、同一の Path メッセージと Resv メッセージを送信することによって、ネットワーク上でセッションごとにパス状態と予約状態をアプリケーションで定期的にリフレッシュする必要があるという意味です。あるセッションについて、一定の時間、ルータがリフレッシュ メッセージを受信しない場合、対応する状態が削除され、予約されたリソースが解放されます。これによって、RSVP は動的に、リンク障害によるネットワーク トポロジの変更またはルーティングの変更に対応できます。予約では、単純に、ルーティング プロトコルの決定に従って新しいルートのフローが開始され、古いルートの予約はタイムアウトして最終的に削除されます。

MPLS ネットワークにおける RSVP

一部の MPLS サービス プロバイダー ネットワークでは、カスタマー エッジ（CE）とプロバイダー エッジ（PE）間のリンクで使用する IP アドレスは、その他の MPLS ネットワークには配布されません。そのため、サブネットは PE にローカルにとどまり、PE を越えてアドバタイズされることはありません（これらが一意ではなく、他の場所でも再利用されるためです）。これにより、RSVP メッセージの P Hop（以前のホップ）値がネットワーク内で不明であるため、RSVP が RSVP メッセージを転送できない状況が発生します。図 11-12 は、このタイプの状況を示しています。

図 11-12　　P Hop 上書きしない MPLS 上での RSVP

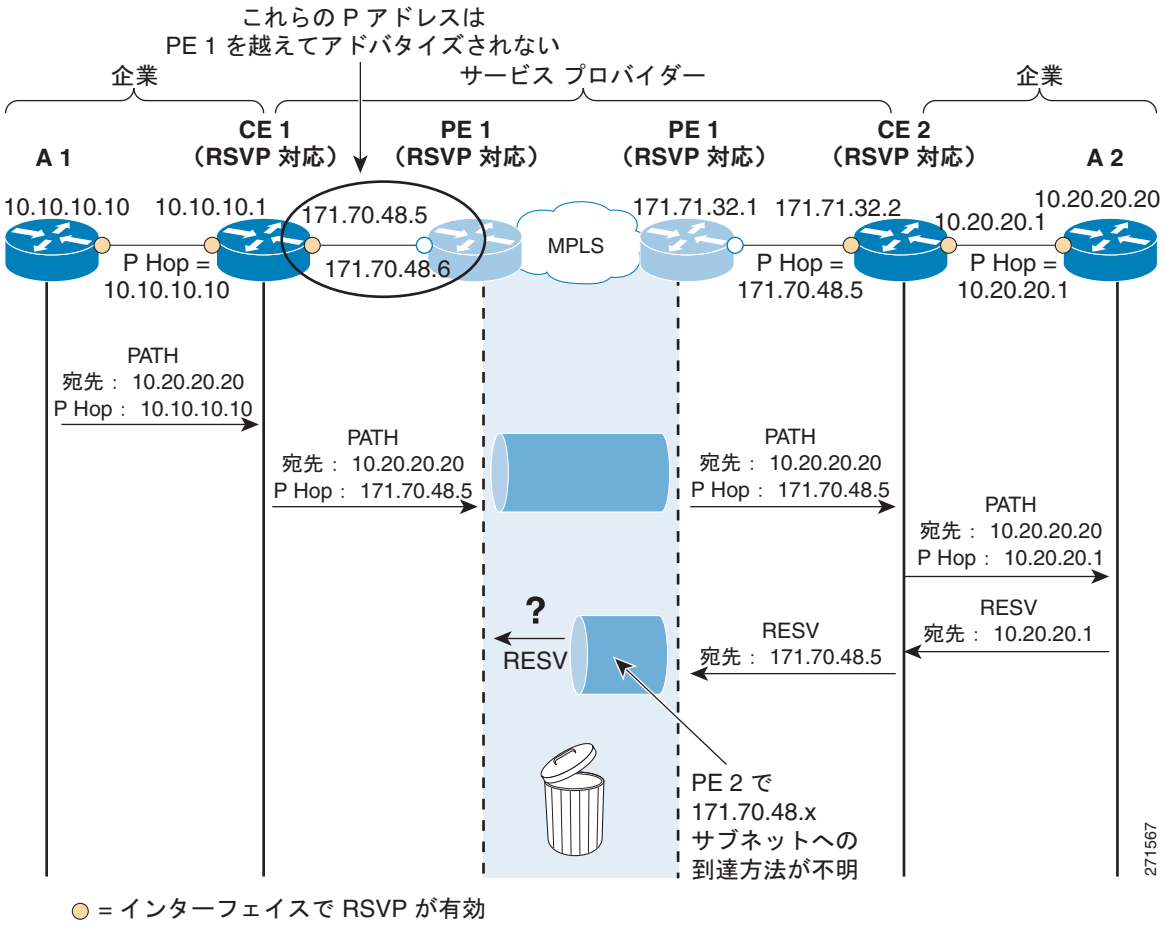


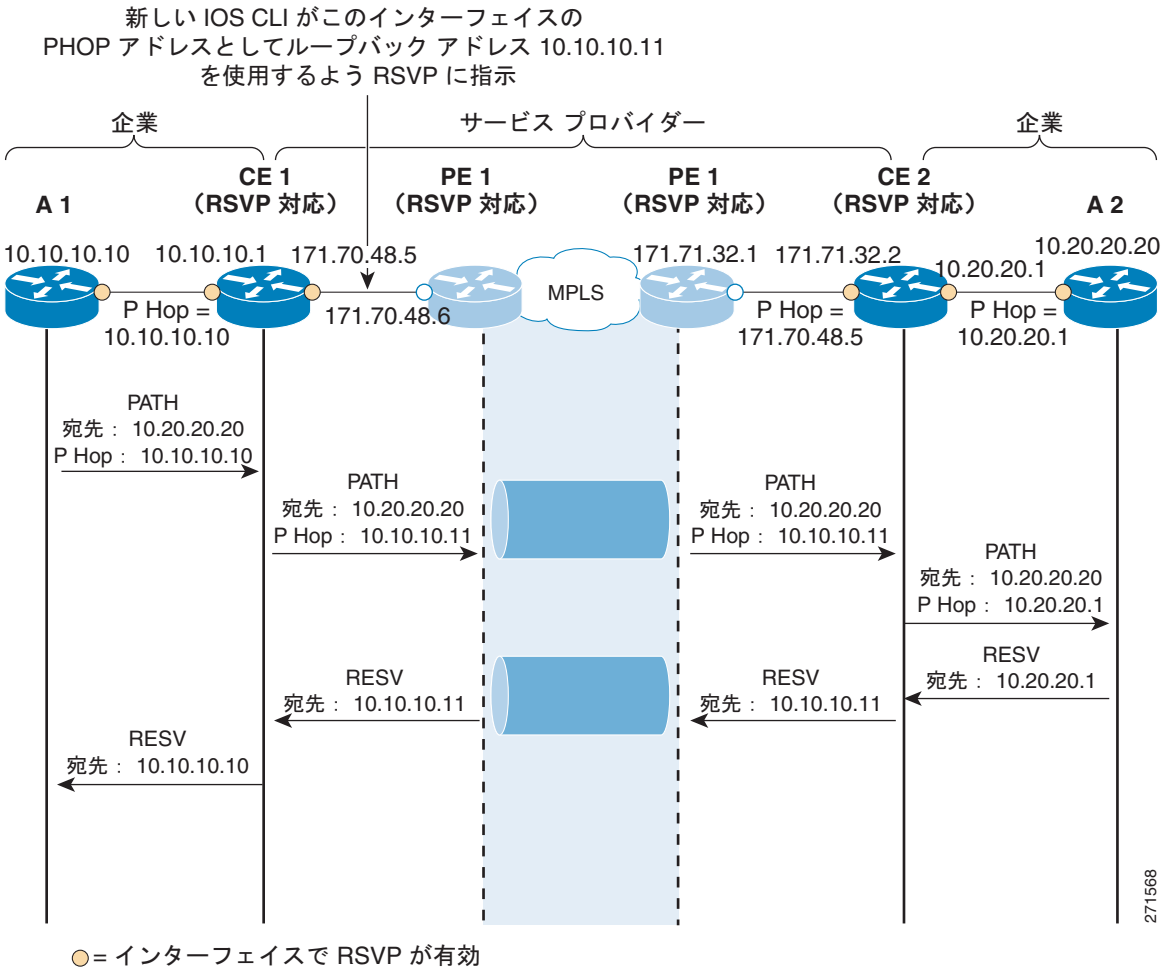
図 11-12 は、企業ネットワークとサービス プロバイダーの MPLS ネットワークを示しています。CE1 と CE2 は RSVP 対応、PE1 と PE2 は RSVP 非対応です。RSVP Path メッセージには P Hop オブジェクトが含まれています。このオブジェクトは、すべての RSVP ホップで書き直されます。これは、CE1 が以前の RSVP ホップ（または P Hop）であることを示すために、RSVP ルータ（たとえば、CE1）が Path メッセージを、次の RSVP ルータ（たとえば、CE2）に送信できるようにするためです。この情報は、対応する Resv メッセージをホップバイホップでアップストリームの送信側に転送するために CE2 によって使用されます。

Cisco IOS では、RSVP ルータは、常に P Hop アドレスを Path メッセージを送信する出力インターフェイスの IP アドレスに設定します。一部の CE1 の IP アドレスが到達可能であるにもかかわらず、その出力インターフェイスの IP アドレスが、リモートの RSVP ルータ CE2 から到達できない場合があります。その結果、CE2 によって生成された対応する Resv メッセージが CE1 に到達しないため、予約が確立されなくなります。

コールが A1 から A2 に発信されると、A1 は RSVP セッションをセットアップしようとして、Path メッセージを CE1 に送信することで開始します。A1 は、発信インターフェイスの IP アドレス（この場合、10.10.10.10）の Path メッセージ内の P Hop オブジェクトを取り込みます。次に、CE1 は、Path メッセージを受信し、それを処理し、対応するパス状態を作成し、その出力インターフェイスの IP アドレス（171.70.48.5）を持つメッセージの P Hop フィールドを更新します。このアドレスは、ルーティング可能な IP アドレスではないため、Path メッセージをダウンストリームに転送します。この Path メッセージは、サービス プロバイダーのネットワークを通り抜け、CE2 によって処理されます。Path メッセージを受信した後、CE2 は、P Hop オブジェクトの IP アドレス（CE1 の出力インターフェイスの IP アドレス）を記録し、Path メッセージをダウンストリームの A1 に転送します。A1 は、Path メッセージを記録および処理して、RSVP メッセージを CE2 に発信します。CE2 は、RSVP メッセージを処理し、それ自身の RSVP メッセージをアップストリームの CE1 に送信します。ただし、CE2 がこの Resv メッセージに対して応答する場合、CE2 は CE1 から受信した Path メッセージから以前に記録した IP アドレスに送信しようとします。この IP アドレス（171.70.48.5）は CE2 からルーティングできないので、Resv メッセージは失敗し、この結果予約試行は失敗します。

この動作を解決するため、Cisco IOS Release 12.4(20)T には Previous Hop Overwrite（以前のホップの上書き）という機能を導入しています。P Hop の上書きは、カスタマーの VPN で到達可能なルータ上の他のインターフェイスからの IP アドレスを含む Path メッセージ内の Hop オブジェクトを CE が取り込むメカニズムです。この方法で、Resv メッセージは送信側に戻る経路を見つけ、予約を確立できます。P Hop の上書きメカニズムは、図 11-13 に示されています。

図 11-13　Cisco IOS 12.4(20)T における RSVP P Hop の上書き機能



RSVP（TSpec）におけるデータ フロー特性の説明

RSVP は、音声またはビデオだけに限らず、レイヤ 2 テクノロジーの広範囲にわたる任意のトラフィック フローの Quality of Service（QoS）の要求をサポートするように設計されました。このような処理を実現するために、RSVP は、QoS を要求しているトラフィック フローを詳細に記述して、中間ルータが正しくアドミッションを決定できるようにする必要があります。

RSVP セッションのデータ フローの帯域幅の要件は、Path メッセージに含まれる TSpec（トラフィック仕様）の送信側によって特性が設定され、Resv メッセージの受信側によって送信される RSpec（予約仕様）にミラーリングされます。TSpec は、ネットワークを経由して、すべての中間ルータと宛先エンドポイントに転送されます。中間ルータはこのオブジェクトを変更せず、オブジェクトは最終受信者へ無変更のまま送信されます。

TSpec オブジェクトには、次の要素が含まれています。

- AverageBitRate（kbps）
- BurstSize（バイト）
- PeakRate（バイト）

オーディオ TSpec

オーディオ フローでは、TSpec の計算が次の測定値を指定します。

- AverageBitRate（kbps）：IP オーバーヘッドを含む
- BurstSize（バイト）：この値は、バースト内のパケットのサイズにパケット数を掛けて算出されます。オーディオ フローでは、バーストは通常 1 ～ 2 を指定します。
- PeakRate（バイト）：ピーク レート（バイト単位）は、エンドポイントが任意の時間に送信する最大バイト/秒を指します。オーディオ ストリームの場合と同様に、バーストが小さい場合、ピーク レートは tokenRate の 1.1（または 1.2）倍として計算できます。

コールが応答されたときに、帯域幅予約を上方に調整するのを回避するために、Cisco Unified CM は、各リージョン コーデックに対する最大帯域幅をコール セットアップ時間で予約します。次に、Unified CM は、コールが応答されたときに、接続された当事者のメディア能力に基づく帯域幅を変更または調整します。

Unified Communications 対応 RSVP の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

（注） この項では、RSVP の原理とメカニズムの概要を中心に説明しています。プロトコルの動作および拡張の詳細、完全なメッセージ形式、および他のプロトコルとの対話については、http://www.ietf.org で入手可能な RSVP に関する多くの RFC ドキュメントを参照してください。

WAN ルータでの RSVP と QoS

RSVP は、長い間 Cisco ルータでサポートされていましたが、このマニュアルで推奨するほとんどの設定は、Cisco IOS Release 12.2(2)T で最初に導入された RSVP Scalability Enhancements 機能に基づいています。

各 Cisco IOS ルータ インターフェイス上で、次の Cisco IOS コマンドをインターフェイス コンフィギュレーション モードで発行すると、RSVP を有効にし、RSVP で制御できる帯域幅の最大量を定義できます。

```
ip rsvp bandwidth [interface-kbps] [single-flow-kbps]
```

interface-kbps パラメータには、RSVP が所定のインターフェイス上で予約できる帯域幅の上限を指定します。*single-flow-kbps* パラメータには、予約 1 つあたりの帯域幅の上限を指定します（要求している帯域幅がこれより大きいフローは、インターフェイス上に使用可能な帯域幅がある場合でも拒否されます）。

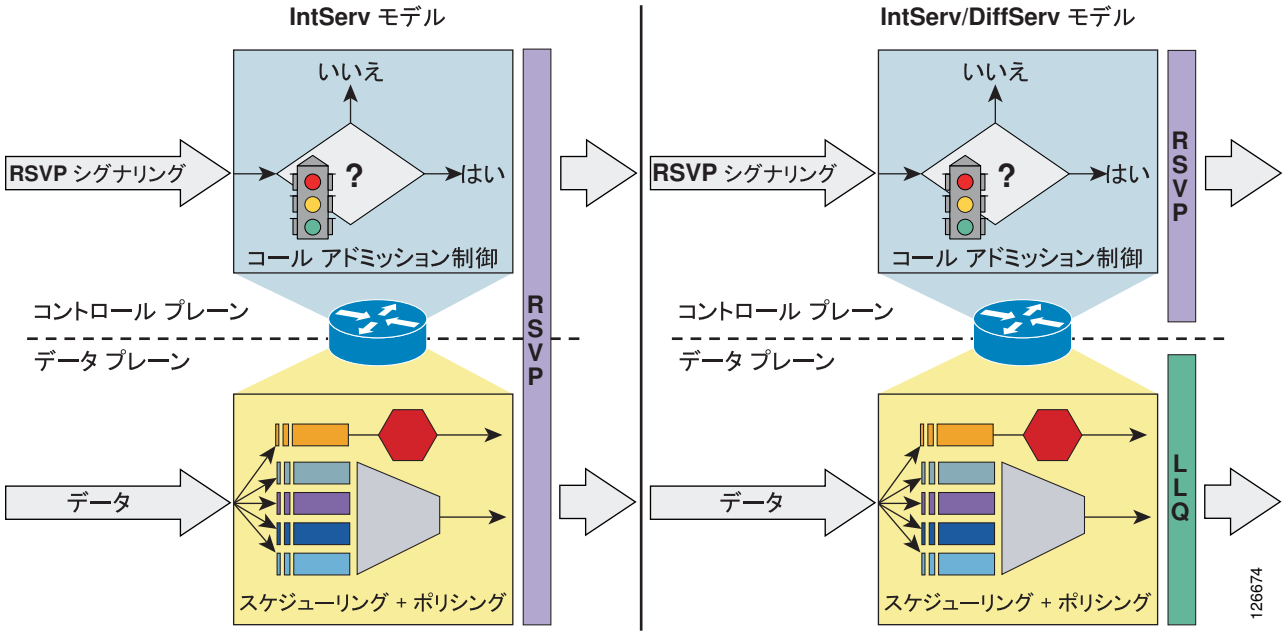
（注） ルータ インターフェイスで RSVP を有効にすると、そのルータで RSVP に対応していないその他のすべてのインターフェイスが、RSVP メッセージをドロップします。RSVP メッセージのドロップを防ぐには、RSVP シグナリングが通過すると予想されるすべてのインターフェイスで RSVP を有効にします。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。

Cisco IOS では、2 つの異なるモデルに従って運用するように RSVP を設定できます。RFC 2210 で記述されている統合サービス（IntServ）モデル、および RFC 2998 で記述されている統合サービス/ディファレンシエーテッド サービス（IntServ/DiffServ）モデルです。どちらの RFC ドキュメントも、次の IETF Web サイトで入手できます。

http://www.ietf.org

図 11-14 に、Cisco IOS ルータから見た、これらの 2 つのアプローチの相違点を示します。

図 11-14　2 つの RSVP 運用モデル：IntServ と IntServ/DiffServ

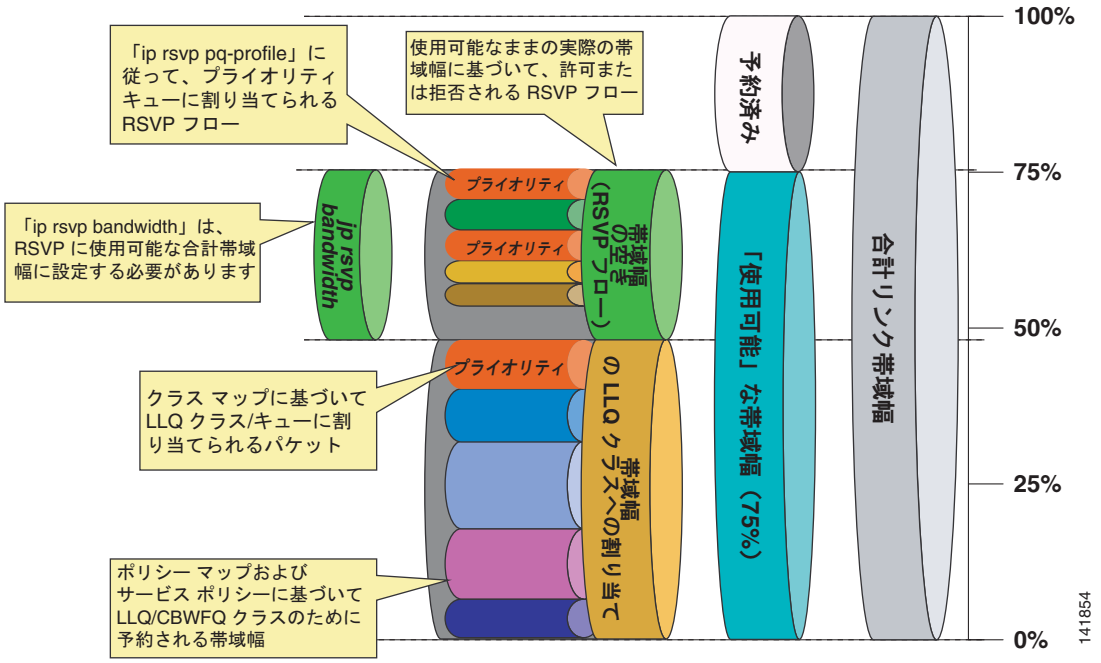


IntServ モデル

図 11-14 の左側に示すように、IntServ モデルの RSVP には、コントロール プレーンとデータ プレーンの両方が関係します。コントロール プレーンでは、RSVP が予約要求を許可または拒否します。データ プレーンでは、データ パケットを分類し、RSVP メッセージに含まれているトラフィック記述に基づいてポリシングし、適切なキューに入れます。RSVP が実行する分類は、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、およびプロトコル番号を構成している、5 つのタプルに基づいています。このモデルでは、ルータを通過するすべてのデータ パケットを RSVP で代行受信して、RSVP でこの 5 タプルを検査し、確立済みの予約と一致するかどうかを検索できるようにする必要があります。一致が見つかった場合は、その予約のトラフィック仕様に従って、パケットが RSVP によってスケジューリングされ、ポリシングされます。

図 11-15 で示すように、IntServ モデルを Low Latency Queuing（LLQ）と組み合せる場合、使用可能な帯域幅が RSVP と事前定義済みの LLQ キューで分割されます。RSVP は、RSVP 予約された帯域幅への入力基準を制御します。ポリシー マップは、事前定義済みキューの入力基準を制御します。

図 11-15　IntServ モデルと LLQ の組み合せ



Cisco IOS ルータで IntServ 運用モデルを使用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

```
ip rsvp resource-provider wfq [interface | pvc]
no ip rsvp data-packet classification
```

これらのコマンドがアクティブになっている場合、RSVP は、新しい予約を許可または拒否するとき、**ip rsvp bandwidth** コマンドで定義した帯域幅上限に加えて、使用可能な実際の帯域幅リソースも基準にします。たとえば、bandwidth ステートメントを持つ LLQ クラスが存在する場合は、RSVP 予約に割り当てることのできる帯域幅プールから、それらの量が減分されます。LLQ クラスは、設定すると帯域幅を静的に割り当てます。これに対して、RSVP は、予約要求を受信するまでは帯域幅を一切割り当てません。このため、LLQ クラスに割り当てられることがない使用可能インターフェイス帯域幅を適度に確保して、予約要求を受信したときに RSVP が使用できるようにしておくことが重要です。

リンクで QoS メカニズムに割り当てることができる合計最大帯域幅はリンク速度の 75% なので、リンク帯域幅の 33% を RSVP で許可されるフローに予約するには、LLQ クラスに割り当てる帯域幅がリンク帯域幅の（75 - 33）= 42% を超えないようにする必要があります。

このモデルでは、各種キューへのパケットの割り当てを RSVP が制御します。このため、次の Cisco IOS コマンドをインターフェイス コンフィギュレーション モードで使用すると、データ フロー T-Spec 値に基づくプライオリティ キュー（PQ）にフローを配置するかどうかを RSVP に通知するメカニズムを定義できます。

```
ip rsvp pq-profile [r [b [p-to-r]]]
```

Cisco IOS RSVP は、RSVP TSpec パラメータ *r*、*b*、および *p-to-r* を使用して、シグナリングの対象になっているフローが PQ 処理を必要とする音声フローかどうかを判定します。これらのパラメータは、次の値を表しています。

- *r* = トラフィックの平均レート（単位：バイト/秒）
- *b* = フローの最大バースト（単位：バイト）
- *p-to-r* = ピーク レートと平均レートの比率（単位：%）

特定のフローに関して RSVP TSpec メッセージで指定されているトラフィック特性が、Cisco IOS コマンドのパラメータ以下である場合、RSVP はフローを PQ に入れます。このコマンドにパラメータを指定しない場合は、一般に利用されている音声コーデック（G.711）の最大値である、次の値がデフォルトとして使用されます。

- *r* = 12,288 バイト / 秒
- *b* = 592 バイト
- *p-to-r* = 110%

IntServ/DiffServ モデル

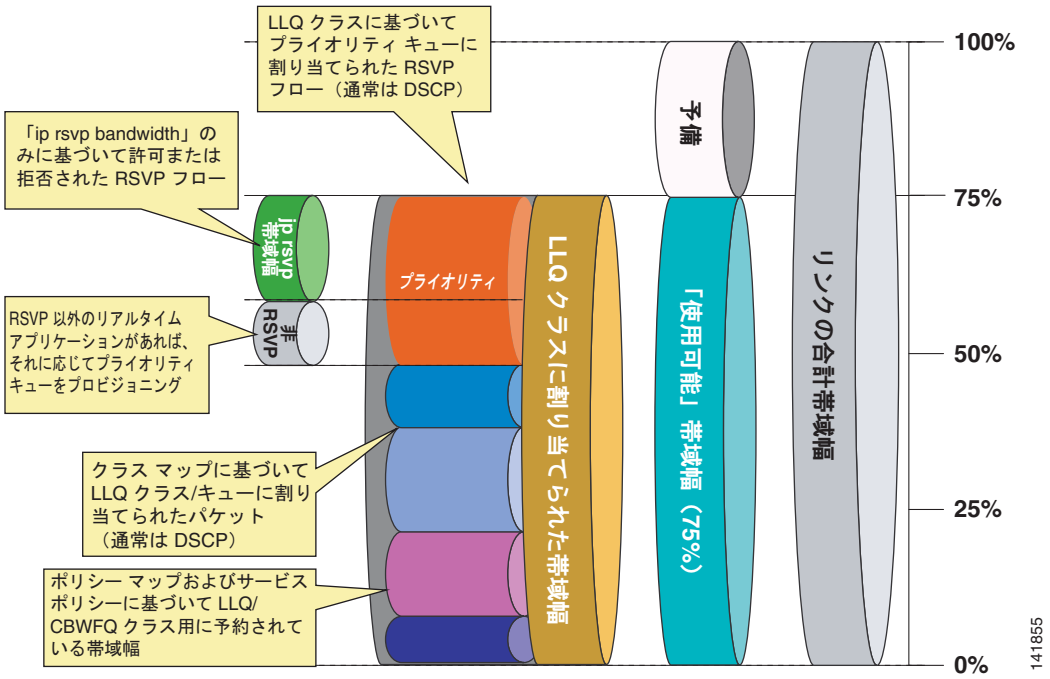
図 11-14 の右側に示すように、IntServ/DiffServ モデルの RSVP では、アドミッション制御を実行するコントロール プレーンだけが関係し、データ プレーンは関係しません。つまり、コール アドミッション制御機能は、スケジューリング機能およびポリシング機能とは独立しています。スケジューリングとポリシングは、事前定義済みのクラス マップ、ポリシー マップ、およびサービス ポリシーに従って、Low Latency Queuing（LLQ; 低遅延キュー）アルゴリズムによって実行できます。

このため、IntServ/DiffServ モデルでは、すでに QoS にディファレンシエーテッド サービス アプローチを使用しているネットワークに対して、RSVP コール アドミッション制御を追加できます。RSVP は、事前に設定された帯域幅量に基づいてコールを許可または拒否しますが、実際のスケジューリングは、各パケットの DSCP 値など、既存の LLQ 基準に基づいています。

図 11-16 に示すように、使用可能な帯域幅全体（リンク速度の 75%）を LLQ クラスに割り当てることができます。これが現在、一般的に行われている割り当てです。ポリシー マップは、各キューに許可されるトラフィックを定義します。RSVP は通常、優先トラフィック用に定義されている帯域幅の量までのフローを許可するように設定されますが、このモデルでは、RSVP がスケジューリングを調整しないため、事前定義済みのプライオリティ キューを超えて RSVP で許可されるトラフィックがドロップされたり、より低い優先度のキューにマッピングし直されたりする可能性があることに注意してください。

優先トラフィックを送信するすべてのアプリケーションが RSVP 対応の場合は、RSVP 帯域幅がプライオリティ キューのサイズと一致するように設定できます。一方、図 11-16 に示すように、優先トラフィックを送信する必要がある RSVP 未使用アプリケーション（Unified CM スタティック ロケーション、ゲートキーパーなど）がある場合は、非 RSVP メカニズムで制御される優先トラフィックと RSVP で制御される優先トラフィックの間で、プライオリティ キューが分割されます。非 RSVP アドミッション制御と RSVP アドミッション制御のメカニズムを組み合せた場合は、プライオリティ キューでオーバーサブスクリプションが発生しないように、割り当てられた量を超える帯域幅を使用しないでください。

図 11-16　RSVP との LLQ 帯域幅割り当て



Cisco IOS ルータで IntServ/DiffServ 運用モデルを使用するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

```
ip rsvp resource-provider none
ip rsvp data-packet classification none
```

これらのコマンドがアクティブになっている場合、RSVP は、**ip rsvp bandwidth** コマンドで定義された帯域幅上限だけに基づいて新しい予約を許可または拒否します。インターフェイス上で使用可能な実際の帯域幅リソースは考慮されません。許可された RSVP フローは、RSVP 以外の他のすべてのトラフィックと同じスケジューリング規則（たとえば、LLQ クラスとポリシー マップ）に従います。このため、RSVP 対応トラフィックを適切な DSCP 値を使用してマーキングし、対応する PQ または CBWFQ キューの帯域幅は、RSVP 対応トラフィックと他のすべてのトラフィックの両方に対応できるように設定することが重要です。

この運用モデルでは、RSVP はスケジューリング機能を制御しないため、**ip rsvp pq-profile** コマンドは非アクティブです。

RSVP のアプリケーション ID

アプリケーション ID（app-id）は、RSVP メッセージのポリシー要素に挿入可能な RSVP オブジェクトです。このオブジェクトは、RFC 2872 で説明されています。このポリシー オブジェクトは、アプリケーションを識別し、RSVP 予約要求に関連付けるために役立ちます。これによって、パスのルータは、アプリケーション情報に基づいて適切な決定ができます。

RSVP は、音声とビデオなど複数のアプリケーションのサポートに使用されるため、app-id が必要です。

app-id を使用しないと、RSVP でインターフェイスごとに設定できる帯域幅の値が 1 つだけになります。RSVP は、この帯域幅の上限に達するまで、要求を許可します。要求は区別されず、帯域幅が要求されているアプリケーション タイプも認識されません。その結果、RSVP が 1 つのタイプのアプリケーションだけに対応する要求を許可することで、許可されている帯域幅を使い切ってしまい、これによって、帯域幅が使用できずに後続のすべての要求を拒否してしまう可能性があります。この場合、少

数のビデオ コールが原因で、すべてまたはほとんどの音声コールが許可されないことがあります。たとえば、1000 ユニットを RSVP に割り当てた場合に、RSVP が 2 つの 384 kbps ビデオ コールで帯域幅のほとんどを使い切ってしまい、音声コール用の帯域幅がほとんど残らない可能性があります。

この問題は、個別のアプリケーションまたはトラフィック クラスごとに、個別の帯域幅上限を設定すると解決できます。アプリケーションごとに帯域幅を制限するには、アプリケーション帯域幅制限と対応する RSVP ローカル ポリシーをルータ インターフェイスに適用する必要があります。また、適切な帯域幅制限に対して許可できるように、アプリケーションを各予約要求フラグに割り当てる必要があります。

app-id は単一の情報ではなく、複数の可変長文字列になっています。RFC 2872 で説明されているように、オブジェクトには次の属性を含めることができます。

- アプリケーションの ID（APP）。この属性は必須です。
- グローバル一意識別情報（GUID）。オプションです。
- アプリケーションのバージョン番号（VER）。この属性は必須です。
- サブアプリケーション ID（SAPP）。任意の数のサブアプリケーション要素を含めることができます。オプションです。

次の例を参考にしてください。

- APP = AudioStream
- GUID = CiscoSystems
- VER = 5.0.1.0
- SAPP =（指定なし）

Unified CM がアプリケーション ID を使用する方法の詳細については、「RSVP アプリケーション ID と Unified CM」（P.11-47）を参照してください。

Cisco IOS の機能

この項では、Cisco Unified CM 8.5 以降のリリースを使用した配置の設計に利用される新しい Cisco IOS の機能について説明します。これらの機能は、Cisco IOS Release 15.1(3)T で新しく追加されており、利用するには正しいバージョンの Cisco IOS を使用することが重要です。

RSVP 入力コール アドミッション制御

「RSVP の原理」（P.11-18）の項で説明しているように、RSVP プロトコルでソース デバイスが宛先デバイスと通信するために要求するリソースが予約されます。この予約は単方向です。ソース デバイスは、要求されているリソースをアドバタイズするパス メッセージを送信します。パス メッセージを受信した後、宛先デバイスは予約メッセージによって応答します。RESV メッセージは、ソース デバイスと宛先デバイスの間の中間ノードをホップバイホップ（RSVP のみが認識するホップ）で通過し、これらのノードが要求されているフローにリソースを割り当て可能かを判断します。予約は宛先デバイスの方向にダウンストリームしながら発信インターフェイス（ストリームの方向に関する出力）のみのリソースに対しチェックされます。

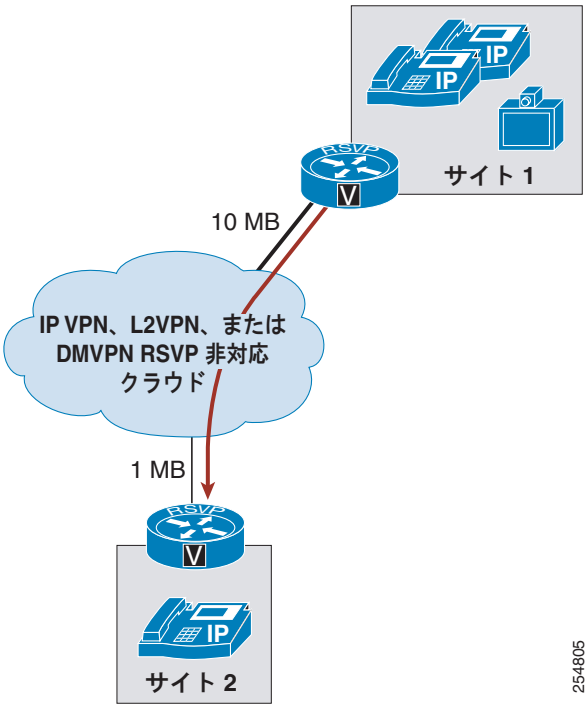
次のシナリオでは、RESV メッセージは、予約されたリソースに対してソース デバイスと宛先デバイス間の通信が保証されたことを示すものではありません。

2 つの RSVP 認識ルータ間の非対称リンク

図 11-17 では、パス メッセージは RSVP 非認識クラウドに 10 MB リンクを使用して入力され、RSVP 非認識クラウドから 1 MB リンクに出力されます。サイト 1 からサイト 2 へのストリームの流れでは、サイト 1 での RSVP 認識ルータの出力インターフェイスのみが考慮されます。ダウンストリームであ

るサイト 2 での 1 MB リンクは、予約の際は考慮されません。多くのシナリオでは、これは問題にはなりません。すべてのコールにはストリームが 2 つあり、反対方向のストリーム（サイト 2 からサイト 1 へ）にはサイト 2 RSVP 認識ルータの帯域幅が予約されるためです。

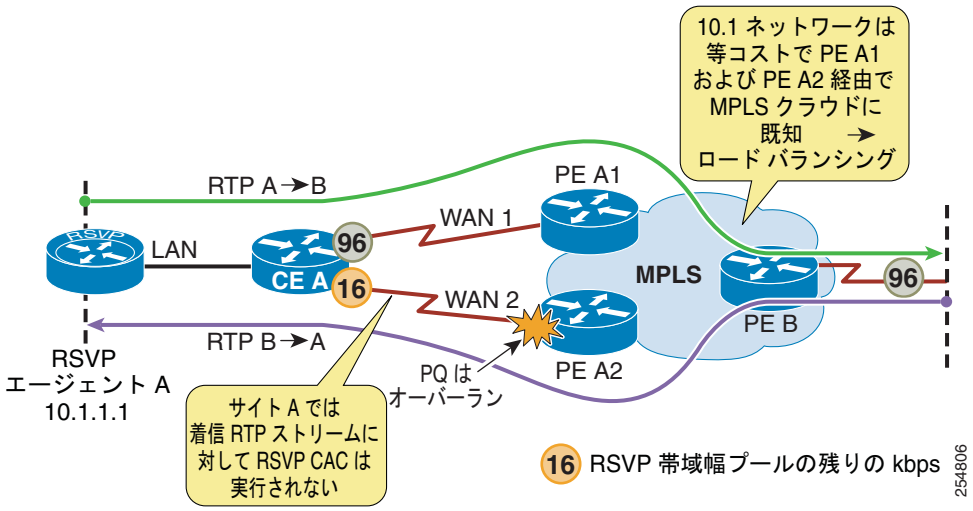
図 11-17　　RSVP 認識ルータ間の非対称リンク



ロード バランシング対応顧客機器（CE）などの非対称ルーティング パス

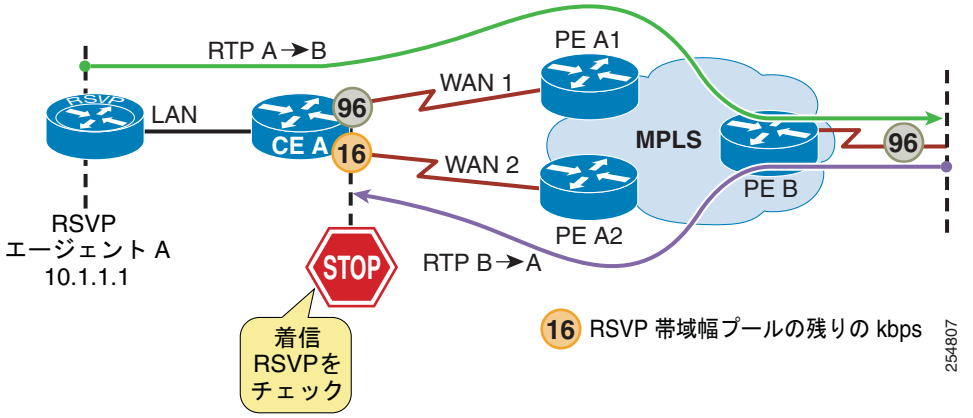
図 11-18 では、音声コール（2 ストリームで各方向について 1 つずつ）が RSVP エージェント A と RSVP エージェント B の間で確立されます。A から B への方向のストリームは WAN 1 を経由するフローで、もう 1 つの B から A への方向のストリームは WAN 2 を経由するフローです。これは、非対称ルーティング コールと呼ばれ、サービス プロバイダーからのロード バランシングに対応した二重接続ネットワークで一般的です。RSVP が、RSVP を認識しない WAN ネットワークへの出力インターフェイスのみを考慮している場合、たとえばサービス プロバイダー クラウドの場合のように、WAN のプロビジョニングされた帯域幅が、トラフィックがロード バランスされたときにオーバーランする可能性があります。

図 11-18　ロード バランシング対応二重接続顧客機器（CE）向けの非対称ルーティング



前述のシナリオによって示された制限を克服し、RFC 2205 に準拠するには、Cisco IOS Release 15.1(3)T でサポートされている入力コール アドミッション制御機能を使用します。入力コール アドミッション制御で、RSVP 要求の予約を、出力のみではなく、ルータへの入力での帯域幅プールに対して検証できます（図 11-19 を参照）。出力帯域幅の検証は通常どおり機能しています。

図 11-19　RSVP 入力コール アドミッション制御



RSVP VPN トンネルのサポート

Dynamic Multipoint Virtual Private Network（DMVPN; Dynamic Multipoint バーチャル プライベート ネットワーク）では、GRE トンネル、IPsec 暗号化、および Next Hop Resolution Protocol（NHRP）を組み合わせることにより IPsec VPN を拡張および縮小できます。RSVP VPN トンネル機能は、次の種類の構成をサポートしています。

- 手動で構成された Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルおよび multipoint Generic Routing Encapsulation（mGRE; マルチポイント総称ルーティング カプセル化）トンネル上での RSVP
- IPsec 保護モードでの、手動で構成された GRE トンネルおよび mGRE トンネル上での RSVP
- DMVPN 環境での、GRE トンネルおよび mGRE トンネル（IPsec 保護および IPsec 非保護）上での RSVP

DMVPN および RSVP VPN トンネル機能の詳細については、次の Web サイトで入手可能な『*Cisco IOS Quality of Service Solutions Configuration Guide, Release 15.1*』を参照してください。

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/15_1/qos_15_1_book.html

柔軟な帯域幅のインターフェイスでの RSVP

「RSVP の原理」（P.11-18）の項で説明しているように、RSVP 帯域幅がインターフェイスで設定されている場合、そのインターフェイスに対する帯域幅の値は固定されます。これにより、Multi-Link PPP、ATM IMA、FRF12、Gigabit EtherChannel（GEC; ギガビット EtherChannel）などの柔軟なインターフェイス（またはバンドル インターフェイスとしても知られています）に問題が発生します。この問題とは、スタティックな RSVP 帯域幅量をリンクのバンドルを含む柔軟な帯域幅のインターフェイスで設定すると、1 つまたは複数のリンクに障害が発生して合計帯域幅が低下した場合に RSVP 帯域幅は固定のままになるという問題です。つまり、RSVP 帯域幅と柔軟なインターフェイス帯域幅の合計との比率が設定した値と等しくならなくなり、柔軟な帯域幅のインターフェイスのオーバーサブスクリプションの原因になることがあります。

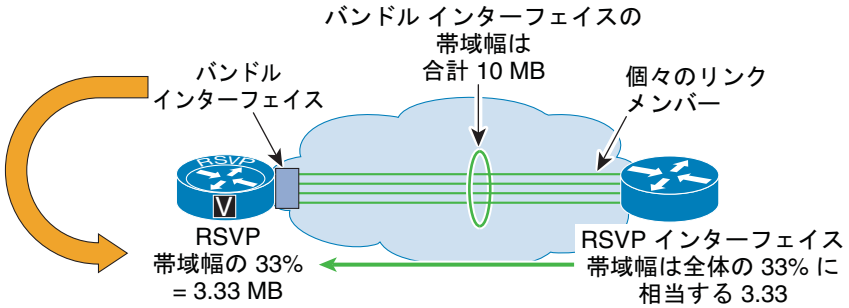
Low Latency Queuing（LLQ; 低遅延キューイング）により、すでにプライオリティ キューおよびクラスベース では比率の実装が可能です。したがって、柔軟な帯域幅のインターフェイスに適用すると、LLQ パラメータは、パラメータが設定されているインターフェイスと連動して変化します。

柔軟な帯域幅のインターフェイス機能で、**ip rsvp bandwidth** コマンドが拡張され、インターフェイス帯域幅の比率の設定ができるようになります。これにより、RSVP 帯域幅をインターフェイス帯域幅と並行的に変更でき、1 つのリンクにバンドルされている複数の物理リンクから構成されるインターフェイスに適用できます。

ネットワークまたはサービス プロバイダーに、バンドルされた WAN インターフェイスを利用したサイトを持つ企業の顧客の場合、この機能により完全な動作時間中は RSVP コール アドミッション制御で帯域幅の使用率を完全に最大化でき、一方で、リンク障害中は同じ比率のバンドルの帯域幅を直接使用できます。

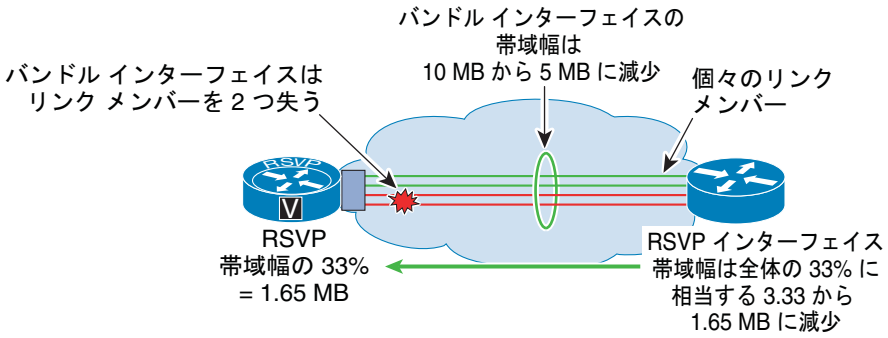
図 11-20 および 図 11-21 に、柔軟な帯域幅のインターフェイスで RSVP を使用する場合の例を示します。

図 11-20　　合計帯域幅が 10 MB の柔軟な帯域幅のインターフェイス



ip rsvp bandwidth percent *rsvp-bandwidth [max-flow-bw* **| percent** *flow-bandwidth]*

図 11-21　合計帯域幅が 5 MB まで低下した柔軟な帯域幅のインターフェイス



ip rsvp bandwidth percent *rsvp-bandwidth [max-flow-bw* **| percent** *flow-bandwidth]*

柔軟な帯域幅のインターフェイスでの RSVP の使用の詳細については、次の Web サイトで入手可能な『*Cisco IOS Quality of Service Solutions Configuration Guide, Release 15.1*』を参照してください。

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/15_1/qos_15_1_book.html

RSVP 設計上のベスト プラクティス

Unified CM と組み合せて RSVP を IP WAN に配置する場合は、次の設計上のベスト プラクティスに従います。

- 次のいずれかの条件に該当する場合は、IntServ/DiffServ モデルを採用することを推奨します。
  - IP WAN インターフェイスのプライオリティ キュー（PQ）に入るトラフィックは、RSVP 対応トラフィックだけである。
  - PQ に入る RSVP 未使用トラフィックは、アウトオブバンドのコール アドミッション制御メカニズム（Unified CM ロケーションや Cisco IOS ゲートキーパーなど）によって、すべて確定的に一定量に制限される。
- プライオリティ キュー帯域幅のレイヤ 2 のオーバーヘッドを考慮すると、すべての PQ トラフィックが RSVP 対応の場合、**ip rsvp bandwidth** コマンドで指定した値と **priority** コマンドで指定した値は一致する必要があります。
- ルータの 1 つ以上のインターフェイスで RSVP を有効にする場合は、RSVP メッセージがドロップされないように、RSVP シグナリングが通過すると考えられるすべてのインターフェイスでも RSVP を有効にする必要があります。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。
- 一部の PQ トラフィックが RSVP 非対応の場合は、**ip rsvp bandwidth** コマンドとアウトオブバンド コール アドミッション制御メカニズムで指定した値の合計が、**priority** コマンドで指定した帯域幅値を超えないようにする必要があります。
- 音声コールおよびビデオ コールで使用する最大帯域幅を制限する必要がある場合は、RSVP アプリケーション ID のサポートを有効にします。アプリケーション ID のサポートは、Cisco IOS Release 12.4(6)T で導入されました。
- WAN リンクの両側のルータの WAN インターフェイスなど、ネットワークの両端で RSVP を有効にします。
- 速度が異なる冗長リンクなど、可能性があるすべての WAN 輻輳ポイントで RSVP を有効にします。
- ロードバランスされた MPLS WAN リンクで対称ルーティングがない場合、入力コール アドミッション制御が設定されているか確認してください（「RSVP 入力コール アドミッション制御」（P.11-29）を参照）。

- ほとんどの Catalyst スイッチング プラットフォームでは、現在、RSVP を使用できません。

RSVP の帯域幅のプロビジョニング

ここでは、RSVP だけに関係する帯域幅のプロビジョニングについて説明します。帯域幅のプロビジョニング全般の詳しい説明については、「帯域幅のプロビジョニング」（P.3-47）を参照してください。

Unified CM で使用する RSVP 帯域幅の値の計算

Unified CM が Cisco RSVP Agent にコール フローの初期予約を行うよう指示する時点では、コールに関係するエンドポイントは、コーデック能力を完全には交換していません。この情報がないため、Unified CM がトラフィック フローの記述方法を決定するには、リージョン設定に依存する必要があります。トラフィック フローのサイズは、コーデック ビット レートとサンプリング レート（パケット/秒）の関数です。リージョン設定に最大コーデック ビット レートは含まれていますが、サンプリング レートは記述されていません。音声コーデックの優先サンプリング レートは、クラスタ全体の次のサービスパラメータで定義されています。

- Preferred G722 millisecond packet size：デフォルトは 20 ms
- Preferred G711 millisecond packet size：デフォルトは 20 ms
- Preferred G729 millisecond packet size：デフォルトは 20 ms

ただし、コーデックのサンプリング レートはコールごとにネゴシエートされ、1 つ以上のエンドポイントでサポートされないために、優先設定が使用されないことがあります。呼び出し後の失敗の原因となる、能力が完全に交換された後で予約サイズが増加することを防ぐには、この初期予約をコーデックの最悪のケース（最小パケット サイズを使用した最大コーデック ビット レート）に対応したものにします。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。ほとんどの場合、デフォルトのサンプリング レートが使用され、結果として予約が削減されます。

（注）　Unified CM は、RSVP 予約に SRTP オーバーヘッドまたはレイヤ 2 オーバーヘッドを含めません。RSVP T Spec 帯域幅の値と比較する場合、レイヤ 3 IP RSVP 帯域幅のステートメントは、任意の SRTP トラフィックを考慮する必要があり、SRTP トラフィックが存在する場合は、レイヤ 2 プライオリティ キューの値も余分にプロビジョニングする必要があります（表 3-10 および表 3-11 を参照）。

音声ベアラ トラフィック

音声コーデックが G729 に設定されているリージョン間コール。G.729 を使用して接続。

- 初期要求：40 kbps。最悪ケースのシナリオの 10 ms を使用。
- 更新後の要求：24 kbps。優先サンプル サイズの 20 ms を使用。

音声コーデックが G.728/iLBC の最大値に設定されているリージョン間コール。iLBC を使用して接続。

- 初期要求：48 kbps。最悪ケースのシナリオの 10 ms の G.728 を使用。
- 更新後の要求：31.2 kbps。優先サンプル サイズの 20 ms を持つ iLBC 使用。

音声コーデックが G711 に設定されているリージョン間コール。G.711 を使用して接続。

- 初期要求：96 kbps。最悪ケースのシナリオの 10 ms を使用。
- 更新後の要求：80 kbps。優先サンプル サイズの 20 ms を使用。

ビデオ ベアラ トラフィック

オーディオ ストリームと同様に、ビデオ ストリームの初期予約も、予約の時点でエンドポイントのコーデック能力が完全にはネゴシエートされていないため、リージョン設定に依存します。ビデオ コールのリージョン設定には、オーディオ ストリームの帯域幅が含まれます（詳細については、「IP ビデオ テレフォニー」（P.12-1）を参照してください）。オーディオ ストリームには独自の予約があるため、最終的なビデオ ストリームの予約は、リージョン設定から音声コーデックのビット レートを減算した値になります。ただし、これらのコーデックは完全にはネゴシエートされていないため、ビデオ ストリーム予約は、オーディオ ストリームがないという前提で、最悪のケースのシナリオで行われます。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。

ビデオは本質的にバースト性が高いため、ストリーム要件にオーバーヘッドを追加する必要があります（詳細については、「音声ベアラ トラフィック」（P.3-49）を参照してください）。Unified CM は、次のように、ストリーム帯域幅を使用してオーバーヘッドの計算方法を決定します。

- ストリームが 256 kbps 未満の場合は、オーバーヘッドが 20% になる。
- ストリームが 256 kbps 以上の場合は、オーバーヘッドが 7% になる。

音声コーデックが G.729 で、ビデオ設定が 384 kbps のリージョン間ビデオ コールの場合

- 初期要求：384 × 1.07 = 410 kbps
- 更新後の要求：(384 - 8) × 1.07 = 402 kbps

音声コーデックが G.711 で、ビデオ設定が 384 kbps のリージョン間ビデオ コールの場合

- 初期要求：384 × 1.07 = 410 kbps
- 更新後の要求：(384 - 64) × 1.07 = 342 kbps

設定の推奨事項

初期予約は実際のパケット フローよりも大きくなるため、必要なコール数に対応するには、RSVP 帯域幅および LLQ 帯域幅を多めにプロビジョニングする必要があります。

N コールの RSVP 帯域幅をプロビジョニングする場合、N 番めのコールが許可されるように、N 番めの値を最悪のケースの帯域幅にすることを推奨します。

次の例を参考にしてください。

- 4 つの G.729 ストリームをプロビジョニングする場合

  (3 × 24) + 40 = 112 kbps
- 4 つの G.711 ストリームをプロビジョニングする場合

  (3 × 80) + 96 = 336 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.729 オーディオ）をプロビジョニングする場合

  (3 × (384 - 8) + 384) × 1.07 = 1618 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.711 オーディオ）をプロビジョニングする場合

  (3 × (384 - 64) + 384) × 1.07 = 1438 kbps

Cisco IOS アプリケーション ID サポートの設定

RSVP アプリケーション ID 機能のサポートは、Cisco IOS Release 12.4(6)T で導入されました。次の例では、このリリース以降が必要です。

プライオリティ キューの組み合せ

Unified CM によるアプリケーション ID サポートの実装で許可される機能（プライオリティ キューで使用可能なすべての帯域幅を音声コールで消費可能にする機能）を利用するために、音声とビデオのプライオリティ キューを分離するという以前の推奨事項を変更する必要があります（「RSVP アプリケーション ID と Unified CM」（P.11-47）を参照してください）。この機能を使用するには、音声とビデオの両方の一致基準を 1 つのクラスマップに組み合せる必要があります。音声トラフィックまたはビデオ トラフィックのいずれかが一致することが要件になるため、次のように、クラスマップの一致基準 **match-all** の代わりに **match-any** を使用する必要があります。

```
class-map match-any IPC-RTP
 match ip dscp ef
 match ip dscp af41  af42
```

音声トラフィックとビデオ トラフィックの両方をサポートするように、プライオリティ キューを設定します。次の設定例では、リンク帯域幅の 33% がプライオリティ キューに割り当てられます。

```
policy-map Voice-Policy
 class IPC-RTP
  priority percent 33
```

アプリケーション ID から RSVP ポリシー ID へのマッピング

RSVP ローカル ポリシーによって、アプリケーション ID を基に予約を制御するメカニズムが提供されます。アプリケーション ID は、**ip rsvp policy identity** コマンドで、RSVP ローカル ポリシーにマッピングされます。RSVP ローカル ポリシー ID はグローバルに定義され、コマンドにより、各インターフェイスで使用できます。各 ID には、アプリケーション ID と照合するために定義された 1 つのポリシー ロケータがあります。

ユーザができるだけ柔軟にアプリケーション ポリシー ロケータとローカル ポリシーを照合できるように、RSVP ローカル ポリシー Command Line Interface（CLI; コマンドライン インターフェイス）は、Unix 形式の正規表現によるポリシー ロケータに対するアプリケーション ID 一致基準を受け付けます。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）など、既存の Cisco IOS コンポーネントの CLI では、正規表現が常に使用されます。Cisco IOS で正規表現を使用する方法の詳細については、次のマニュアルを参照してください。

- *Access and Communication Servers Command Reference*
  http://www.cisco.com/en/US/docs/ios/11_0/access/command/reference/arbook.html
- *Using Regular Expressions in BGP*
  http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a0080094a92.shtml
- *Regex Engine Performance Enhancement*
  http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_rexpe.html

デフォルトの Unified CM アプリケーション ID を照合するための RSVP ポリシー ID

```
ip rsvp policy identity rsvp-video policy-locator .*VideoStream.*
ip rsvp policy identity rsvp-voice policy-locator .*AudioStream.*
```

インターフェイスの RSVP ローカル ポリシー

アプリケーション ID サポートを設定するかどうかにかかわらず、RSVP をサポートするインターフェイスでは、**ip rsvp bandwidth** < *値*> コマンドを設定する必要があります。この値は、アプリケーション ID サポートの有無にかかわらず、そのインターフェイス上での 1 つの RSVP 予約または RSVP 予約の合計を超えることはできません。予約がローカル ポリシー チェックをパスした場合、予約の前に、インターフェイスの RSVP 帯域幅チェックにパスする必要があります。

アプリケーション ID に基づくローカル ポリシーは、**ip rsvp policy local identity** コマンドでインターフェイスに適用されます。

ポリシー ロケータ値と一致する予約については、ローカル ポリシーによって次の機能を実行できます。

- その予約がグループまたは単一の送信者として予約できる最大帯域幅の定義
- RSVP メッセージを転送するかどうか
- RSVP メッセージを受け入れるかどうか
- グループまたは送信者が予約できる最大帯域幅の定義

たとえば、Serial T1 でビデオ帯域幅の量を 384 kbps に制限するには、次のコマンドを使用します。

```
interface Serial0/0/1:0
 ip rsvp bandwidth 506
 ip rsvp policy local identity rsvp-video
  maximum bandwidth group 384
  forward all
```

catch-all ローカル ポリシーというデフォルト ローカル ポリシーもあります。このローカル ポリシーは、リンクで設定されているその他の RSVP ローカル ポリシーと一致しなかったすべての RSVP 予約と一致します。デフォルト ローカル ポリシーは、アプリケーション ID のタグ予約、またはタグなしトラフィックとして処理するアプリケーション ID のタグ予約と照合するために使用できます。

例

次の例は、「Cisco Unified CM でのアプリケーション ID の使用方法」（P.11-48）で説明したモデルを使用する音声コールとビデオ コールの両方をサポートします。音声コールには 352 kbps の帯域幅が保証され、ビデオ コールは 154 kbps の帯域幅に制限されます。音声コールは、使用可能な RSVP 帯域幅のすべてを使用できます。

```
interface Serial0/0/1:0
 ip address 10.2.101.5 255.255.255.252
 service-policy output Voice-Policy
 ip rsvp bandwidth 506
 ip rsvp data-packet classification none
 ip rsvp resource-provider none
 ip rsvp policy local identity rsvp-voice
  maximum bandwidth group 506
  forward all
 ip rsvp policy local identity rsvp-video
  maximum bandwidth group 154
  forward all
 ip rsvp policy local default
  no accept all ! Will not show in the configuration
  no forward all! Will not show in the configuration
```

この例では、アプリケーション ID を持たない RSVP 予約を受信したとき、またはアプリケーション ID が 2 つの設定済みオプションと一致しない RSVP 予約を受信したときに、予約が失敗します。この設定は、RSVP トラフィックが Unified CM で制御される Cisco RSVP Agent からだけ発信される場合に機能します。ただし、IP-IP ゲートウェイを経由するクラスタ間 RSVP トラフィックがある場合、または Unified CM 以外のコントローラからの RSVP メッセージがこのリンクを通過する場合は、予約を受け付けて転送するデフォルト ローカル ポリシーを設定し、このポリシーで最大帯域幅の値を設定す

る必要があります。複数の RSVP ローカル ポリシーを使用すると（ポリシーの合計が RSVP インターフェイス帯域幅より大きい場合）、RSVP 帯域幅をオーバーサブスクリプションにすることは可能ですが、予約は先着順になります。

RSVP および集中型コール処理を使用した呼制御トラフィック用のプロビジョニング

ここでは、集中型コール処理配置で RSVP をコール アドミッション制御メカニズムとして使用する場合に、呼制御トラフィック用に帯域幅をプロビジョニングする方法について説明します。RSVP を使用しない場合の帯域幅プロビジョニング全般については、「集中型コール処理を使用した呼制御トラフィック用のプロビジョニング」（P.3-52）を参照してください。

RSVP を使用するコールに関する考慮事項

コール アドミッション制御で RSVP を使用するシステムでは、WAN を経由する IP コールが発生したときに、Unified CM と支店の Cisco RSVP Agent の間に追加の SCCP 呼制御トラフィックが発生します。関連する帯域幅を計算するには、次の公式を使用します。

帯域幅（bps）=（21 × CHW）×（支店内の IP Phone とゲートウェイの数）

CHW は、異なる支店の IP Phone 間のコールや、異なるサイトにあるゲートウェイを通過するコールなど、IP WAN を経由する電話機あたりの毎時のコール数を表します。たとえば、20 台の電話機があり、電話機あたり毎時 10 コールが発生するサイトで、コールの 20% が IP WAN を経由する場合、CHW = 2 です。そこで、公式は（21 × 2）× 20 = 840 bps になります。

この公式で求めた帯域幅を電話呼制御に必要な帯域幅に追加します。

Unified CM の RSVP 対応ロケーション

Cisco Unified CM は、Resource Reservation Protocol（RSVP; リソース予約プロトコル）に基づくトポロジ対応コール アドミッション制御メカニズムを備えています。RSVP は、すべてのネットワーク トポロジに適用可能で、従来のハブアンドスポーク トポロジの制限を緩和します。Cisco RSVP Agent は Cisco IOS の機能であり、Unified CM が RSVP ベースのコール アドミッション制御を実行できるようにするものです。Cisco RSVP エージェントをサポートする Cisco IOS プラットフォームについては、次の Web サイトで入手可能な『*Cisco RSVP Agent Data Sheet*』を参照してください。

http://www.cisco.com/en/US/partner/products/ps6832/products_data_sheets_list.html

Cisco RSVP Agent は、Unified CM で、メディア ターミネーション ポイント（MTP）または RSVP をサポートするトランスコーダ デバイスのいずれかとして登録されます。エンドポイント デバイスが帯域幅の予約を必要としてコールを行う場合、Unified CM は、帯域幅を予約するためのエンドポイントに対するプロキシとして機能する Cisco RSVP Agent を呼び出します。

図 11-22 は、Unified CM とさまざまなその他のデバイス間で使用されるシグナリング プロトコルと、特定のロケーションで WAN を通じたコールのために関連付けられる RTP ストリームを示しています。WAN を通じたすべてのコールで、Unified CM は、ローカル Cisco RSVP Agent にメディア ストリームを送信するようエンドポイント デバイスに指示します。このローカル Cisco RSVP Agent は、リモート ロケーションにある Cisco RSVP Agent への RSVP 予約と同期された別のコール レッグを発信します。図 11-22 は、次のシグナリング プロトコルを示しています。

- Skinny Client Control Protocol（SCCP）による Unified CM への Cisco RSVP Agent の登録
- SCCP または Session Initiation Protocol（SIP）による Unified CM への IP Phone の登録
- Media Gateway Control Protocol（MGCP）、SIP、または H.323 プロトコルによる Unified CM への公衆網ゲートウェイの登録

図 11-22　RSVP をサポートするロケーションのプロトコル フロー

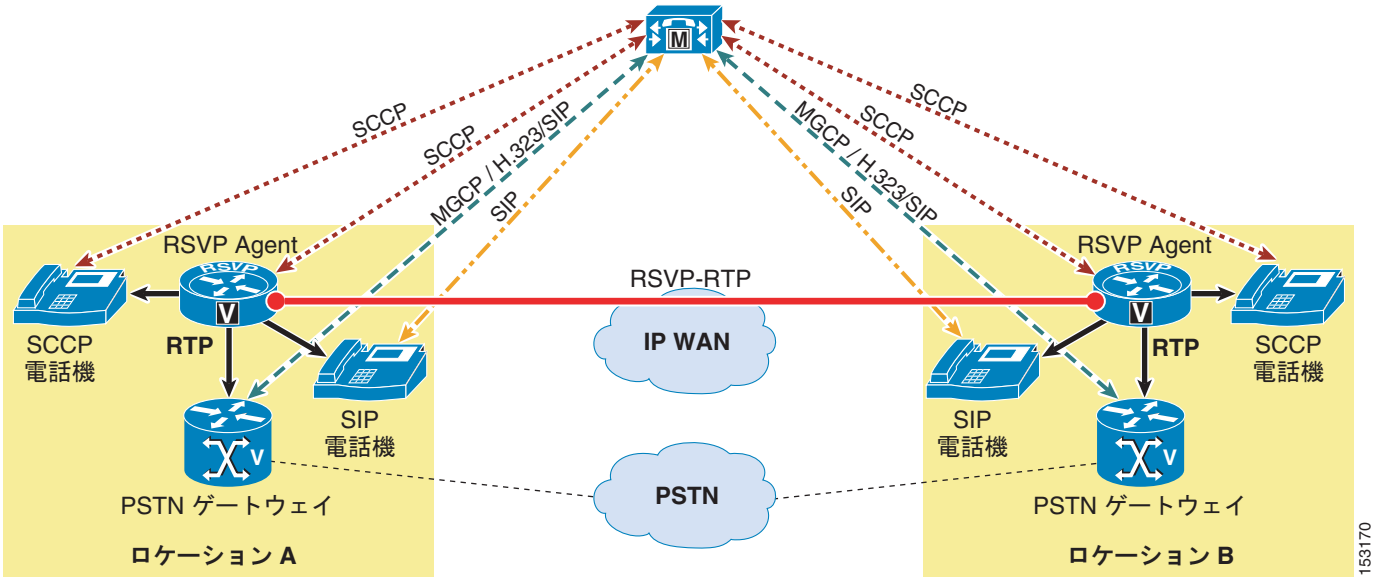
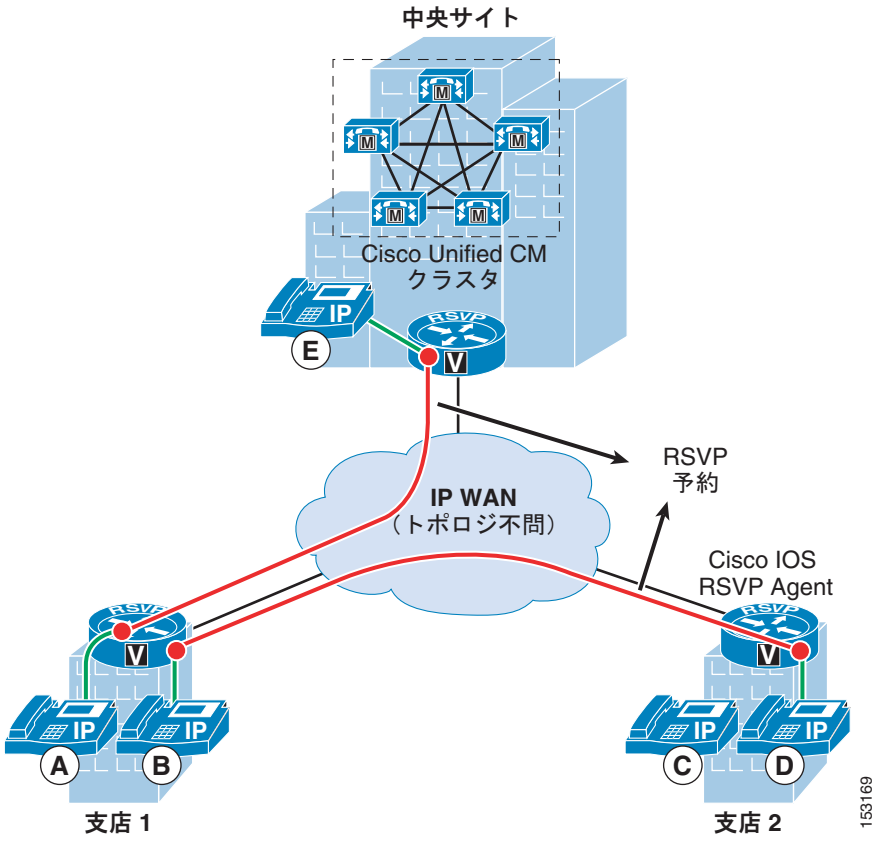


図 11-23 は、Unified CM クラスタ内の代表的な Cisco RSVP Agent 配置を示しています。これには、中央サイト、支店 1、および支店 2 の 3 つのロケーションが含まれます。3 つのロケーションを接続する IP WAN は、任意のトポロジ タイプにすることができ、ハブアンドスポーク トポロジに制限されません。メディア パスで RSVP 予約を必要とする 2 つのロケーション間のコールに対して、Cisco RSVP Agent のペアが、Unified CM から動的に呼び出されます。Cisco RSVP Agent は、Cisco RSVP Agent と同じロケーションにある IP Phone の RSVP 予約を行うためにプロキシとして動作します。たとえば、支店 1 の電話機 A が中央サイトの電話機 E をコールする場合、RSVP 予約が、支店 1 ロケーションと中央サイト ロケーションの Cisco RSVP Agent 間で確立されます（図 11-23 の赤線）。

このコールのメディア ストリームに対しては、3 つのコール レッグがあります。第 1 のコール レッグは電話機 A と支店 1 の Cisco RSVP Agent との間、第 2 のコール レッグは支店 1 と中央サイトの Cisco RSVP Agent との間、第 3 のコール レッグは中央サイトの Cisco RSVP Agent と電話機 E との間です。同様に、支店 1 の電話機 B が、支店 2 の電話機 D をコールした場合、RSVP 予約が支店 1 と支店 2 の Cisco RSVP Agent 間で確立されます。この場合、2 つの支店ロケーション間のコールのメディア ストリームは、中央サイト経由で送信されません。静的ロケーションに基づき、コール アドミッション制御を使用して、従来のハブアンドスポーク トポロジを通じて行われるコールとは異なっています。

（注）　RSVP 対応ロケーションおよび Cisco RSVP Agent を使用すると任意の WAN トポロジがサポートされますが、これらはロケーションに対するデバイスの静的な割り当てに基づいています。つまり、ある物理的なサイトから別のサイトにデバイスを移動するたびに、Unified CM の設定を更新する必要があります。デバイス モビリティを使用すると、デバイスを新しい物理的なサイトに移動したときに、サイト固有のデバイス設定情報を自動的に更新できます。詳細については、「デバイス モビリティ」（P.25-15）の項を参照してください。

図 11-23　Cisco RSVP Agent の概念



Cisco RSVP Agent のプロビジョニング

同時コール（セッションとも呼ばれる）に対する Cisco RSVP Agent の容量は、次の要因によって変化します。

- ソフトウェアベースの MTP 機能では、ルータ プラットフォームおよび相対的な CPU 負荷によってセッション容量が決まる（http://www.cisco.com/en/US/products/ps6832/products_data_sheets_list.html で入手可能な『*Cisco RSVP Agent Data Sheet*』を参照）。
- ハードウェアベースの MTP およびトランスコーダの機能では、使用可能な DSP の数によってセッション容量が制限される（DSP のサイジングの考慮事項については、「メディア リソース」（P.17-1）を参照してください）。

サポート対象プラットフォーム、要件、および容量の詳細については、次の Web サイトで入手可能な『*Cisco RSVP Agent Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/ps6832/products_data_sheets_list.html

ソフトウェアベースの MTP 機能に関して、『*Cisco RSVP Agent Data Sheet*』では、Cisco RSVP Agent 専用のルータおよび 75% の CPU 使用率を基準としたセッション容量のガイドラインを示しています。これらの数値は、特定の Cisco IOS Release に適用されるもので、大まかなガイドラインと考えてください。特定のサービス、設定、トラフィック パターン、ネットワーク トポロジ、ルーティング テーブル、およびその他の要因の異なる組み合せは、特定の配置のパフォーマンスに著しい影響を与え、サポートされる同時セッション数が減少することがあります。実稼動環境でマルチサービス ルータを配置する前に、慎重に計画および検証試験を行うことを推奨します。

Cisco RSVP Agent の登録

Cisco RSVP Agent は、RSVP をサポートする MTP またはトランスコーダ デバイスとして、Unified CM に登録されます。Cisco RSVP Agent は、MTP デバイスとして登録する場合、トランスコーディング機能をサポートしません。トランスコーディング機能をサポートするには、Cisco RSVP Agent をトランスコーダ デバイスとして Unified CM に登録する必要があります。

登録のスイッチオーバーとスイッチバック

プライマリ Unified CM に障害が発生した場合、Cisco RSVP Agent はセカンダリ Unified CM にスイッチオーバーします。プライマリ Unified CM が障害から回復すると、Cisco RSVP Agent はプライマリ Unified CM に登録をスイッチバックします。Cisco RSVP Agent 登録のスイッチオーバーとスイッチバックを設定するには、次のコマンドを使用します。

```
sccp ccm group
 switchover method immediate
 switchback method guard timeout 7200
!
gateway
  timer receive-rtp 180
```

- **switchover method immediate** は、プライマリ Unified CM サーバの障害が検出されたら、すぐにセカンダリ Unified CM サーバに登録をスイッチオーバーすることを指定します。使用可能な DSP リソースは、スイッチオーバーが完了するとすぐに、新しいコールで利用できるようになります。
- **switchback method guard timeout 7200** コマンドは、プライマリ Unified CM が障害から回復した後の登録のスイッチバック メカニズムを指定します。このコマンドを設定すると、Cisco RSVP Agent は最後のアクティブなコールの切断後に、プライマリ Unified CM への登録の正常なスイッチバックを開始します。保護タイマーの期限内に登録の正常なスイッチバックが開始されない場合、Cisco RSVP Agent は即時のスイッチバック メカニズムを使用してすぐに Unified CM に登録します。保護タイマーのデフォルト値は 7200 秒で、60 ～ 172800 秒の範囲で静的に設定できます。
- ゲートウェイ コンフィギュレーション モードでの **timer receiver-rtp** コマンドは、RSVP 予約のための RTP クリーンアップ タイマーを定義します。障害が発生した場合、既存のコール用の RSVP 予約は、RTP クリーンアップ タイマーの期限が切れるまで有効です。このタイマーのデフォルト値は、1200 秒です。このタイマーは可能な最小値である 180 秒に設定することを推奨します。

最大セッション サポート

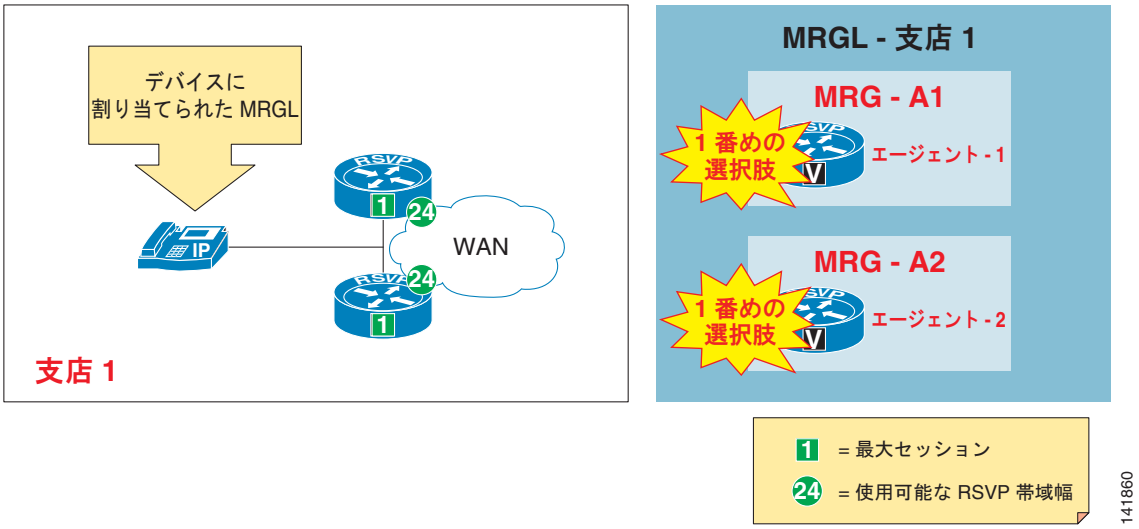
Cisco RSVP Agent は、Cisco RSVP Agent ルータに搭載されるソフトウェアベースのリソース（CPU）とハードウェアベースのリソース（DSP）に基づく、コールまたはセッションの最大数をサポートしています。**dspfarm profile** コンフィギュレーション モードの **maximum sessions** コマンドは、Cisco RSVP Agent が処理できるコールの最大数を指定します。Cisco RSVP Agent は、この設定に基づいてセッション容量を Unified CM に通知します。セッションの最大数は、コールが Cisco RSVP Agent を通過するごとに 1 つずつ減少します。カウンタが 0 になると、Cisco RSVP Agent には使用可能なリソースがないと見なされ、Unified CM はそれ以降のコールでその Cisco RSVP Agent をスキップします。

図 11-24 は、2 つの Cisco RSVP Agent がある支店サイトを示しています。Cisco RSVP Agent は WAN ルータと共存し、Cisco RSVP Agent の冗長性は、同じ MRGL の別の MRG に 2 つの Cisco RSVP Agent を割り当てることによって実現されます。MRG-1 の Agent-1 が使用できないか、セッション容量を超えている場合、Unified CM は支店 1 を宛先または発信元とする RSVP コールのために、MRG-2 に Agent-2 を割り当てようとします。Agent-1 の容量に達したときに Agent-2 が選択されるようにするには、Cisco RSVP Agent の WAN インターフェイスで設定する **ip rsvp bandwidth** でサポートされるコール数と正確に一致するセッションの最大数を設定することを推奨します。この例では、両方の Cisco RSVP Agent を **maximum sessions 1** に設定する必要があります。この推奨事項は、WAN

を経由するすべてのコールが同じタイプのコーデックを使用し、WAN 経由のコール数を正確に計算できることを前提としています。このコール数は、使用可能な RSVP 帯域幅をコールごとに必要な帯域幅で割ることによって計算します。

（注）　セッションの最大数が **ip rsvp bandwidth** 設定でサポートされるコール数よりも大きい場合でも、Unified CM はそのコールを Cisco RSVP Agent に送りますが、使用可能な帯域幅がないため RSVP 予約は失敗します。Unified CM は、コール アドミッション制御失敗の通常の処理に従います（コールを拒否するか、AAR 機能を呼び出します）。

図 11-24　Cisco RSVP Agent での最大セッションの設定



パススルー コーデック

パススルー コーデックを使用すると、Cisco IOS Enhanced MTP デバイスは、ストリームのメディア エンコーディングを認識していなくても、エンドポイントから受信した RTP メディア ストリームを終端できます。つまり、メディア ストリームの UDP パケットは、デコードされずに MTP を通過します。この方法により、MTP は、Unified CM で定義されるすべての音声、ビデオ、およびデータのコーデックをサポートできます。MTP はメディア ストリームをデコードしないため、パススルー コーデックは暗号化（SRTP）メディア ストリームでも使用できます。実際にビデオおよび SRTP メディア ストリームが MTP を使用するには、パススルー コーデックをサポートする必要があります。パススルー コーデックで設定した場合、Cisco RSVP Agent はパケットの IP/UDP ヘッダーのソース IP アドレスを独自の IP アドレスで置き換えて、パケットを通過させます。

Cisco RSVP Agent は、次のすべての条件が満たされる場合にだけ、パススルー コーデックを使用します。

- コールに関与する 2 つのエンドポイント デバイスの音声コーデック能力が一致し、リージョン設定により同一のコーデックの使用がコールに対して許可されている。つまり、コールにトランスコーダ デバイスを挿入する必要はありません。
- [MTP Required] が、いずれのエンドポイント デバイスに対しても設定されていない。
- すべての中間リソース デバイスが、パススルー コーデックをサポートしている。

（注） Cisco RSVP Agent が MTP デバイスとして登録され、トランスコーダ デバイスをコールに挿入する必要がある場合、Cisco RSVP Agent の dspfarm MTP プロファイルで設定されるコーデックは、Unified CM Administration で設定されるリージョン間コーデックと一致している必要があります。たとえば、G.729 コーデックが Unified CM Administration で設定されるリージョン間コーデックの場合は、dspfarm MTP プロファイルでも G.729 コーデックを設定する必要があります。

次の例は、Cisco 2800 IOS プラットフォーム上の Cisco RSVP Agent 設定を示しています。

```
interface Loopback0
 ip address 10.11.1.100 255.255.255.255
!
sccp local Loopback0
sccp ccm 20.11.1.50 identifier 1 priority 1 version 8.0
sccp ccm 20.11.1.51 identifier 2 priority 2 version 8.0
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate profile 1 register RSVPAgent
 switchover method immediate
 switchback method guard timeout 7200
!
dspfarm profile 1 mtp
 codec pass-through
 codec g729ar8
 rsvp
 maximum sessions software 100
 associate application SCCP
```

RSVP ポリシー

Unified CM は、ロケーション ペアごとに異なる RSVP ポリシーを適用できます。RSVP ポリシーは、Unified CM Administration で設定できます。RSVP ポリシーでは、RSVP 予約試行が失敗した場合に、Unified CM がコールを許可するかどうかが定義されます。次の RSVP ポリシー設定は、任意の 2 つのロケーション間で設定できます。

- No Reservation

  RSVP 予約試行は行われず、静的ロケーション コール アドミッション制御だけが、Unified CM で実行されます。

- Mandatory

  Unified CM は、音声ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端エンドポイント デバイスを呼び出しません。

- Mandatory (Video Desired)

  ビデオ ストリームの予約はできないが、音声ストリームの予約に成功した場合、ビデオ コールは音声専用コールとして処理できます。

- Optional (Video Desired)

  音声ストリームとビデオ ストリームの両方に対して予約が得られなかった場合、コールはベストエフォートの音声専用コールとして処理できます。Cisco RSVP Agent は、ベストエフォートとしてメディア パケットを再マーキングします。

- Use System Default

  ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。デフォルトのクラスタ全体の RSVP ポリシーは、No Reservation です。Unified CM Administration でデフォルトの RSVP ポリシーを変更するには、[System] > [Service Parameters] > [Cisco CallManager Service] > [Default Inter-location RSVP Policy] を選択します。

（注）　Optional (video desired) ポリシーでは、RSVP 予約が失敗しただけでなく、Cisco RSVP Agent も使用できない場合にだけ、IP WAN コールをベストエフォートとして処理できます。この場合、Unified CM は、ベストエフォートとしてトラフィックを再マーキングするように SCCP デバイスおよび MGCP デバイスに指示します。しかし、H.323 デバイスと SIP デバイスではこの再マーキングを行うことができないため、デフォルトの QoS マーキングでトラフィックの送信が続けられます。後者の場合にプライオリティ キューのオーバーサブスクリプションを防ぐため、IP WAN ルータで Access Control List（ACL; アクセス コントロール リスト）を設定し、ソース IP アドレスが Cisco RSVP Agent のアドレスの場合に、DSCP EF または AF41 とマークされたパケットだけを許可することを推奨します。

図 11-25 では、クラスタ全体の RSVP パラメータのデフォルト設定と推奨設定の両方を示しています。RSVP ポリシーは、[Mandatory] または [Mandatory (Video Desired)] に設定することを推奨します。これらの設定では、帯域幅の予約とコールの音声品質が保証されます。クラスタ全体の RSVP ポリシーを設定するための最も効率的な方法としては、Cisco CallManager Service の Service Parameter Configuration のクラスタ全体の RSVP パラメータに [Default Inter-location RSVP Policy] を設定し、ロケーション設定の RSVP 設定を [Use System Default] のままにします。

図 11-25　クラスタ全体の RSVP パラメータの設定

クラスタ全体の RSVP パラメータ設定には、[Mandatory RSVP mid call error handle option] という名前のサービス パラメータがあります。RSVP ポリシーを [Mandatory] または [Mandatory (Video Desired)] に設定した場合、このパラメータは Unified CM がコール中の RSVP 予約試行の失敗に基づいて既存の RSVP を処理する方法を指定します。コール中の RSVP 予約試行は、WAN の障害後にネットワークのコンバージェンスや、既存の音声専用コールがビデオ コールになることなどでトリガーされることがあります。ネットワークのコンバージェンスでは、Cisco RSVP Agent は、新たにコンバージされたパスを通じてメディア ストリームの送信が開始されるだけでなく、新しいパスを通じて新しい RSVP 予約も試行されます。

[Mandatory RSVP mid call error handle option] のデフォルト設定は、[Call Becomes Best Effort] です。デフォルト オプションの設定では、Unified CM はコール中の RSVP 予約試行が失敗しても既存のコールを保持しますが、RTP ストリームはベストエフォートとしてマークされます（DSCP 0）。このパラメータは、[Call Fails Following Retry Counter Exceeded] オプション付きで設定することを推奨します。このオプションを設定すると、Unified CM は RSVP 予約試行が一定の試行回数を超えて失敗し続けた場合に、コールを切断します。再試行カウンタのデフォルト値は 1 です。これは [RSVP Mandatory mid-call retry counter] サービス パラメータで定義され、[RSVP retry timer] のデフォルト値は 60 秒です。再試行カウンタと再試行タイマーの両方のサービス パラメータを、デフォルト値で設定することを推奨します。両方のパラメータをデフォルト値に設定すると、Unified CM はコール中の RSVP 再試行が失敗した場合に、60 秒待機してからそのコールを切断します。この間は、RSVP 予約が存在せず、RTP ストリームはベストエフォートとしてマーキングされるため、音声品質が低下することがあります。

静的ロケーションから RSVP コール アドミッション制御への移行

この項の例では、従来の静的ロケーション コール アドミッション制御から RSVP ベースのコール アドミッション制御メカニズムに移行するためのベスト プラクティスを示します。

図 11-26 では、静的ロケーション コール アドミッション制御メカニズムによるコール処理の集中型配置を示しています。Hub_None ロケーションや 3 箇所の支店など、Unified CM クラスタには 4 つのロケーションがあります。説明を簡単にするために、この例で使用する帯域幅は音声ストリームの帯域幅だけを示しています。表 11-5 と表 11-6 は、256 kbps の帯域幅で静的にプロビジョニングされるすべての支店ロケーションと、[Unlimited] の帯域幅でプロビジョニングされる Hub_None ロケーションを示しています。ロケーションの任意のペア間の RSVP 設定は [Use System Default] で設定され、クラスタ全体の RSVP 設定はデフォルト値 [No Reservation] で設定されます。

図 11-26　静的ロケーションでのコール アドミッション制御の設定

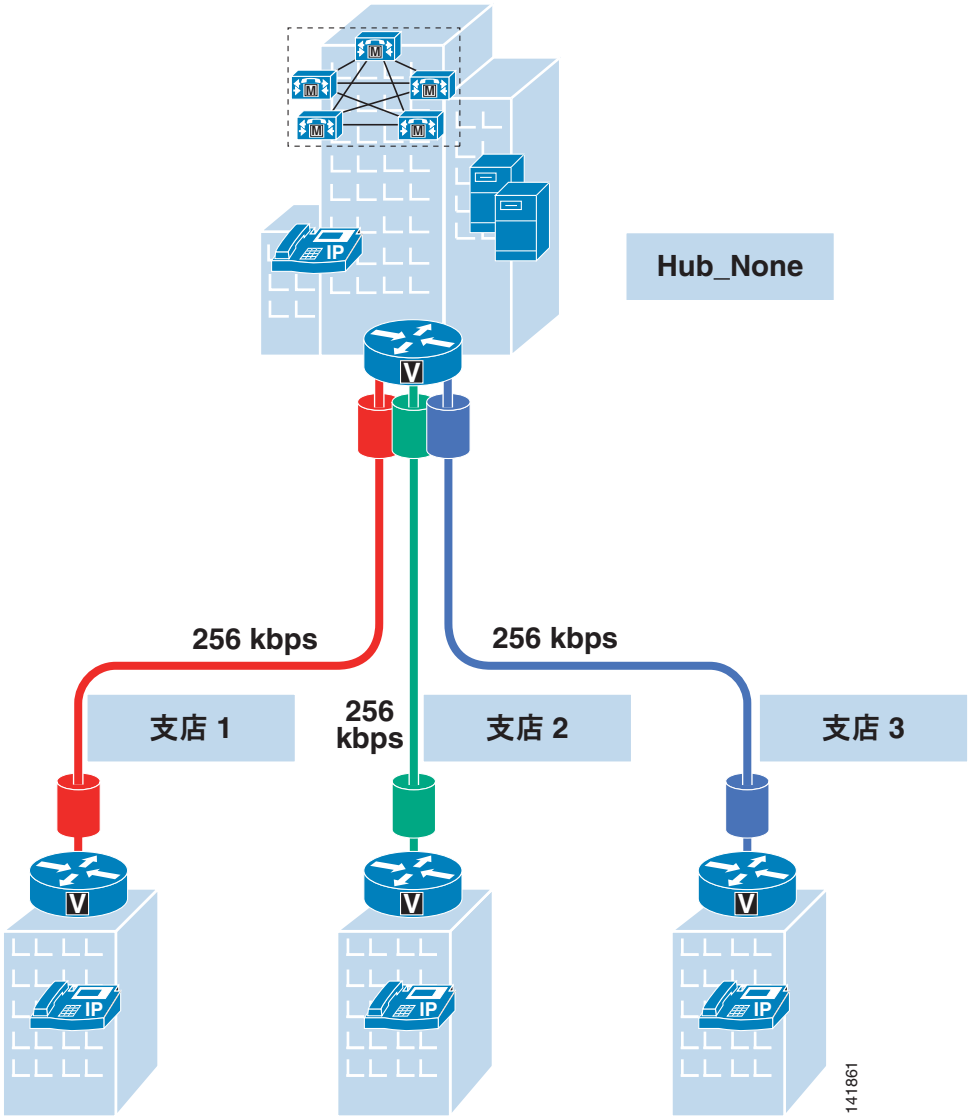


表 11-5　図 11-26 の例でのロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	256 kbps
支店 2	256 kbps
支店 3	256 kbps

表 11-6　図 11-26 の例での RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	No Reservation

RSVP ベースのコール アドミッション制御に移行するには、ロケーションを一度に 1 つずつ移行することを推奨します。たとえば、支店 1 が最初に移行するロケーションの場合は、次の手順に従います。

- 支店 1 ロケーションで Cisco RSVP Agent を設定し、支店 1 の MRG および MRGL に割り当てて、支店 1 の IP Phone に関連付けます。
- Hub_None ロケーションで別の Cisco RSVP Agent を設定し、Hub_None ロケーションを含む残りの 3 つのロケーションのすべての IP Phone に関連付けられた MRG および MRGL に、Cisco RSVP Agent を含めます。Cisco RSVP Agent を、Null MRG または支店 1 MRG に含めないでください。含めると、支店 1 の IP Phone が Hub_None ロケーションで Cisco RSVP Agent を使用して、RSVP 予約を行う可能性があります。
- 支店 1 の帯域幅を [Unlimited] に設定します。
- 支店 1 とその他の任意のロケーション間の RSVP 設定を [Mandatory] に設定します。たとえば、支店 1 と支店 2 の IP Phone 間のコールに対して、音声ストリームは Hub_None ロケーションを通じたヘアピンのままになります。支店 1 ロケーションと Hub_None ロケーション間の最初のコール レッグに対して、RSVP 予約は、支店 1 と Hub_None の Cisco RSVP Agent 間に行われます。Hub_None ロケーションと支店 2 ロケーション間の 2 番めのコール レッグに対して、Unified CM は、支店 2 ロケーションの帯域幅の可用性をチェックすることにより、静的ロケーションに基づくコール アドミッション制御を実行します。

表 11-7 と表 11-8 は、支店 1 での移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。

表 11-7　支店 1 への移行後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	256 kbps
支店 3	256 kbps

表 11-8　支店 1 への移行後の RSVP ポリシー

ロケーション ペア		ポリシー
支店 1	任意	Mandatory
その他すべてのロケーション	その他すべてのロケーション	No Reservation

表 11-9 と表 11-10 は、クラスタ全体の移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。クラスタ全体の移行が完了すると、サイト間のコールでは 2 つの Cisco RSVP Agent 間で RSVP 予約を直接行う必要があり、音声ストリームは帯域幅予約パスを通じて転送されます。

次の手順を使用すると、支店 2 および支店 3 を RSVP コール アドミッション制御に移行できます。

- 支店 2 ロケーションで Cisco RSVP Agent を設定し、支店 2 の IP Phone に関連付けられた支店 2 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 2 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 2 の MRG から削除してください。
- 支店 2 の帯域幅を [Unlimited] に設定します。
- 支店 2 とその他の任意のロケーション間の RSVP 設定を [Mandatory] に設定します。
- 支店 3 ロケーションで Cisco RSVP Agent を設定し、支店 3 の IP Phone に関連付けられた支店 3 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 3 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 3 の MRG から削除してください。
- 支店 3 の帯域幅を [Unlimited] に設定します。
- 支店 3 とその他の任意のロケーション間の RSVP 設定を [Mandatory] に設定します。

表 11-9　移行の完了後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	Unlimited
支店 3	Unlimited

表 11-10　移行完了後の RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	Mandatory

RSVP アプリケーション ID と Unified CM

RSVP アプリケーション ID は、Unified CM が音声トラフィックとビデオ トラフィックの両方に識別子を追加できるようにするメカニズムです。これにより、Cisco RSVP Agent は、受け取った識別子に基づいていずれかのトラフィックに個別の帯域幅制限を設定できます。ネットワークに RSVP アプリケーション ID を配置するには、Cisco RSVP Agent ルータで、最低でも Cisco IOS Release 12.4(6)T 以降を使用する必要があります。RSVP アプリケーション ID 文字列は、クラスタ全体の RSVP パラメータ設定の 2 つのサービス パラメータ（**RSVP Audio Application ID** と **RSVP Video Application ID**）で設定できます。

Unified CM は SCCP を使用して、RSVP アプリケーション ID を Cisco RSVP Agent に伝達します。Cisco RSVP Agent は、RSVP シグナリング メッセージ（RSVP PATH メッセージや RESV メッセージなど）に RSVP アプリケーション ID を挿入し、ダウンストリームまたはアップストリームの RSVP ルータにこれらのメッセージを送信します。

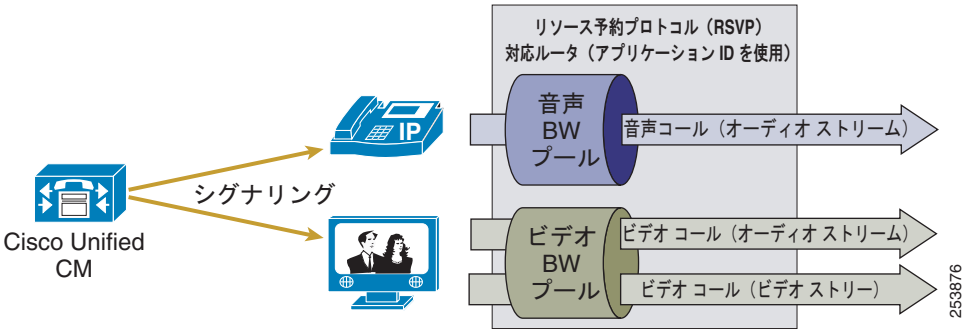
Cisco Unified CM でのアプリケーション ID の使用方法

Unified CM には次に挙げる 2 つのクラスタ全体のサービス パラメータがあり、RSVP を使用して音声コール予約およびビデオ コール予約にタグ付けするためのアプリケーション ID を定義できます。

- RSVP Audio Application ID（デフォルトは AudioStream）
- RSVP Video Application ID（デフォルトは VideoStream）

図 11-27 に、Unified CM がどのように RSVP で音声コールおよびビデオ コールにアプリケーション ID をタグ付けするかを示します。

図 11-27　Unified CM と RSVP アプリケーション ID



音声コールにタグ付けする方法

RSVP ポリシーを使用してロケーション間の音声コールを作成すると、オーディオ ストリームの予約に RSVP Audio Application ID のタグが付きます。

ビデオ コールにタグ付けする方法

RSVP ポリシーを使用してロケーション間でビデオ コールを発信すると、オーディオ ストリームとビデオ ストリームの両方の予約に RSVP Video Application ID のタグが付きます。ビデオ コールでは、音声とビデオの両方が Video Application ID に関連付けられます。

（注）　この機能は Cisco Unified CM 8.0 で新たに導入されたもので、静的ロケーション モデルに似たモデルを使用して、音声トラフィックとビデオ トラフィックの帯域幅を分けるようになっています。静的ロケーションでは、ビデオ コールの音声ストリームとビデオ ストリームはどちらもビデオ帯域幅カウンタから差し引かれます。Unified CM 8.0 で RSVP アプリケーション ID を使用すると、同じロジックが適用され、ビデオ コールのオーディオ ストリームとビデオ ストリームがビデオ帯域幅アプリケーション ID から差し引かれます。

RSVP アプリケーション ID の設計上の考慮事項とベスト プラクティス

- AudioStream Application ID は、音声専用コールのオーディオ ストリームに使用されます。
- VideoStream Application ID は、ビデオ コールのオーディオ ストリームとビデオ ストリームの両方に使用されます。
- アプリケーション ID は、現時点ではテレプレゼンス ビデオなどのさまざまなビデオ タイプを区別しません。RSVP セッションのすべてのビデオが、Video Application ID とビデオ DSCP 値でマーキングされます。

- Unified CM には現在、シグナリング ストリームおよびメディア ストリームのアプリケーション ID と DSCP 値の両方の設定が別々に用意されています。これらの値は別々に管理されますが、互いに連動して動作するように設定されているため、デフォルト値を使用することを推奨します。
- ビデオ エスカレーションが発生すると、オーディオ ストリームの RSVP 予約が Video Application ID および設定済みの DSCP 値（デフォルトでは PHB AF41）で再許可されます。十分な帯域幅がないためにオーディオ ストリームの再許可が失敗した場合、Video Application ID プールへの予約が成功するまで、オーディオ ストリームは Video Application ID 付きでベストエフォート型として続行します。
- ビデオ デエスカレーションが発生すると、オーディオ ストリームの RSVP 予約が Audio Application ID および設定済みの DSCP 値（デフォルトでは PHB EF）で再許可されます。十分な帯域幅がないためにオーディオ ストリームの再許可が失敗した場合、Audio Application ID プールへの予約が成功するまで、オーディオ ストリームは Audio Application ID 付きでベストエフォート型として続行します。

アプリケーション ID 付きのビデオ エスカレーションの例

音声専用コールは AudioStream Application ID 付きでセットアップされ、ストリームの DSCP は PHB 値 EF に設定されます。コールをビデオへとエスカレーションすると、ビデオ ストリームが VideoStream Application ID 付きでセットアップされます。ビデオ ストリーム予約が失敗した場合、コールは AudioStream Application ID 付きの音声専用コールのままとなります。一方、ビデオ ストリーム予約が成功した場合は、オーディオ ストリームが AudioStream Application ID から VideoStream Application ID へと再許可されます。再許可が成功すると、ビデオ ストリームとオーディオ ストリームのどちらでも、VideoStream Application ID が PHB 値 AF41 に設定されます。再許可が失敗すると、ビデオ ストリームでは VideoStream Application ID が PHB 値 AF41 に設定され、オーディオ ストリームでは VideoStream Application ID が PHB 値 0 に設定されます（ビデオ失敗時の DSCP 値）。

RSVP SIP プレコンディションを使用した分散 Unified CM 環境でのビデオのエスカレーションとデエスカレーションについては、「RSVP SIP プレコンディションを使用した Unified CM ビデオ コール」（P.11-56）を参照してください。

RSVP SIP プレコンディション

RSVP SIP プレコンディションは、RFC 3312 および RFC 4032 に規定されている SIP プレコンディションに基づいています。RSVP SIP プレコンディションにより、シスコ コール処理製品はサービス品質レベルをネゴシエートし、RSVP プロトコルを使用してコール アドミッション制御を実行できます。RSVP SIP プレコンディションという用語は、ポリシー情報要素、つまりプレコンディションを SIP シグナリングで受け渡して Quality of Service（QoS）ポリシーをネゴシエートすることを識別するために使用します。実際の RSVP メッセージは、SIP トランクで通知されません。ポリシー関連の情報要素だけが通知されます。RSVP メッセージは、RSVP Agent または RSVP 対応ルータによって伝送されます。このように SIP プレコンディションを使用すると、Unified CM クラスタで実施される RSVP サービス品質ポリシーのネゴシエーションが Unified CM Express および SIP-TDM Cisco IOS ゲートウェイへと拡大されて、このようなさまざまな呼制御アプリケーション間で RSVP レイヤおよび呼制御レイヤを同期できるようになります。

SIP プレコンディションの概要

上記のように、SIP プレコンディションを使用すると、呼制御アプリケーション間で RSVP ポリシー情報をネゴシエートできます。これにより、呼制御アプリケーション間でリソース予約のために RSVP レイヤを同期し、コールのセットアップと確立のために呼制御レイヤを同期できます。

また、SIP シグナリングでのプレコンディションという概念により、独立した呼制御アプリケーション間に「ゴースト呼び出し音」と呼ばれるものが発生しないようにすることもできます。発信者間にメディアを確立するために必要なリソースを予約せずに着信側を呼び出すと、セッション確立時にゴースト呼び出し音が発生することがあります。ゴースト呼び出し音を最小限に抑えるためには、着信側を呼び出す前に、セッションのネットワーク リソースを予約する必要があります。ただし、ネットワーク リソースを予約するには、着信側から頻繁に IP アドレス、ポート、およびセッション パラメータを学習する必要があります。この情報は、SIP でオファーとアンサーを初めて交換したときに取得されます。この交換の際には通常、電話機の呼び出し音が鳴って、ループ ジレンマが発生します。つまり、初期オファー / アンサー交換を実行しないとリソースを予約できず、リソース予約を実行しないと初期オファー / アンサー交換を行えません。

RSVP SIP プレコンディションは、オファーで導入するセッションに関して SIP プレコンディションまたは制約を設定して、このジレンマを解決します。オファーの受信者はアンサーを生成しますが、ユーザに警告せず、セッション確立も続行しません。プレコンディションが満たされているときにだけ次の処理に進みます。この情報は、リソース予約の確認などのローカル イベントか、または発信側が送信した新たなオファーを通して取得できます。

図 11-28 に、このような SIP プレコンディションが汎用 SIP シグナリング コール フローでどのように機能するかを示します。

図 11-28　　コール エージェント間での SIP と RSVP

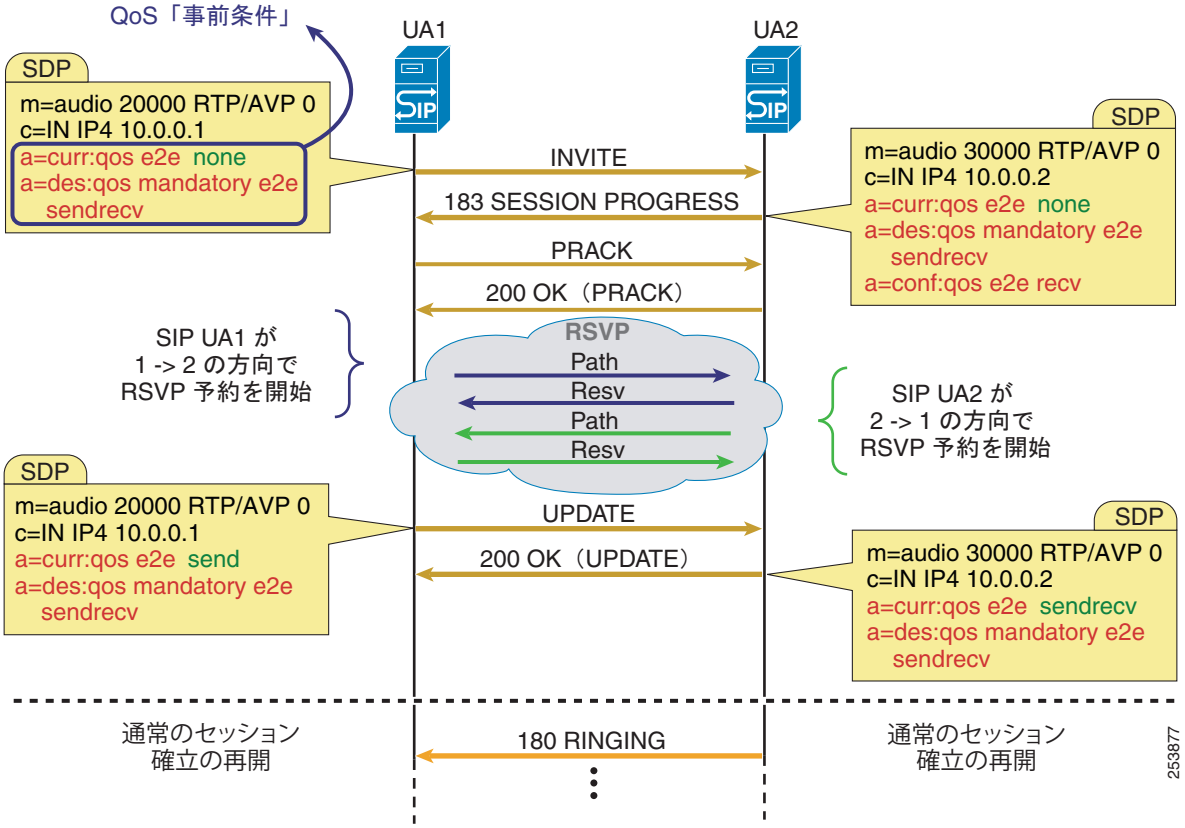


図 11-28 では、SIP ユーザ エージェント（SIP UA 1）が、SIP INVITE メッセージを送信して、コールを開始しています。Session Description Protocol（SDP）の SIP INVITE にはプレコンディションが含まれており、これにより発信側の IP アドレスおよびポート番号が識別されます。プレコンディションは現在の QoS ポリシー（a=curr:qos）および目的の QoS ポリシー（a=des:qos）を要求します。この例では、SIP UA 1 は SIP UA 2 に INVITE を送信して、音声回線用の現在の QoS ポリシーを **none** に設定し、目的の QoS ポリシーを **mandatory e2e sendrecv** に設定します。これにより、コールをオ

ファーする（エンド デバイスの呼び出し音を鳴らす）前に、RSVP 予約が必須であることが受信側に伝えられます。SIP UA 2 は INVITE を受信すると、183 SESSION PROGRESS メッセージで応答します。その結果、SDP により、送信されたプレコンディションへの応答が求められます。この例では、SIP UA 2 は、現在の QoS ポリシーを **none**、目的の QoS ポリシーを **mandatory e2e sendrecv**、さらに設定済みの QoS ポリシー（a=conf:qos）を **e2e recv** としてそれぞれ送信して、要求を受信したことと、RSVP を使用して予約を開始することを示します。この時点で、両ユーザ エージェントとも、RSVP をネゴシエートして、SDP の記述どおりにメディアの帯域幅を予約します。この予約が成功すると、UA は最新の QoS ポリシー前提条件で互いを更新し、エンド ユーザの呼び出し音を鳴らしてコールを続行します。例では、SIP UA 2 は 180 RINGING メッセージで応答し、コールは通常の確立を続行できます。予約が失敗した場合、どちらの SIP UA も着信側の呼び出し音を鳴らさずにコールを終了できます。これにより、「ゴースト呼び出し音」が鳴る条件を回避できます。

Unified Communications Manager および RSVP SIP プレコンディション

Unified CM の RSVP SIP プレコンディションにより、分散型 Unified CM 配置でクラスタ間コール アドミッション制御を機能させることができます。Unified CM に RSVP SIP プレコンディションを配置する場合は、RSVP SIP プレコンディションを有効にする前に、ローカル RSVP 対応ロケーションベースのコール アドミッション制御を完全に機能させることを推奨します。また、このアプローチは移行目的にも推奨します。クラスタ内 RSVP コール アドミッション制御を有効にする方法の詳細については、「Unified CM の RSVP 対応ロケーション」（P.11-38）を参照してください。

RSVP SIP プレコンディションには、ローカル RSVP とエンドツーエンド RSVP の 2 つの設定モードがあります。これらのモードは、[Unified CM Administration] ページの SIP トランク プロファイルに設定します。

ローカル RSVP

ローカル RSVP は、別々のクラスタにある 2 つの RSVP Agent 間での予約をサポートしません。クラスタごとに 2 つの RSVP Agent を使用します。クラスタを接続するトランクを越えて RSVP を使用することはありません。これは、SIP トランク プロファイルのデフォルト設定です。

図 11-29 に、分散型 Unified CM 配置でのローカル RSVP を示します。

図 11-29　分散型 Unified CM 配置でのローカル RSVP

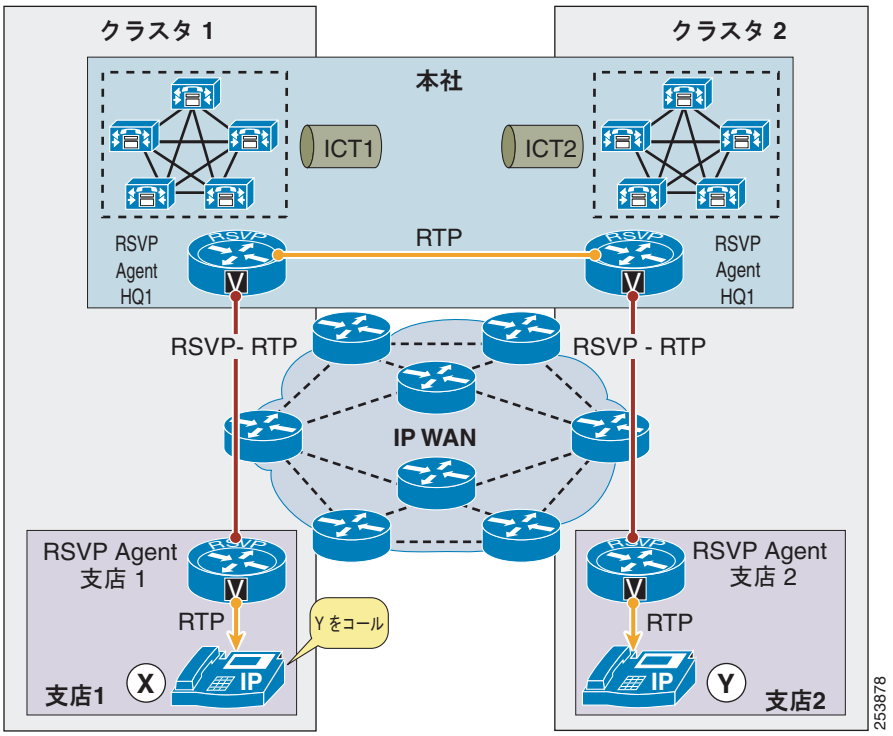


図 11-29 では、X はクラスタ 1 のエンドポイントを示し、Y はクラスタ 2 のエンドポイントを示し、ICT1 と ICT2 はそれぞれクラスタ 1 とクラスタ 2 に設定されたクラスタ間トランクを示します。それぞれのデバイスに関連付けられた RSVP Agent も示しています。このシナリオでは、Cisco Unified CM クラスタ 1 が AgentBr1 と AgentHQ1 間の予約を制御し、Cisco Unified CM クラスタ 2 が AgentBr2 と AgentHQ2 間の予約を制御します。

エンドツーエンド RSVP

クラスタ間を SIP トランクで接続すると、エンドツーエンド RSVP 設定が使用可能になります。エンドツーエンド RSVP は、RSVP Agent 間の接続全体で RSVP を使用し、クラスタごとに RSVP Agent を 1 つだけ使用します。

図 11-30 に、Unified CM でのエンドツーエンド RSVP を示します。

図 11-30　エンドツーエンド RSVP

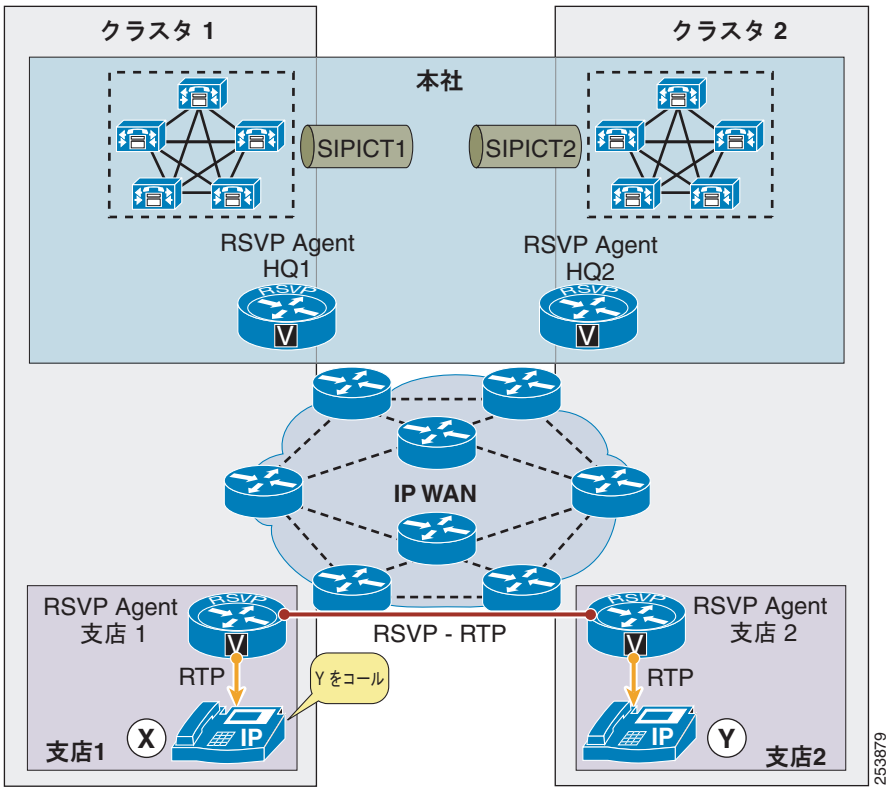


図 11-30 では、X はクラスタ 1 のエンドポイントを示し、Y はクラスタ 2 のエンドポイントを示し、ICT1 と ICT2 はそれぞれクラスタ 1 とクラスタ 2 に設定されたクラスタ間トランクを示します。それぞれのデバイスに関連付けられた RSVP Agent も示しています。このシナリオでは、Cisco Unified CM が AgentBr1 と AgentBr2 間に直接エンドツーエンド RSVP 接続を確立します。

RSVP SIP プレコンディションおよびローカル RSVP へのフォールバック

SIP トランク プロファイルで [Fall back to local RSVP] を設定して、エンドツーエンド RSVP からローカル RSVP にフォールバックするように Unified CM を設定できます。このフォールバックが発生するのは、SIP トランクの着信側が SIP 420 応答（Bad Extension）を返して、着信側がプレコンディションを認識していないことを示したときだけです。SIP 580 応答（Precondition Failed）などの応答が返されたときには、フォールバックは発生しません。コールの確立中に SIP 420（Bad Extension）応答でエンドツーエンド RSVP SIP プレコンディションが失敗した場合には、Unified CM はローカル RSVP を呼び出します。この動作が目的にかなう場合は、RSVP Agent 関連付けを記載したメディア リソース グループ リストを SIP クラスタ間トランクに割り当てる必要があります。ローカル RSVP へのフォールバックを設定しない場合、トランクまたはゲートウェイをもう 1 つ設定していると、Unified CM はルート グループおよびルート リストを使用してそのトランクまたはゲートウェイへとたどります。トランクまたはゲートウェイを設定していないと、コールは失敗します。

この機能は、1 つの SIP トランクが複数の宛先で終端する設計、両方の SIP プレコンディションがサポートされる設計、および両方の SIP プレコンディションがサポートされない設計に使用できます。たとえば、Unified Proxy Server を使用する例を考えてみます。SIP プロキシに対して SIP トランクが 1 つ設定されており、宛先として返されるのは SIP プレコンディションを認識する着信側クラスタか、または SIP プレコンディションを認識しない着信側クラスタまたは SIP サーバとなっています。この場合、SIP トランクが 1 つだけであるため、そのトランクが RSVP SIP プレコンディションで有効になってフォールバックが有効になります。着信側が SIP プレコンディションを認識しない場合には、フォールバック モードの SIP トランクに RSVP Agent を関連付けることができます。そのため、SIP 420 メッ

セージ（Bad Extension）が受信され、フォールバックが発生すると、SIP プレコンディションなしで新たな SIP INVITE が送出されます。SIP プレコンディションをサポートしている場合は、「SIP プレコンディションの概要」（P.11-49）で説明するとおりに、コールの処理が進められます。

ローカル RSVP フォールバックを有効にすることは推奨*しません*。その代わり、宛先に到達するルートを別に設定してください。ローカル ルート グループや同じような機能を使用して、RSVP コール アドミッション制御に失敗したコールを発信側デバイスにローカルなゲートウェイに再ルーティングし、コールが公衆網を経由できるようにすることを推奨します。

ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションへの移行

ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションに移行するときは、「静的ロケーションから RSVP コール アドミッション制御への移行」（P.11-45）の項で説明している移行の推奨事項にまず従うことが重要です。ローカル RSVP コール アドミッション制御へのローカルな静的ロケーション コール アドミッション制御の移行が完了すると、SIP クラスタ間トランクで RSVP SIP プレコンディションを有効にできます。

RSVP SIP プレコンディションを有効にするには、次の手順が必要です。

ステップ 1　各クラスタに SIP クラスタ間トランクを設定し、他のクラスタにつなぎます。

ステップ 2　SIP クラスタ間トランクをそれぞれ独自のロケーションに配置します。すべてのデバイスが SIP クラスタ間トランク ロケーションとは別のロケーションにあり、どのデバイスにも [Mandatory] または [Mandatory (Video Desired)] のロケーション間 RSVP ポリシーがある必要があります。ロケーション間ポリシーによって、プレコンディションの SIP トランク経由で送信される RSVP ポリシーが決まります（表 11-11 を参照。SIP オーディオとビデオのプレコンディション属性に対応する Unified CM ロケーション間ポリシーの一覧があります）。

ステップ 3　SIP クラスタ間トランクのロケーション内 RSVP ポリシーを [Mandatory] または [Mandatory (Video Desired)] に設定します。指定したロケーションのロケーション間 RSVP ポリシーを自らに設定して、ロケーション内 RSVP ポリシーを実現します。これは同じ SIP クラスタ間トランク上のクラスタにコールを転送する場合に必要であり、そうすると転送が失敗しません。

ステップ 4　各 Unified CM クラスタで SIP クラスタ間トランクの SIP プロファイルを設定します。そのためには、[RSVP Over SIP] を [E2E]、[Fall back to local RSVP] フィールドを好みの値、[SIP Rel1XX Options] を [Send PRACK if 1XX contains SDP] にそれぞれ設定します。

（注）　SIP トランク設定の場合、RSVP SIP プレコンディションで IPv6 はサポートされません。したがって、IPv6 有効化チェックボックス [Enable ANAT for early offer calls] は、RSVP SIP プレコンディションではサポートされないためオフにします。

（注）　Unified CM をエンドツーエンド RSVP 用に設定した場合、SIP トランクでは [MTP Required] チェックボックスと [Use TRP] チェックボックスが無視されます。

上で説明したように、RSVP SIP プレコンディション機能を使用すると、Unified CM エンドポイントはクラスタを越えて直接 RSVP Agent 間予約を確立できます。図 11-31 に、RSVP SIP プレコンディションを使用したコールの発信に関与するコンポーネントを示します。

図 11-31　RSVP SIP プレコンディション、分散型 Unified CM 配置デュアル クラスタ設計

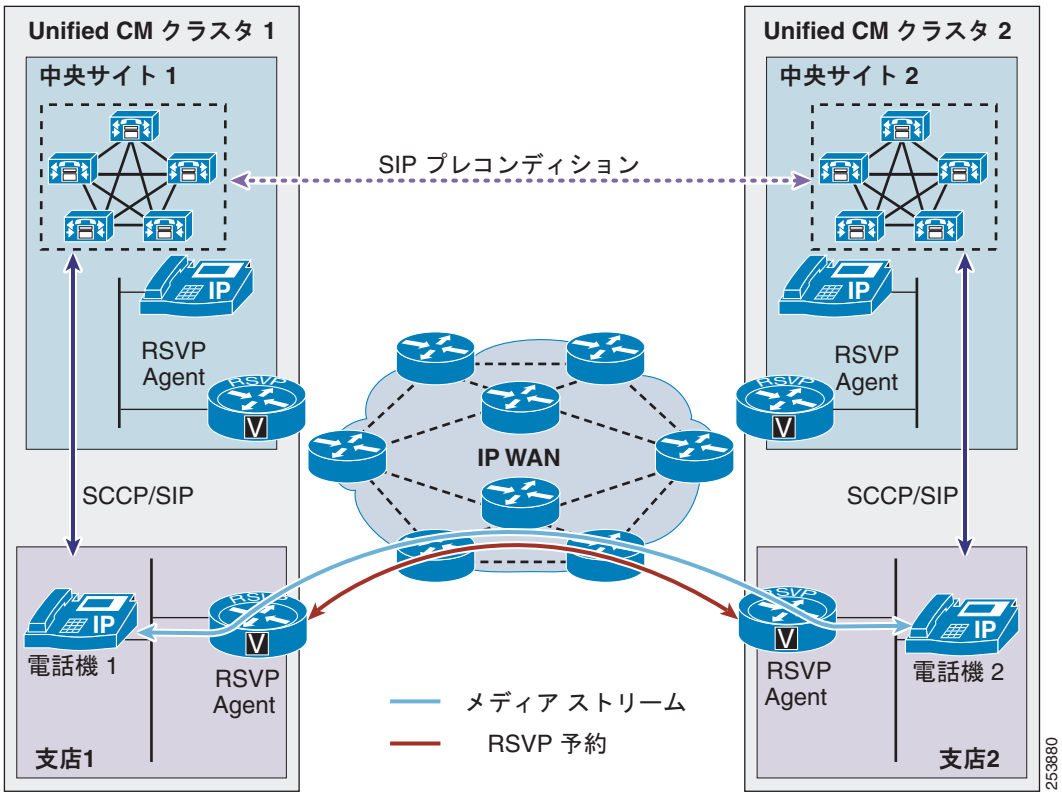


図 11-31 に、RSVP SIP プレコンディションが有効で代表的なデュアル クラスタ配置を示します。この配置には、中央サイト 1、支店 1、中央サイト 2、支店 2 の 4 つのロケーションが含まれています。4 つのロケーションを接続する IP WAN は、任意のトポロジ タイプにすることができ、ハブアンドスポーク トポロジに制限されません。メディア パスで RSVP 予約を必要とする 2 つのクラスタ間のコールに対して、Cisco RSVP Agent が、各 Unified CM クラスタから動的に呼び出されます。Cisco RSVP Agent は、Cisco RSVP Agent と同じロケーションにある IP Phone の RSVP 予約を行うためにプロキシとして動作します。たとえば、支店 1 の電話機 1 が支店 2 の電話機 2 をコールすると、支店 1 ロケーションの Cisco RSVP Agent と支店 2 ロケーションの Cisco RSVP Agent との間に RSVP 予約（図 11-31 の赤線で示した部分）が確立されます。これは、単一クラスタ RSVP 対応ロケーション ソリューションのメディア ストリーム セットアップに似ています。異なるのは、SIP トランクが 2 つの Unified CM クラスタ間で RSVP ポリシー ネゴシエーションを渡して、それぞれの電話機に関連付けられたクラスタ ロケーションごとに RSVP Agent を 1 つだけ割り当てるようにしている点です。

このコールのメディア ストリームに対しては、3 つのコール レッグがあります。第 1 のコール レッグは電話機 1 と支店 1 の Cisco RSVP Agent との間、第 2 のコール レッグは支店 1 と支店 2 の Cisco RSVP Agent との間、第 3 のコール レッグは支店 2 の Cisco RSVP Agent と電話機 2 との間です。この場合、2 つの支店ロケーション間のコールのメディア ストリームは、中央サイト経由で送信されません。静的ロケーションに基づき、コール アドミッション制御を使用して、従来のハブアンドスポーク トポロジを通じて行われるコールとは異なっています。

この同じコールのシグナリングに対しては、5 つのコール レッグがあります。第 1 のコール レッグは電話機 1 と Unified CM クラスタ 1 との間、第 2 のコール レッグは支店 1 の Cisco RSVP Agent と Unified CM クラスタ 1 との間、第 3 のコール レッグは Unified CM クラスタ 1 と Unified CM クラスタ 2 との間、第 4 のコール レッグは Unified CM クラスタ 2 と支店 2 の Cisco RSVP Agent との間、最後の第 5 のコール レッグは Unified CM クラスタ 2 と電話機 2 との間です。

図 11-31 では、クラスタ 1 支店 1 の電話機 1 がクラスタ 2 支店 2 の電話機 2 をコールします。電話機と Unified CM との間のコール シグナリングは SCCP または SIP であり、Unified CM 間のシグナリングは SIP で RSVP SIP プレコンディション機能が有効になります。電話機 1 が電話機 2 へのコールを開始すると、電話機 1 のメディア リソース グループおよびリストにある RSVP Agent に基づいて、クラスタ 1 サーバが RSVP Agent を電話機 1 に割り当て、SIP プレコンディション（RSVP ポリシー）を使用してコールを SIP トランク経由でクラスタ 2 に送信します。クラスタ 2 への SIP INVITE でアドバタイズされるプレコンディションは、電話機 1 のロケーションとクラスタ 1 の SIP トランク間に設定されたロケーション間ポリシーから派生したものです。そのため、クラスタ 1 ではロケーション支店 1 とロケーション HQ との間のロケーション間ポリシーを [Mandatory (Video Desired)] に設定します。Unified CM ポリシーの詳細については、「RSVP ポリシー」（P.11-43）を参照してください。このロケーション間ポリシーによって、クラスタ 2 に発信される SIP INVITE のポリシー セットが決まります。この時点で、クラスタ 2 がクラスタ 1 から SIP INVITE を受信します。プレコンディションは [Mandatory] に設定されています。次に、クラスタ 2 は、自身のメディア リソース グループおよびリストに基づいて、RSVP Agent を電話機 2 に割り当て、さらにクラスタ 2 の SIP トランクと支店 2 の電話機 2 との間に設定されたロケーションを確認します。このポリシーも [Mandatory] であると、クラスタ 2 は 183 SESSION PROGRESS メッセージで応答し（このあとに PRACK が続きます）、支店 1 と支店 2 の 2 つの RSVP Agent 間で RSVP ネゴシエーションを開始します。コール予約のネゴシエートが正常に完了すると、RSVP Agent がそれぞれのクラスタにその旨通知し、SIP シグナリングが呼び出し段階へと進みます。

表 11-11 に、Unified CM ロケーション間ポリシーと、対応する SIP オーディオ/ビデオ プレコンディション属性との比較を示します（Unified CM RSVP ポリシーの詳細については、「RSVP ポリシー」（P.11-43）を参照してください）。

表 11-11　Unified CM RSVP ポリシーと対応する SIP プレコンディション

Unified CM RSVP ポリシー	SIP プレコンディション（音声コール）	SIP プレコンディション（ビデオ コール）
No Reservation	audio = none	audio = none video = none
Optional (Video desired)	audio = optional	audio = optional video = optional
Mandatory	audio = mandatory	audio = mandatory video = mandatory
Mandatory (Video desired)	audio = mandatory	audio = mandatory video = optional

RSVP SIP プレコンディションを使用した Unified CM ビデオ コール

Unified CM は、RSVP SIP プレコンディションを使用して、Unified CM クラスタ全体でビデオ エスカレーションおよびデエスカレーションをサポートします。進行中の音声専用コールがビデオにエスカレーションするか、またはビデオ ストリームが音声専用コールに追加されると、ビデオ エスカレーションが発生します。デエスカレーションはこれとは逆で、ビデオ コールが音声専用コールにダウングレードすることです。

RSVP SIP プレコンディションを使用してクラスタ全体でビデオ エスカレーションおよびデエスカレーションをサポートするため、Unified CM は SIP Session Description Protocol（SDP）内の SIP プレコンディションで 2 つのメディア回線（M 回線）を通知します。1 つはオーディオ ストリーム用で、もう 1 つはビデオ ストリーム用です。音声とビデオ用にそれぞれ別のメディア回線を用意すると、SIP シグナリングに各ストリーム独自の RSVP ポリシーおよびステータスを確保できます。Unified CM ではオーディオ ストリームとビデオ ストリームに独自のプレコンディション属性が用意されているため、RSVP ポリシーを容易にプレコンディションにマッピングできます。この機能により、Unified CM は

オーディオ ストリーム予約の正常完了ステータスを渡す一方で、同時に [Mandatory (Video Desired)] のポリシーによるビデオ ストリーム予約の失敗ステータスも渡すことができるため、コール全体を拒否するのではなくコールをビデオ コールから音声専用コールにダウングレードできます。

RSVP SIP プレコンディションのために予約されるビデオ帯域幅は、リージョン ペア間に設定された値となります。この場合は、エンドポイントのリージョンと SIP クラスタ間トランク リージョンです。ビデオ チャネルの確立後に、ビデオ帯域幅が調整されます。リージョン ペア間の 2 つのエンドポイントでネゴシエートする際に想定されるビット レート以上のビデオ帯域幅にすることを推奨します。

コール中のビデオ エスカレーションの場合、ビデオ ストリームはビデオ帯域幅が予約されたあとにだけセットアップされます。

ビデオ コールの保留/保留解除中、保留音に接続しつつ、ビデオと音声の帯域幅が引き続き予約されます。

転送など他の付加サービスの場合、オーディオ ストリームのセットアップ完了後に、Unified CM はビデオ予約およびビデオ ストリーム セットアップをトリガーします（これは、遅延ビデオ エスカレーションとも呼ばれます）。

例 11-1　遅延ビデオ エスカレーション：RSVP SIP プレコンディションを使用した音声専用からビデオ コールへのコールの転送

クラスタ A のビデオ デバイス A が、RSVP SIP プレコンディションを有効にして SIP トランク経由でクラスタ B のオーディオ デバイス B をコールします。コールは音声コールとしてセットアップされ、そのオーディオ ストリームが AudioStream Application ID および Per Hop Behavior（PHB）値 EF とともに音声プールに割り当てられます。

デバイス B が、クラスタ B のビデオ デバイス C にコールを転送します。A と C 間のオーディオ ストリームが、まず AudioStream Application ID および PHB 値 EF とともに音声プールに確立されます。

オーディオ メディア接続が正常に完了したあとにだけ、A と C との間に遅延ビデオ エスカレーションが発生します。ビデオ ストリームは、VideoStream Application ID とともにビデオ プールに割り当てられます。ビデオ ストリーム割り当てが失敗した場合、コールは AudioStream Application ID および PHB 値 EF 付きの音声専用コールのままとなります。ビデオ ストリーム予約が成功した場合、オーディオ ストリームは VideoStream Application ID とともに音声プールからビデオ プールに再許可されます。再許可が成功すると、ビデオ ストリームとオーディオ ストリームで VideoStream Application ID が PHB 値 AF41 に設定されます。一方、再許可が失敗すると、ビデオ ストリームでは VideoStream Application ID が PHB 値 AF41 に設定され、オーディオ ストリームでは VideoStream Application ID が PHB 値 0 に設定されます（ビデオ失敗のベストエフォート値）。

Unified CM および RSVP SIP プレコンディションのベスト プラクティスおよび設計上の考慮事項：

- SIP トランクには、常にロケーション間とロケーション内の両方の RSVP ポリシーが必要です。ロケーション間ポリシーでは、着信コールと発信コールに正しい RSVP ポリシーを設定します。ロケーション内ポリシーでは、（クラスタ間の転送操作および自動転送操作のために）同じトランクにヘアピンされたコールにエンドツーエンド RSVP ポリシーを確保します。
- [Mandatory] または [Mandatory (Video Desired)] の RSVP ポリシーを設定することを推奨します。これらの設定では、帯域幅の予約とコールの音声品質が保証されます。
- SIP トランク プロファイルで [SIP Rel1XX Options] フィールドを [Send PRACK if 1XX contains SDP] に設定することを推奨します。RSVP SIP プレコンディション操作には SIP PRACK メッセージが必要ですが、1XX メッセージが SDP を含む場合にかぎられます。

- RSVP SIP プレコンディションの配置での各クラスタの設定をソリューション全体で標準化して、RSVP Agent だけでなく WAN 全体で使用する RSVP クラスタ サービス パラメータ、ロケーション間ポリシー、およびコーデックを同じものにします。コールの確立を試行しているときに、クラスタ間で機能または設定に不整合がないようにすることが重要です。
- Unified CM で RSVP SIP プレコンディションを使用している場合、次のガイドラインおよび制限の下、クラスタ間でシェアド ラインへの終端がサポートされます。
  - クラスタ間でシェアド ラインへのコールを設定するとき、発信側デバイスの RSVP Agent とシェアド ライン デバイスに最初に割り当てられた RSVP Agent との間で RSVP 予約が発生します（これは、プログラミングで制御できません）。別のロケーションでこのシェアド ラインを使用する他のすべてのデバイスは RSVP Agent を割り当てるだけで、予約を確立することはありません。
  - シェアド ラインのデバイスが 1 つ以上存在する各ロケーションに RSVP Agent を 1 つ割り当てます。
  - 最初に割り当てた RSVP Agent があるデバイスがコールに応答するデバイスである場合、コールの確立が実行され、他のロケーションの他のシェアド ライン デバイスに割り当てた RSVP Agent が解放されます。
  - 予約を確立していないデバイスがコールに応答した場合、発信側デバイスの RSVP Agent と応答したデバイスに割り当てられた RSVP Agent との間で、オプションの RSVP ポリシーを使用して新しい予約が開始されます。RSVP Agent は、予約が正常に完了するまでコール期間中予約の確立を続けます。コールがオプションのポリシーの制約下にある間、[Mandatory RSVP mid call error handle option] が [Call becomes best effort]（デフォルト）に設定され、予約が成功するまで 2 つのデバイス間のメディア ストリームがベストエフォート型にマーキングされます。予約が成功すると、メディアは Per Hop Behavior（PHB）値 EF（音声）または AF41（ビデオ）に再マーキングされます。
  - 最初に割り当てた RSVP Agent があるデバイスで、必須のポリシーによる RSVP 予約が失敗した場合、そのデバイスでもそのロケーションにあるどのデバイスでも呼び出し音が鳴りません。ただし、他のすべてのロケーションにあるシェアド ライン デバイスでは呼び出し音が鳴ります。
- 上のシェアド ライン制限に基づいて、シェアド ラインを同じロケーション内のデバイス グループに制限することを推奨します。
- Unified CM で RSVP SIP プレコンディションを使用している場合、次のガイドラインおよび制限の下、モバイル コネクト宛先（リモート接続先）への終端がサポートされます。
  - ローカル RSVP：発信側デバイス、ゲートウェイ、またはトランクからリモートとなるデバイス、ゲートウェイ、またはトランクへのリモート接続先には、シェアド ラインのサポートで述べたように同じ規則を適用します。
  - エンドツーエンド RSVP：単一回線でつながるリモート接続先では、複数の RSVP SIP プレコンディションの宛先を指さないようにします。Unified CM は、リモート接続先につながる回線ごとに RSVP SIP プレコンディション コールを 1 つだけサポートします。
- MoH サーバが保留側（別の相手を保留中のユーザ）と同じロケーションにある場合、初期予約が再利用され、新しい予約は確立されません。
- 保留 / 保留解除機能で RSVP SIP プレコンディションを使用すると、エンドポイント間および RSVP Agent 間でメディア ストリームが遮断されるものの、予約は確保されます。
- sRTP は RSVP SIP プレコンディションに対応しており、メディア セットアップ中と RSVP 予約後にネゴシエートされます。プレコンディション段階では、Unified CM は RTP/SAVP および暗号属性を通知しません。

- T.38 は RSVP SIP プレコンディションに対応しており、T.38 FAX 転送をサポートする SIP、H.323、MGCP の各エンドポイントからネゴシエートされます。Unified CM は、リージョン間音声帯域幅（エンドポイントと SIP クラスタ間トランクとの間）を使用して、初期予約をネゴシエートします。コールの確立後および T.38 の切り替え時に、帯域幅の使用量がまだ設定されていない場合は 80 kbps に再調整されます。
  - 制限：リージョン間ビット レートを 80 kbps 未満に設定した場合は、T.38 の切り替え後に、RSVP 予約が 80 kbps に再調整されます。このことが原因で、新たに調整した帯域幅を予約できない場合には障害が発生することがあります。このような場合、切り替え後に予約が失敗しても、コールの処理が継続されます。Unified CM が SIP クラスタ間トランクでこの障害を通知しないためです。
  - 前述の理由から、RSVP SIP プレコンディションを使用して T.38 FAX を配置するときは、RSVP SIP プレコンディションが有効になっている T.38 エンドポイントとクラスタ間トランクとの間のリージョン間オーディオ ビット レートとして 80 kbps を使用することを推奨します。
- 保留 / 保留解除、転送、会議などの付加サービス、保留音サーバ、Annunciator、カンファレンス ブリッジなどのメディア リソースで RSVP SIP プレコンディションをサポートするには、それぞれのデバイス プールの Media Resource Group List（MRGL; メディア リソース グループ リスト）にローカル RSVP Agent を割り当てる必要があります。

（注）　保留 / 保留解除、転送、会議などの付加サービスのさまざまなコール フローで、数種類のメディア リソースが RSVP SIP プレコンディション コールに投入されます。カンファレンス ブリッジ、保留音サーバ、Annunciator などのメディア リソースでも、他のデバイスが RSVP SIP プレコンディションまたは RSVP 対応ロケーション コールに呼び出されるときと同じく、RSVP Agent 関連付けが必要になります。このようなメディア リソースは、設定済みのデバイス プールに関連付けられたメディア リソース グループ リストから RSVP リソースを取得します。

クラスタ間のエクステンション モビリティのアーキテクチャおよび考慮事項

Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）を使用すると、あるクラスタのユーザが別のクラスタの IP Phone にログインできます。クラスタ間のエクステンション モビリティの機能、ハイ アベイラビリティ、およびスケーラビリティの詳細については、「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10）を参照してください。EMCC 機能はコール アドミッション制御にも当てはまることであるため、この項で取り上げます。また、「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10）で取り上げている情報を理解していることが前提となります。

EMCC 配置では、RSVP SIP プレコンディションを使用した RSVP 対応ロケーションというのが、唯一サポートされるコール アドミッション制御の形式となります。静的ロケーションベースのコール アドミッション制御はサポートされず、EMCC 環境では機能しません。

EMCC および RSVP 対応環境

RSVP 対応ロケーション（単一クラスタまたはクラスタ内の場合）または RSVP SIP プレコンディション（分散型クラスタまたはクラスタ間の場合）を使用した Unified CM RSVP 対応配置では、IP Phone に代わって RSVP シグナリングを実施するために、Unified CM がローカル RSVP Agent をコール フローに呼び出す必要があります。これを EMCC 環境で実現するには、Unified CM クラスタ間で呼制御情報を渡して、リモートからログインした EMCC ユーザが RSVP でクラスタ内とクラスタ間の両方のコールを発信できるようにします。

EMCC 配置には、任意のログインまたは登録操作用に常に 2 つのクラスタがあります。EMCC ユーザ側から見ると、これはホーム クラスタと Visiting クラスタになります（図 11-32 を参照）。ホーム クラスタは、ユーザが元々所有するクラスタで、ユーザ情報が格納されます。Visiting クラスタは、電話機が元々所有するクラスタで、クラスタ間をローミングする EMCC ユーザのログイン先であり、デバイス情報が格納されます。

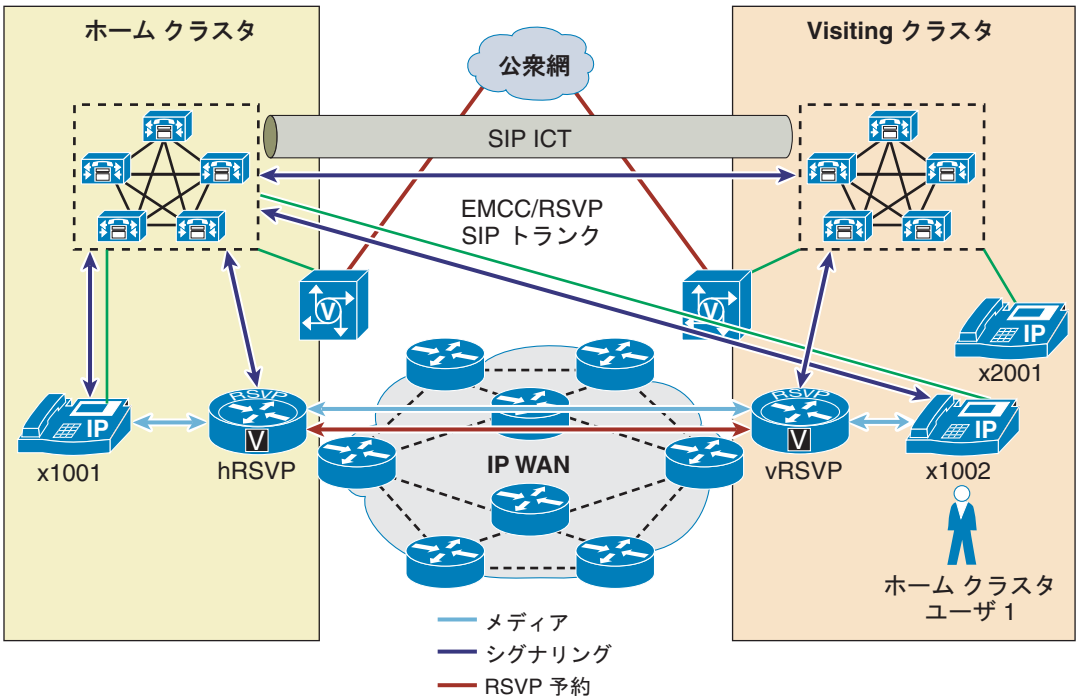
ユーザが Visiting クラスタの電話機（Visiting 電話機）にログインすると、その電話機が直接 EMCC ユーザのホーム クラスタに登録されます。その後、そのユーザおよび Visiting 電話機から発信されるすべてのコールが、ホーム クラスタの呼制御から発信されます。このため、ホーム クラスタが Visiting 電話機を管理し、Visiting 電話機に EMCC ローミング デバイス プールを提供します（EMCC ローミング デバイス プールの詳細については、「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10）を参照してください）。

ホーム クラスタは、必要に応じて RSVP Agent に代わって Visiting クラスタに要求を送ります。その際、（特に SIP REFER メッセージでは）2 つのクラスタ間で EMCC 対応 SIP トランクが使用されます。Visiting クラスタから RSVP Agent への要求が発生するのは、エンドポイントからのコールに RSVP Agent が必要であるとホーム クラスタが判断したときだけです。ホーム クラスタは、（EMCC ローミング デバイス プールの）Visiting 電話機のロケーション（着信側デバイス、ゲートウェイ、またはトランク）と着信側のロケーションとの間のロケーション間 RSVP ポリシーを基にその判断を下します。

RSVP ポリシーが決まると、Visiting 電話機の Visiting クラスタから RSVP Agent への要求が発生します。RSVP Agent へのこの要求で、ホーム クラスタはデバイス名（sep*xxxxxxxxxxxx*）を送信して、Visiting クラスタがデバイス名を検索して（デバイス自体またはデバイス プールに関する MRGL から）RSVP Agent を特定できるようにします。ホーム クラスタは、RSVP Agent を Visiting 電話機に関連付けるための情報を入手すると、ローカル RSVP コール（クラスタ内の RSVP 対応ロケーション）または RSVP SIP プレコンディション コール（クラスタ間）を確立するための手順を開始できます。

図 11-32 に、SIP 対応トランク経由で RSVP を使用した EMCC コールに関与する各種コンポーネント間のシグナリング接続およびメディア接続を示します。

図 11-32　SIP 対応トランク経由で RSVP を使用した EMCC コール



ベスト プラクティス

- EMCC ローミング デバイス プール ロケーションと他のすべてのロケーションとの間のロケーション ポリシーを [Mandatory (Video Desired)] に設定します。
- RSVP 対応ロケーションベースのコール アドミッション制御を機能させてから、EMCC で RSVP SIP プレコンディションを使用できるようにします。
- EMCC ユーザがログインできる IP Phone には、ローカル RSVP Agent を関連付ける必要があります。

Unified CM の相互運用性と機能の考慮事項

ここでは、Unified CM と Cisco IOS ゲートウェイと Unified CME との相互運用性の考慮事項について説明します。

Cisco IOS ゲートウェイと Unified CME

Cisco IOS SIP/TDM ゲートウェイと Cisco Unified Communication Manager Express（Unified CME）のどちらも、RSVP SIP プレコンディションをサポートします。このサポートにより、SIP シグナリングで RSVP ポリシーを通知して、Unified CM と Cisco IOS SIP/TDM ゲートウェイまたは Unified CME との間に音声専用コールを確立できます。

Cisco IOS での SIP RSVP 機能および SIP/TDM Cisco IOS ゲートウェイおよび Unified CME で RSVP SIP プレコンディション機能を使用する際の制約事項の詳細については、次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

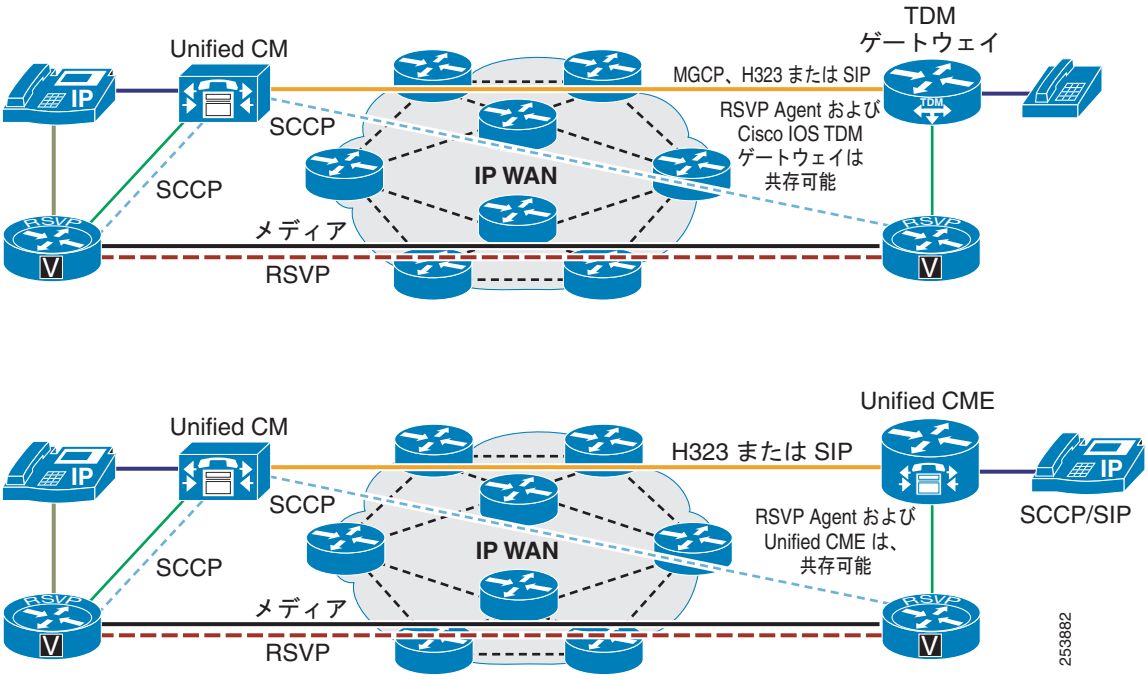
RSVP 配置で Cisco IOS ゲートウェイと Unified CME との相互運用性を確保するときに、Unified CM には 2 つの設定モードがあります。MGCP、H.323、および SIP コール シグナリングをサポートするローカル RSVP と、SIP シグナリングだけをサポートするエンドツーエンド RSVP です。Cisco IOS ゲートウェイと Unified CME との相互運用性を確保するときに、Unified CM はどちらの動作方法もサポートできます。ただし、どちらの方法を使用するにしても、以降の項で説明するように、いくつか検討すべき事項があります。

Cisco IOS ゲートウェイおよび Unified CME での Unified CM とローカル RSVP

ローカル RSVP モードでは、Unified CM は MGCP、H.323、または SIP コール シグナリング プロトコル対応の Cisco IOS TDM ゲートウェイとの相互運用性、および H.323 または SIP 対応の Unified CME との相互運用性をサポートします。このモードでは、Unified CM はゲートウェイを宛先または発信元としてコールが確立されると RSVP Agent を Cisco IOS TDM ゲートウェイに割り当てます。また、プレコンディションおよび RSVP ポリシーを Cisco IOS TDM ゲートウェイに通知しません。これは、Unified CM での MGCP、H.323、および SIP のデフォルト設定です。

図 11-33 に、Unified CM のローカル RSVP と、Cisco IOS TDM ゲートウェイおよび Unified CME との統合を示します。

図 11-33　Unified CM のローカル RSVP と、Cisco IOS TDM ゲートウェイおよび Unified CME との統合



利点

このモデルには、次の利点があります。

- 多種多様な Cisco IOS ゲートウェイ シグナリング プロトコル（MGCP、H.323、SIP）のサポート。
- SIP と SCCP Unified CME の両方のエンドポイントのサポート。
- Unified CM の RSVP ポリシーおよびアプリケーション ID の集中管理。
- コール転送や自動転送の付加サービス シナリオでは、Cisco IOS TDM ゲートウェイで MGCP を使用すると、メディア パスが最適化されます。ローカル システム（Cisco IOS TDM ゲートウェイ）からコールが転送または自動転送された場合、メディアとシグナリングの両方とも終了したあと、転送または自動転送側に対して再確立されます。

欠点

このモデルには、次の欠点があります。

- RSVP Agent セッションを使用します（ソフトウェアまたはハードウェアによるセッション。どちらになるかは、セッション トランスコーディングなどの機能とセッション要件によって決まります）。
- 転送および自動転送付加サービス シナリオでは、Cisco IOS TDM ゲートウェイおよび Unified CME で H.323 と SIP を統合した場合、メディア パスが最適化されません。つまり、ローカル システム（Cisco IOS TDM ゲートウェイまたは Unified CME）からのコール転送または自動転送により、メディアとシグナリングの両方ともローカル システムにヘアピンされて、二重に帯域幅を消費することになります。

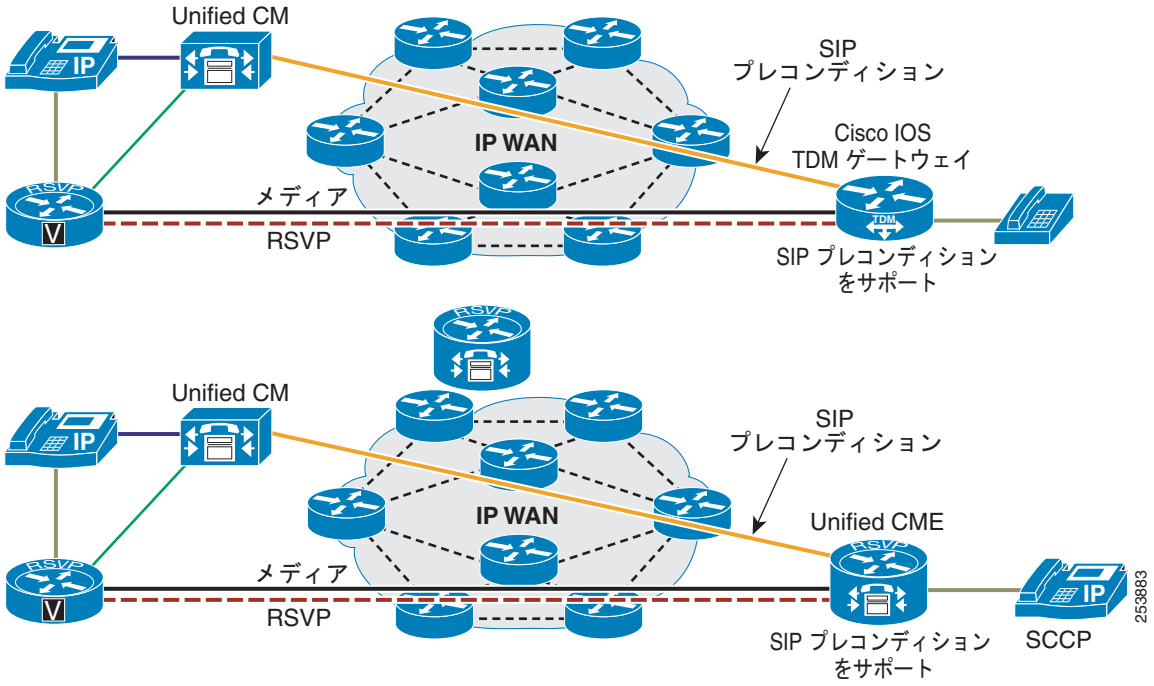
この方法では、「Unified CM の RSVP 対応ロケーション」（P.11-38）の項で説明するように、クラスタ内コール アドミッション制御が機能します。

Cisco IOS ゲートウェイおよび Unified CME での Unified CM とエンドツーエンド RSVP または RSVP SIP プレコンディション

エンドツーエンド RSVP モードでは、Unified CM は RSVP SIP プレコンディション シグナリングを使用して、Cisco IOS ゲートウェイおよび Unified CME との相互運用性をサポートします。このモードでは、Unified CM は RSVP Agent を割り当てません。Cisco IOS ゲートウェイまたは Unified CME は、ネイティブに RSVP をサポートします。この方法は、Cisco Integrated Services Router（ISR; サービス統合型ルータ）での RSVP Agent ソフトウェア セッションの使用率を削減します。

図 11-34 に、Unified CM と、Cisco IOS TDM ゲートウェイまたは Unified CME との RSVP SIP プレコンディション統合を示します。

図 11-34　Unified CM と、Cisco IOS TDM ゲートウェイまたは Unified CME との RSVP SIP プレコンディションの統合



利点

このモデルには、次の利点があります。

- RSVP SIP プレコンディションのサポート。
- SIP Cisco IOS TDM ゲートウェイまたは Unified CME に RSVP Agent リソースを使用しません。

欠点

このモデルには、次の欠点があります。

- SCCP Unified CME エンドポイントだけをサポートします。
- SIP トランク実装だけをサポートします。
- 転送および自動転送付加サービス シナリオでは、メディア パスが最適化されません。つまり、ローカル システム（SIP Cisco IOS TDM ゲートウェイまたは Unified CME）からのコール転送により、メディアとシグナリングの両方ともローカル システムにヘアピンされて、二重に帯域幅を消費することになります。

Unified CM と SIP Cisco IOS TDM ゲートウェイおよび Unified CME との相互運用に関する設計の考慮事項

ローカル RSVP とエンドツーエンド RSVP のどちらかの配置を選択するときは、次の基準に基づいて最適なオプションを判断してください。

- 目的のコール シグナリング プロトコル（H.323、MGCP、または SIP）。ダイヤル プラン、PBX 相互運用性、コール シグナリング機能など、コール アドミッション制御の範囲外の数多くの要件に基づいて判断します。
- ローカル システム（SIP Cisco IOS TDM ゲートウェイおよび Unified CME）からリモートの宛先へのコールの転送および自動転送に必要な付加サービス。たとえば、コールを WAN 経由で中央のボイス メッセージ環境に転送する場合に、これらのサービスが必要になります。
- ソリューションの管理。RSVP ポリシーおよびアプリケーション ID の集中管理と分散管理のどちらかを選択します。
- リソース使用率。RSVP Agent セッションとネイティブ RSVP の使用率を比較検討します。セッション数によっては専用のプラットフォームが必要になることがあり、その場合 SIP Cisco IOS TDM ゲートウェイまたは Unified CME にセッションを確立できません。
- RSVP SIP プレコンディションをサポートする SIP Cisco IOS TDM ゲートウェイまたは Unified CME を指す SIP トランクを Unified CM に設定する場合、トランクには常にロケーション間とロケーション内の両方の RSVP ポリシーを設定します。ロケーション間ポリシーでは、着信コールと発信コールに正しい RSVP ポリシーを設定します。ロケーション内ポリシーでは、（転送および自動転送操作のために）同じトランクにヘアピンされたコールにエンドツーエンド RSVP ポリシーを確保します。
- Unified CM では、単一クラスタに設定されたすべての Cisco IOS TDM ゲートウェイおよび Unified CME に適用できるロケーションを 1 つ別途設定することを推奨します。そのロケーションでは、他のすべてのロケーションとともに、ロケーション間 RSVP ポリシー セットを [Mandatory] または [Mandatory (Video Desired)] に設定します。このような環境で RSVP SIP プレコンディションを正しく機能させるには、RSVP ポリシーが必要です。

（注） SIP Cisco IOS TDM ゲートウェイと物理的に同じ LAN にある IP Phone でも、自身のロケーションと SIP トランク上のロケーションとの間に RSVP ポリシーが必要です。このため IP Phone に RSVP Agent リソースが使用されますが、RTP ストリームがローカルのままであるため WAN の帯域幅が差し引かれません。

- Unified CM に設定した RSVP ポリシーを Cisco IOS TDM ゲートウェイに設定したポリシーと一致したものにします。SIP Cisco IOS TDM ゲートウェイまたは Unified CME に対して RSVP 予約を有効にする場合は、**ダイヤル ピア**設定で次のオプションを使用します。

```
req-qos guaranteed-delay audio
acc-qos guaranteed-delay audio
```

この設定を行うと、各音声コールに対して、SIP Cisco IOS TDM ゲートウェイは遅延保証付きのサービスを使用して RSVP 予約を要求します。要求された QoS と許容可能な QoS の両方がこの RSVP サービスを指定している場合、コールが成功するためには RSVP 予約が必須になります（予約を確立できない場合はコールが失敗します）。

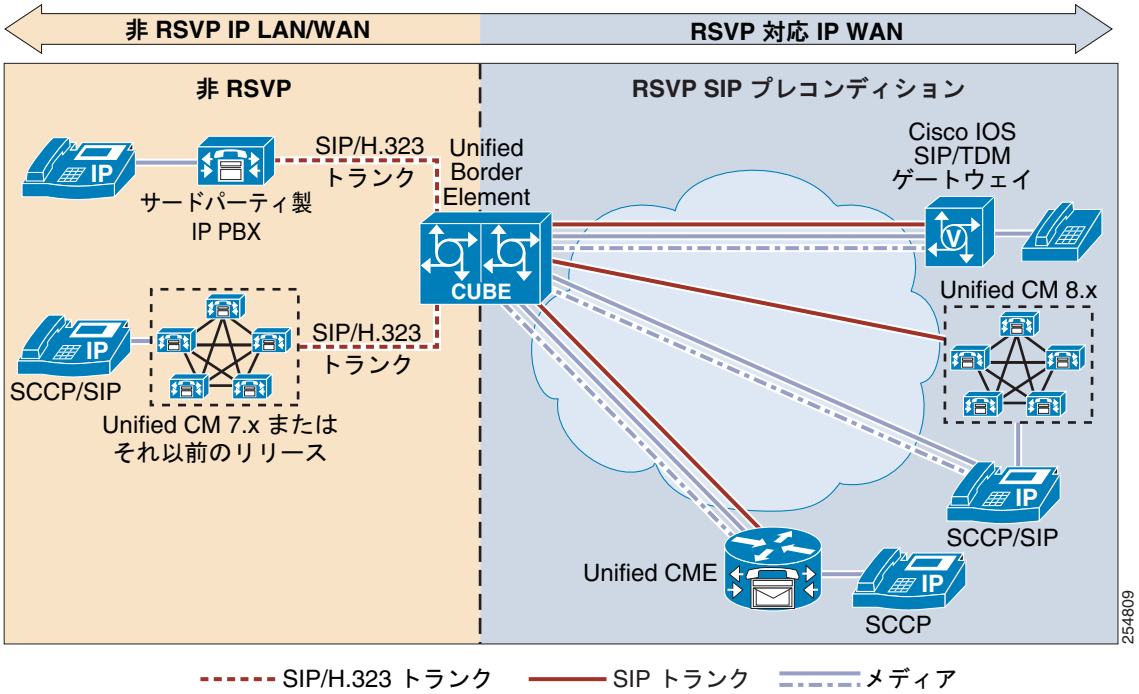
- Unified CM に設定したアプリケーション ID を Cisco IOS TDM ゲートウェイおよび Unified CME に設定したアプリケーション ID と一致したものにします。
- SIP プレコンディションとともに設定した適切なダイヤル ピアが使用されるように、着信と発信のダイヤル ピアを正確に一致させます。詳細については、次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』を参照してください。

  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

Cisco Unified Border Element および RSVP SIP プレコンディション

Cisco Unified Communications システムの 8.5 以降のリリースでは、Cisco Unified Border Element は音声のみのコールで RSVP SIP プレコンディションをサポートしています。このサポートにより、企業は非 RSVP 呼制御アプリケーションを RSVP SIP プレコンディション インフラストラクチャと統合するために Unified Border Element を使用できます。呼制御の非 RSVP 側では、Unified Border Element は H.323 と SIP 両方との統合をサポートしています。コールの RSVP 側では、SIP と RSVP を一緒に使用して Unified CM、Unified CME、および SIP-TDM Cisco IOS ゲートウェイなどの RSVP プレコンディション呼制御と統合できます。図 11-35 はこのタイプのインターワーキングを示しています。

図 11-35　SIP トランクを介した RSVP での Cisco Unified Border Element



呼制御の非 RSVP 側の SIP 統合では、Unified Border Element でアーリー オファーまたはディレイド オファーのいずれかがサポートされます。また、H.323 統合では、Fast Start または Slow Start のいずれかがサポートされます。呼制御の RSVP SIP プレコンディション側では、呼制御アプリケーションを介して RSVP ポリシーをネゴシエートするのに必要なプレコンディションを提供するため、SIP アーリー オファーが常に送信されます。したがって、RSVP SIP プレコンディションは常にアーリー オファーです。

詳細については、次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

Service Advertisement Framework（SAF）および Call Control Discovery（CCD）

Cisco Service Advertisement Framework（SAF）を使用すると、ネットワーク アプリケーションで IP ネットワーク内のネットワーク サービスに関する情報をアドバタイズしたり検出したりできます。Call Control Discovery（CCD; コール制御ディスカバリ）は SAF を使用して、Unified CM、Unified CME などの呼制御エージェントによってホストされる内部 Directory Number（DN; ディレクトリ番号）の可用性に関する情報を配布および維持します。また、CCD は、これらの内部ディレクトリ番号に公衆網から到達できるようにする対応した番号プレフィックスも配布します（「To PSTN」プレフィックス）。

ここでは、RSVP SIP プレコンディションの配置に関係する SAF CCD について説明します。Service Advertisement Framework およびコール制御ディスカバリの詳細については、「ネットワーク インフラストラクチャ」（P.3-1）、「Unified Communications の配置モデル」（P.5-1）、「ダイヤル プラン」（P.9-1）の各章を参照してください。

SAF CCD と RSVP SIP プレコンディションが連携して動作するため、移動、追加、および変更の動的なダイヤル プランと複雑なマルチホーム多層ネットワーク向けのトポロジ対応コール アドミッション制御方式を容易に管理できます。これにより、静的なゲートキーパー インフラストラクチャを動的に置換して、ネットワークの変更に応じたダイヤル プラン解決およびコール アドミッション制御を実現できます。

SAF CCD が RSVP SIP プレコンディション コール アドミッション制御と連携して動作するため、予約が失敗しても宛先に到達するための代替ルートを確保できます。この機能は、コール制御ディスカバリ自動公衆網フェールオーバーと呼ばれます。

コール制御ディスカバリ自動公衆網フェールオーバー

SAF CCD は、特定のコールに対して IP ルートを 1 つだけ選択できるという点で、標準のコール ルーティングとは異なります。一方、標準のコール ルーティングでは、ルート リストおよびルート グループを使用して、単一のコールに複数の IP パスを定義し、連続して試行できます。SAF 学習ルートを使用してコールを発信する場合、次のオプションを選択できます。

- 選択した IP パスを取得して、着信番号に到達します。
- IP パスが使用できない場合、公衆網プレフィックスを使用して、着信番号と、発信側デバイスの Automatic Alternate Routing（AAR; 自動代替ルーティング）Calling Search Space（CSS; コーリング サーチ スペース）を変更し、公衆網経由でコールをルーティングします。

SAF 学習ルートで RSVP SIP プレコンディションを使用し、予約が成功した場合、RSVP を使用して IP パスに確立する通常の手順どおりにコールが確立されます。ただし、IP ルートでの予約が失敗し、Precondition Failure or Reservation Failure（SIP メッセージ 580）または Precondition Unsupported（SIP メッセージ 420）のコール終了原因コードが返された場合は、CCD 自動公衆網フェールオーバーが発生します（フェールオーバーは、次に説明するように、他のコール終了原因コードで発生することもあります）。CCD 自動公衆網フェールオーバーは、コール アドミッション制御障害のために SAF CCD IP ルートが失敗すると発生するという点で、自動代替ルーティング（「Automated Alternate Routing」（P.9-103）を参照）に似ています。AAR も同じく、クラスタ内コール アドミッション制御の障害時に発生します。ただし、CCD 自動公衆網フェールオーバーは、コール アドミッション制御とは別のルーティング障害でも発生することがあるという点で、AAR とは異なります。コールがアラート段階に入る前に学習パターンへのコールが失敗し、コール終了原因コードが通常のコールのクリア、ユーザ ビジー、宛先故障、番号未割り当て、またはジオロケーション不一致以外のものであると、CCD 自動公衆網フェールオーバーが発生します。

CCD 自動公衆網フェールオーバーは、AAR CSS と（CCD が分配する）「To PSTN」プレフィックスを使用して、コールを再ルーティングします。これにより、管理者はローカル コール アドミッション制御で AAR コールの再ルーティングを実現するために、CCD 自動公衆網フェールオーバー用のものと同じサービス クラスを利用できます。主な違いは、CCD 自動公衆網フェールオーバーは AAR プレフィックスではなく SAF CCD 分配機能が提供するプレフィックス（「To PSTN」プレフィックス）を使用することです。

図 11-36 に、RSVP SIP プレコンディション コール アドミッション制御で障害が発生したあとの CCD 自動 PSTN フェールオーバーを示します。

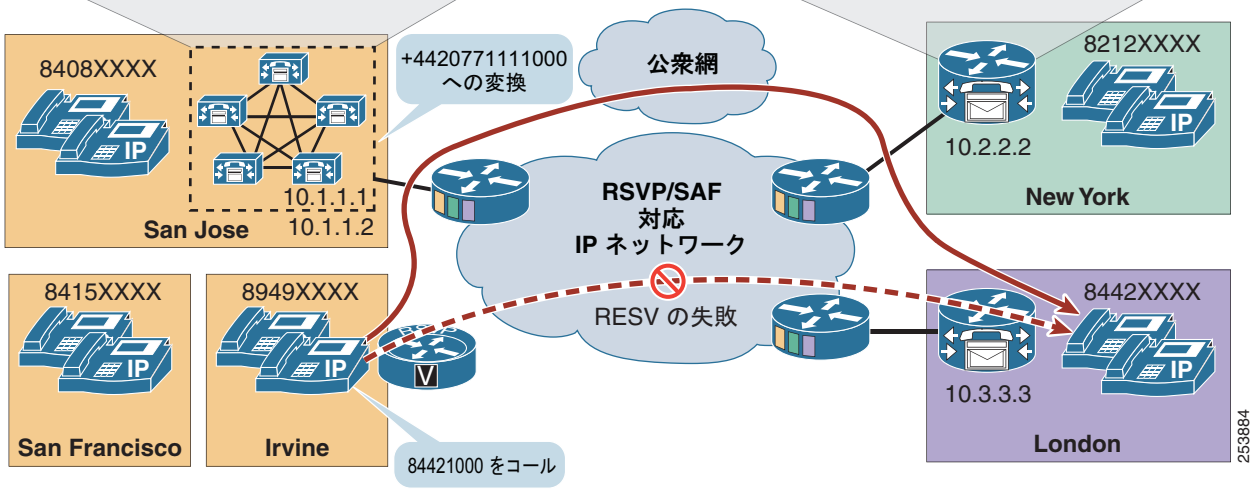
図 11-36　RSVP SIP プレコンディションでの CCD 自動 PSTN フェールオーバー

New York Unified CME ルーティング テーブル

DN パターン	「対 DID」規則	IP アドレス	プロトコル
8408XXXX	+1408555 /4	10.1.1.1/2	SIP
8408XXXX	+1408555 /4	10.1.1.1/2	H.323
8415XXXX	+1415777 /4	10.1.1.1	SIP
8949XXXX	+1949222 /4	10.1.1.1	SIP
8442XXXX	**4:+442077111 /4**	**10.3.3.3**	**SIP**

San Jose Unified CM ルーティング テーブル

DN パターン	「対ダイヤルイン方式（DID）」規則	IP アドレス	プロトコル
8212XXXX	4:+1212444	10.2.2.2	H.323
8442XXXX	**4:+442077111**	**10.3.3.3**	**SIP**



また、SAF CCD 学習ルートによる CCD 自動公衆網フェールオーバーと、静的なルート パターンを使用したルート リストおよびルート グループ機能による再ルーティングとでは、機能に違いがあります。ルート グループおよびルート リストを指す静的なルート パターンを使用した場合、RSVP SIP プレコンディションの予約で障害が発生すると、Unified CM はルート グループおよびリストで次に設定されているトランクまたはゲートウェイにコールをルーティングします。

（SAF と静的なルート パターンを使用した）いずれの場合でも、コール アドミッション制御で障害が発生したら、コールをローカル ルート グループにルーティングすることを推奨します（ローカル ルート グループの詳細については、「ローカル ルート グループ」（P.9-13）を参照してください）。CCD 自動公衆網フェールオーバー機能のコンストラクトでこれを実行する必要があります。発信側の AAR CSS にコーリング サーチ スペースを正しく設定することが重要です。これにより、CCD 自動フェールオーバーの際、コールはルート パターンに送信されます。ルート パターンのローカル ルート グループ機能が働き、コールはローカル ゲートウェイにルーティングされます。このルート パターンとして特にすべての CCD 自動フェールオーバー条件用の catch-all パターンを使用して、コールを発信側のローカルなゲートウェイにルーティングできます。

Cisco Unified SIP Proxy の考慮事項

Cisco Unified SIP Proxy は、ルーティングおよび SIP シグナリング正規化を集中して行える高性能かつハイ アベイラビリティのステートレスな Session Initiation Protocol（SIP）サーバです。呼制御ドメイン間で要求を転送することにより、Cisco Unified SIP Proxy は企業ネットワークおよびサービス プロバイダー ネットワーク内でセッションをルーティングできます。Cisco Unified Communications 配置での Unified SIP プロキシの主な目的は、SIP シグナリング、SIP 正規化、およびダイヤル プラン集中化を統合することです。Cisco Unified SIP Proxy とその機能の詳細については、次の Web サイトで入手可能なドキュメントを参照してください。

http://www.cisco.com/en/US/prod/collateral/modules/ps2797/data_sheet_c78-521390_ps2797_Products_Data_Sheet.html

RSVP SIP プレコンディションの環境では、Unified SIP Proxy は単にさまざまな SIP メッセージの SDP 部分に含まれるプレコンディションを伝えるだけで、プレコンディションにはいっさい変更を加えません。

Adaptive Security Appliance（ASA）の考慮事項

RSVP SIP プレコンディションを使用して、Unified CM、Unified CME、Unified SIP Proxy、Cisco IOS SIP/TDM ゲートウェイなどの Cisco Unified Communications コール処理アプリケーション間に Cisco ASA を配置するときは、次の両方の検査が必要です。

- SIP 検査

  SIP 検査では、どの Cisco SIP シグナリング製品でも SIP シグナリングが ASA を通過できるようにします。ASA はその後、さまざまな SIP メッセージの SDP に記録されている適切なメディア ピンホールを開きます。これは、ASA が RSVP Agent 間のメディア パスにあり、その RSVP Agent が帯域幅を予約中であり、かつ Unified Communications エンドポイントのメディア フローの発信元になっているときに重要です。

- IP オプション検査

  IP オプション検査では、RSVP Agent から RSVP Agent への RSVP シグナリングが ASA を通過できるようにします。どの RSVP メッセージでも、各パケットの IP ヘッダーに [IP Router Alert Option] を設定します。IP オプション検査で [IP Router Alert Option] を許可して、このようなパケットが ASA を通過できるようになっていないかぎり、ASA はデフォルトではこのようなパケットをドロップします。

ASA Software Release 8.3 では、RSVP SIP プレコンディション実装に固有の SIP 検査と IP オプション検査の両方をサポートしています。SIP シグナリングの検査や RSVP パケットの受け渡しのために ASA が必要になる RSVP SIP プレコンディションの配置では、互換性を確保するため、ASA 8.3 以降のソフトウェア リリースを使用する必要があります。

SIP 検査および IP オプション検査用に ASA を設定する方法の詳細については、次の Web サイトで入手可能な『*Cisco ASA 5500 Series Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

コール アドミッション制御の設計上の考慮事項

ここでは、各種の Unified CM コール処理配置モデルおよび次の IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。

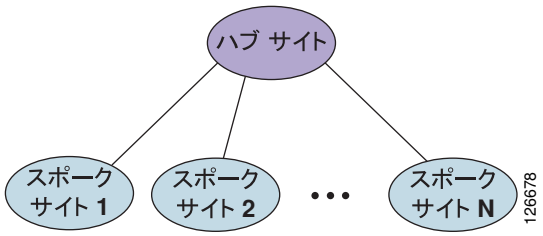
- 「単純なハブアンドスポーク トポロジ」（P.11-69）
- 「2 層ハブアンドスポーク トポロジ」（P.11-73）
- 「単純な MPLS トポロジ」（P.11-77）
- 「汎用トポロジ」（P.11-83）

これらの項では、採用する Unified CM 配置モデルに基づいて、トポロジごとにそれぞれ別の設計考慮事項を示します。

単純なハブアンドスポーク トポロジ

図 11-37 に、スター トポロジとも呼ばれる単純なハブアンドスポーク トポロジを示します。このタイプのネットワーク トポロジでは、すべてのサイト（*スポーク サイト*と呼ばれる）が、1 つの IP WAN リンクを通じて中央サイト（*ハブ サイト*と呼ばれる）に接続されます。スポーク サイト間には直接のリンクが存在しないため、スポーク サイト間の通信は、すべてハブ サイトを経由する必要があります。

図 11-37　　単純なハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する単純なハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、「単純な MPLS トポロジ」（P.11-77）の項を参照してください。

以降では、採用する Unified CM 配置モデルごとに、単純なハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.11-70）

  1 つまたはそれ以上の Unified CM クラスタをハブ サイトに配置し、スポーク サイトには電話とゲートウェイだけを配置します。

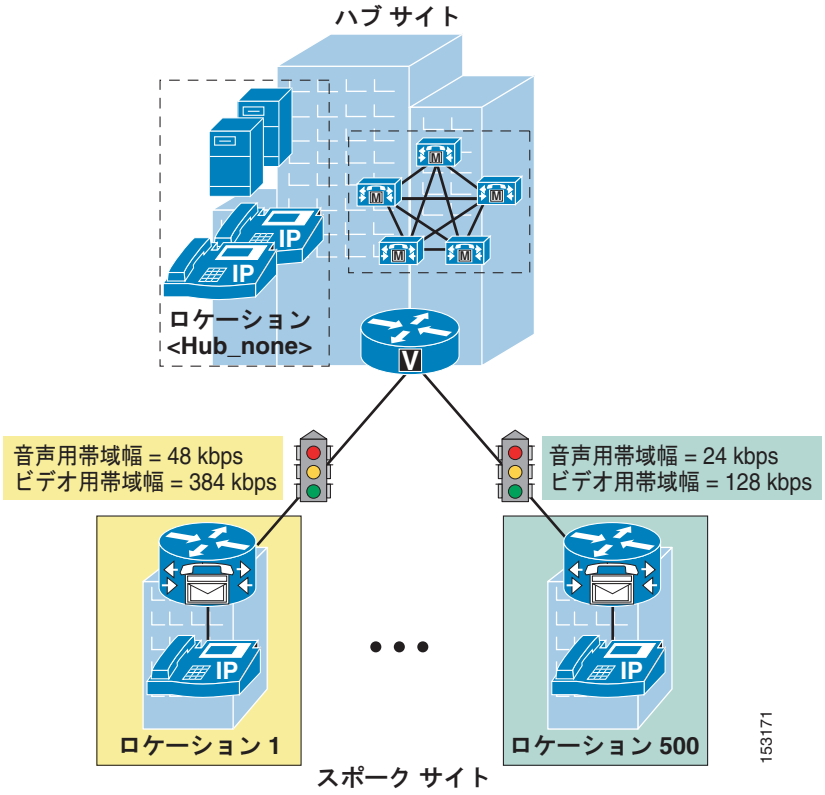
- 「分散型の Unified CM 配置」（P.11-71）

  Unified CM クラスタまたは Cisco Unified Communications Manager Express（Unified CME）を各サイトに配置します。

集中型の Unified CM 配置

単純なハブアンドスポーク トポロジ上にあり、集中型コール処理を使用するマルチサイト WAN 配置では、Unified CM の静的*ロケーション*を使用してコール アドミッション制御を実装します。図 11-38 に、このメカニズムをこのようなトポロジに適用する方法の例を示します。

図 11-38　静的ロケーションを使用した単純なハブアンドスポーク トポロジのコール アドミッション制御



コール アドミッション制御に対して静的ロケーションを使用する場合は、次のガイドラインに従ってください。

- 各スポーク サイトの Unified CM に対しては、個別にロケーション設定が必要です。
- 各サイトの音声コールとビデオ コールに対する帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の推奨設定については、表 11-2 を参照してください）。
- 各スポーク サイトのすべてのデバイスを適切なロケーションに割り当てます。
- ハブ サイトのデバイスは、Hub_None ロケーションのままにします。
- あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Unified CM は、ロケーションを 2000 箇所までサポートします。
- WAN の帯域幅が十分にない場合に、公衆網を介した自動ルーティングを実行する必要があるときは、Unified CM 上で Automated Alternate Routing（AAR）機能を設定します（「Automated Alternate Routing」（P.9-103）を参照）。

- 同じハブ サイトに複数の Unified CM クラスタを配置する場合は、クラスタ間トランク デバイスを Hub_None ロケーションのままにします。ダイヤル プランの解決には、ゲートキーパーを使用できます。ただし、この場合、ゲートキーパーのコール アドミッション制御は必要ありません。これは、すべての IP WAN リンクがロケーション アルゴリズムによって制御されるためです。

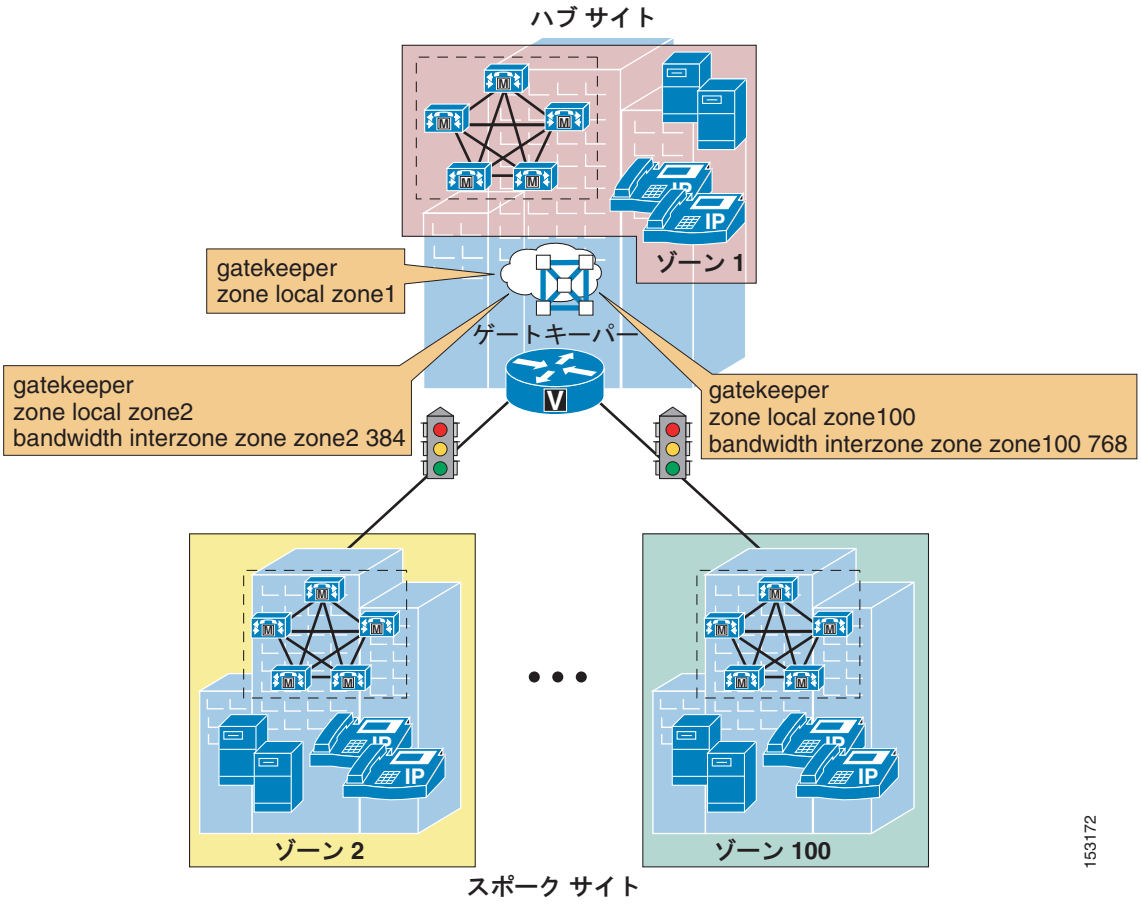
（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.11-83）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することを推奨します。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.11-5）を参照してください。

分散型の Unified CM 配置

単純なハブアンドスポーク トポロジの分散型コール処理配置では、Cisco IOS ゲートキーパーを使用してコール アドミッション制御を実装できます。この設計では、コール処理エージェント（Unified CM クラスタ、Cisco Unified Communications Manager Express（Unified CME）、または H.323 ゲートウェイなど）は Cisco IOS ゲートキーパーに登録し、エージェントが IP WAN コールを発信しようとするたびにゲートキーパーに照会を行います。Cisco IOS ゲートキーパーは、各コール処理エージェントを、特定の帯域幅制限があるゾーンに関連付けます。したがって、Cisco IOS ゲートキーパーは、ゾーンに出入りする IP WAN 音声コールが消費する最大帯域幅量を制限できます。

図 11-39 では、ゲートキーパーを使用したコール アドミッション制御を示しています。つまり、コール処理エージェントは、IP WAN コールを発信するときに、まずゲートキーパーに許可を要求します。ゲートキーパーが許可を与えると、コール処理エージェントは、IP WAN を介してコールを発信します。ゲートキーパーが要求を拒否する場合、コール処理エージェントは別のパス（たとえば、公衆網）を試行するか、単にコールを廃棄させることができます。

図 11-39　ゲートキーパーを使用したハブアンドスポーク トポロジのコール アドミッション制御



ゲートキーパーを使用してコール アドミッション制御を配置する場合は、次のガイドラインに従ってください。

- Cisco Unified Communications Manager Express（Unified CME）と H.323 ゲートウェイの混在環境の場合は、Unified CM で H.225 ゲートキーパー制御トランクを設定します。
- Unified CM クラスタだけに基づく環境の場合は、Unified CM でクラスタ間ゲートキーパー制御トランクを設定します。
- Unified CM で設定したゾーンが、そのサイトの正しいゲートキーパー ゾーンと一致するようにします。
- デバイス プールの Unified CM 冗長性グループにリストされている各 Unified CM サブスクライバは、ゲートキーパー制御トランクをゲートキーパーに登録します（最大で 3 つまで）。
- コールは、Unified CM クラスタ内に登録済みのトランク間にロードバランスされます。
- Unified CM は、複数のゲートキーパーおよびトランクをサポートします。
- トランクをルート グループとルート リスト コンストラクトに配置すると、自動公衆網フェールオーバーを提供できます。詳細については、「ダイヤル プラン」（P.9-1）を参照してください。
- Unified CM、Unified CME、または H.323 ゲートウェイをサポートしている各サイトに対するゲートキーパーのゾーンは、個別に設定します。
- **bandwidth interzone** コマンドをゲートキーパーに使用して、そのゲートキーパーに直接登録済みの Unified CM クラスタ、Unified CME サーバ、および H.323 デバイス間の帯域幅の制御を行います（コーデック タイプ別の帯域幅の設定については、表 11-4 を参照してください）。

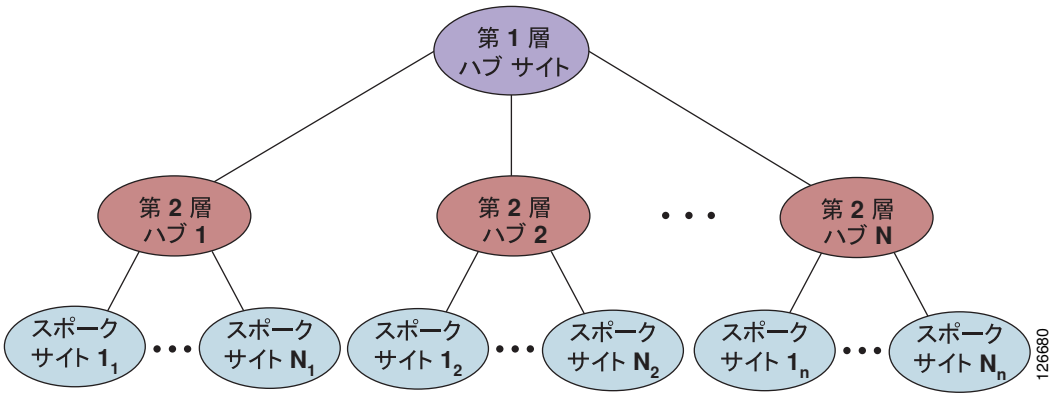
- 1 つの Cisco IOS ゲートキーパーで、100 までのゾーンまたはサイトをサポートできます。
- ゲートキーパーの冗長性は、ゲートキーパー クラスタリング（代替ゲートキーパー）または Cisco Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用すると実装できます。HSRP は、ソフトウェア機能セットにゲートキーパー クラスタリングが使用可能ではない場合に限り使用します。

（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.11-83）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することを推奨します。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.11-5）を参照してください。

2 層ハブアンドスポーク トポロジ

図 11-40 では、2 層ハブアンドスポーク トポロジを示しています。このタイプのネットワーク トポロジは 3 階層のサイト、つまり第 1 層ハブ サイト、第 2 層ハブサイト、およびスポーク サイトから構成されます。スポーク サイトのグループが 1 つの第 2 層ハブ サイトに接続され、各第 2 層ハブ サイトは 1 つの第 1 層ハブ サイトに接続されます。単純なハブアンドスポーク トポロジであるため、スポーク サイト間には直接のリンクが存在しません。したがって、スポーク サイト間の通信は、すべて第 2 層ハブ サイトを経由する必要があります。同様に、第 2 層ハブ サイト間には直接のリンクが存在しないため、これらのハブ サイト間の通信は、すべて第 1 層ハブ サイトを経由する必要があります。

図 11-40　　2 層ハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する 2 層ハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、「単純な MPLS トポロジ」（P.11-77）の項を参照してください。

以降では、採用する Unified CM 配置モデルごとに、2 層ハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.11-74）

  1 つまたはそれ以上の Unified CM クラスタを第 1 層ハブ サイトに配置し、第 2 層ハブ サイトとスポーク サイトには電話とゲートウェイだけを配置します。

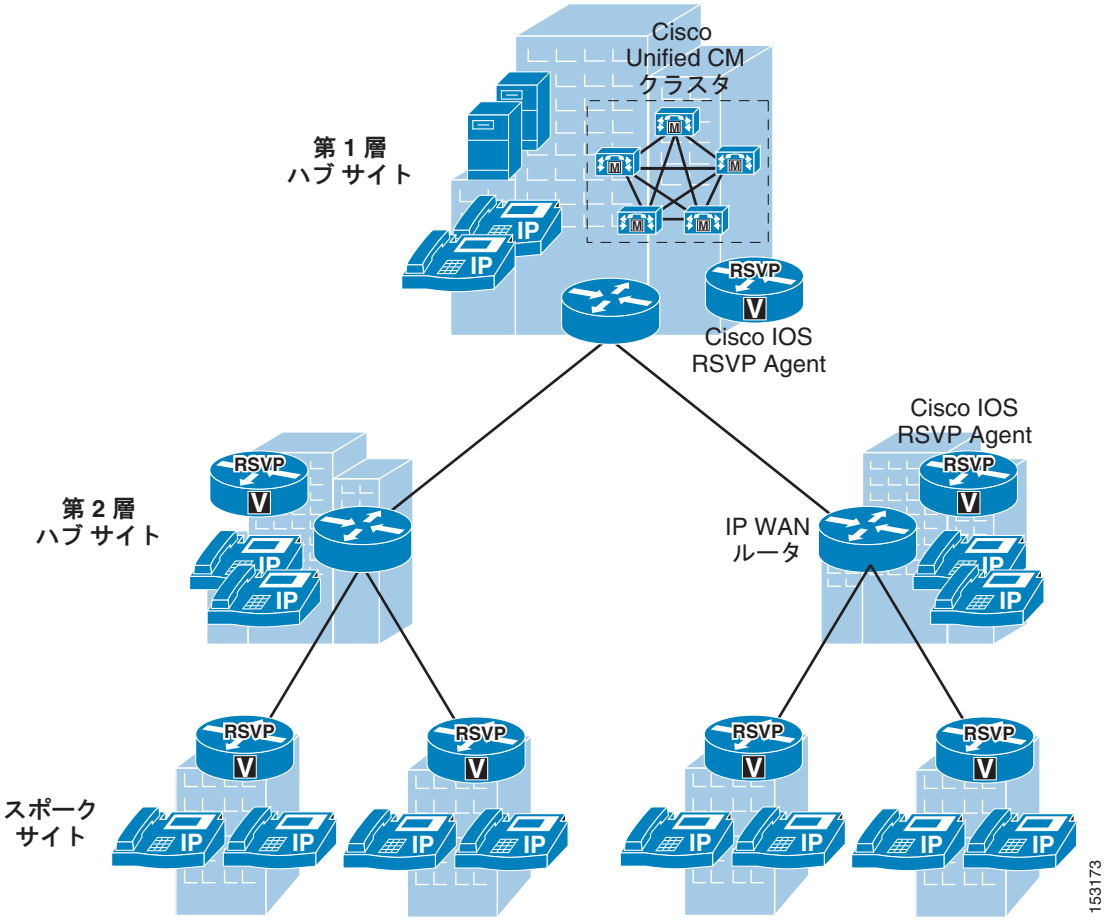
- 「分散型の Unified CM 配置」（P.11-76）

  Unified CM クラスタを第 1 層ハブ サイトと第 2 層ハブ サイトに配置し、スポーク サイトにはエンドポイントとゲートウェイだけを配置します。

集中型の Unified CM 配置

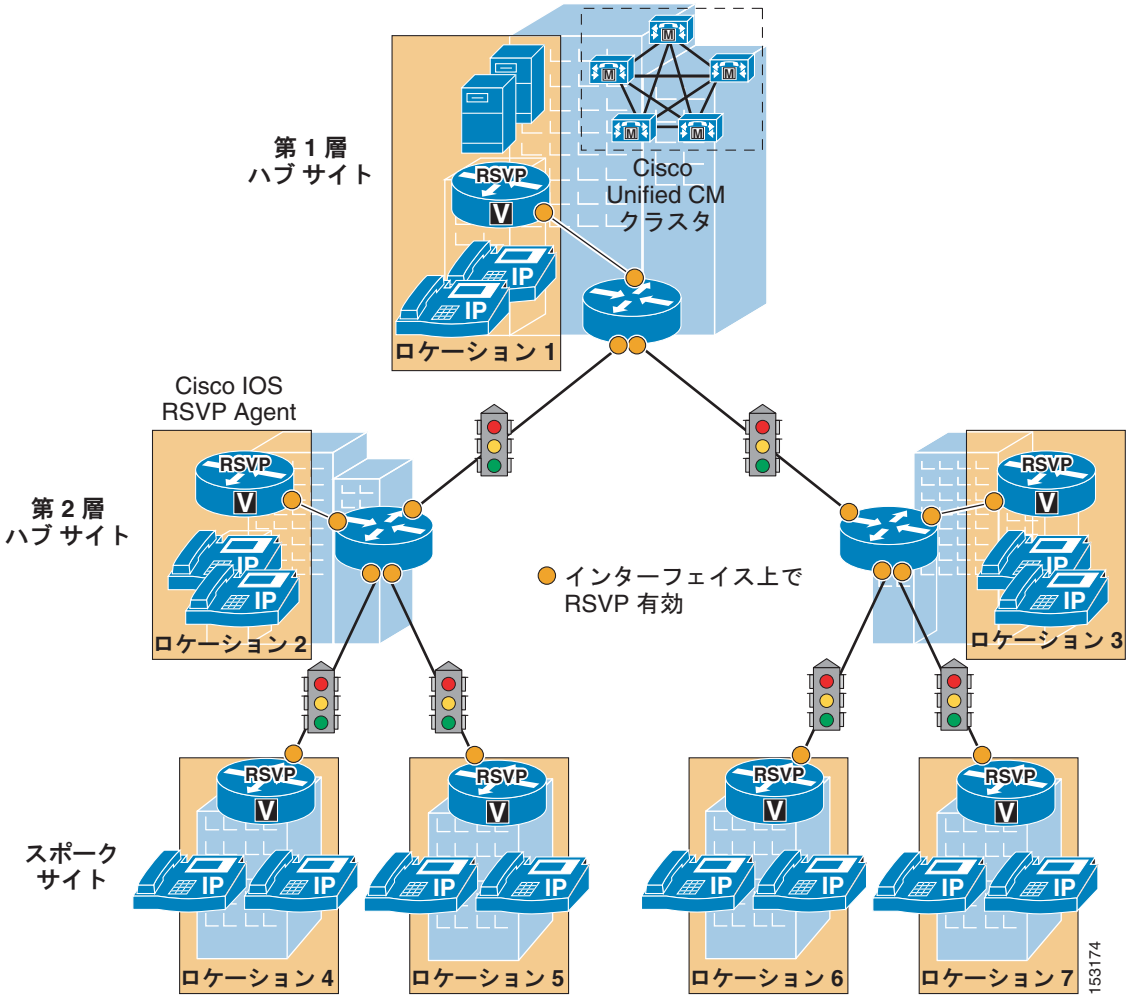
図 11-41 では、2 層ハブアンドスポーク IP WAN トポロジに配置された単一の Unified CM 集中型クラスタを示しています。このシナリオでは、Unified CM クラスタを第 1 層ハブ サイトに配置し、すべての第 2 層ハブ サイトとスポーク サイトにはエンドポイントとゲートウェイだけを配置します。

図 11-41　集中型の Unified CM での 2 層ハブアンドスポーク トポロジ



このシナリオでは、トポロジ対応コール アドミッション制御を配置する必要があります。そのため、単一の Unified CM クラスタにとっては、RSVP 対応ロケーションを使用することになります。図 11-42 では、このメカニズムを配置する方法を示しています。

図 11-42　RSVP 対応ロケーションを使用した 2 層ハブアンドスポーク トポロジのコール アドミッション制御



これらの配置には、次のガイドラインが適用されます。

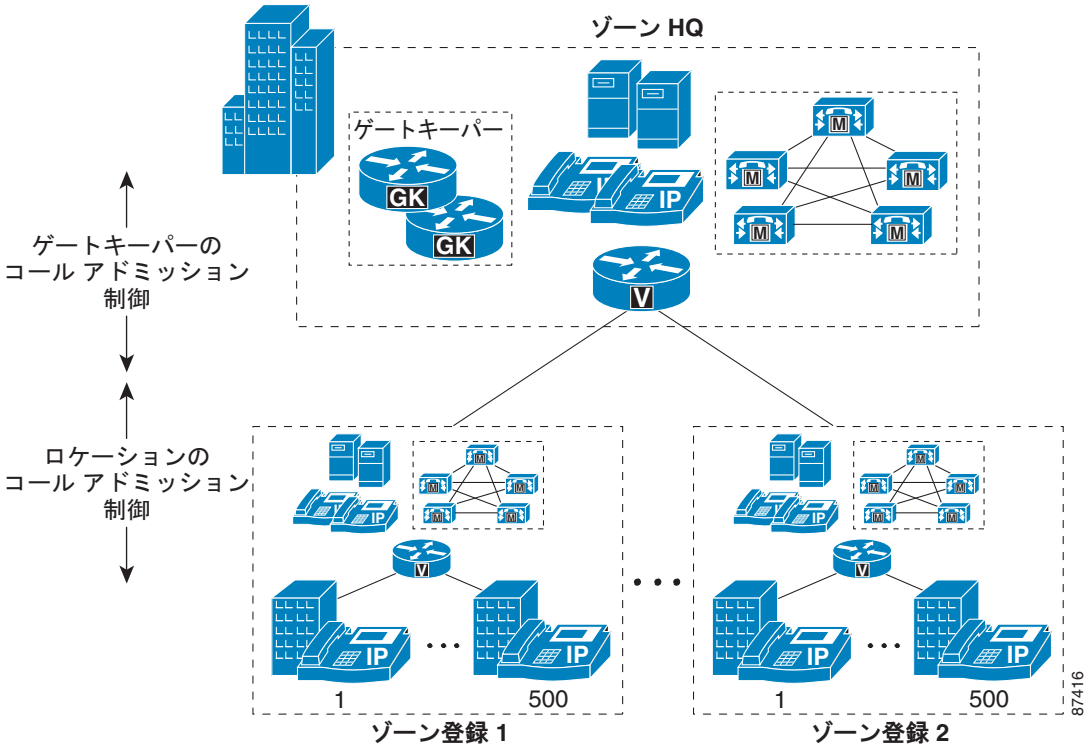
- 各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Unified CM で、各サイトのロケーションを定義し、すべての帯域幅の値を [Unlimited] のままにします。
- 各サイトにあるすべてのデバイスを該当するロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスの Media Resource Group List（MRGL; メディア リソース グループ リスト）の Media Resource Group（MRG; メディア リソース グループ）に属するようにします。
- Unified CM サービス パラメータで、[Default inter-location RSVP Policy] を [Mandatory] または [Mandatory (video desired)] に設定し、[Mandatory RSVP mid-call error handle option] を [Call fails following retry counter exceeded] に設定します。

- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします（図 11-42 を参照）。

分散型の Unified CM 配置

2 層ハブアンドスポーク トポロジを採用していて、第 1 層ハブ サイトと第 2 層ハブ サイトに Unified CM がある配置にコール アドミッション制御を提供するには、図 11-43 に示されているように静的ロケーションとゲートキーパー ゾーン メカニズムを組み合せて対応します。

図 11-43　コール アドミッション制御にロケーションおよびゲートキーパー メカニズムを組み合せる方式



ゲートキーパー ゾーンを静的ロケーションと組み合せてコール アドミッション制御を実行する場合は、次の推奨事項に従ってください。

- ローカル Unified CM を使用していないサイト（つまり、スポーク サイト）には、静的ロケーションに基づくコール アドミッション制御を使用します。
- Unified CM クラスタ間（つまり、第 1 層ハブ サイトと第 2 層ハブ サイト間）には、ゲートキーパー ベースのコール アドミッション制御を使用します。
- ローカル Unified CM を使用していない各サイトには、そのサイトをサポートしている Unified CM クラスタ内にロケーションを設定します。
- 各サイトの帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の設定については、表 11-2 と表 11-4 を参照してください）。
- Unified CM に設定された各デバイスをロケーションに割り当てます。あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Unified CM は、ロケーションを 2000 箇所までサポートします。

- 各 Unified CM クラスタは、ゲートキーパー制御のトランクをゲートキーパーに登録します。
- ゲートキーパーでは、各 Unified CM クラスタに対してゾーンを設定し、**bandwidth interzone** コマンドを使用して各クラスタを宛先および発信元とするコール数を制御します。

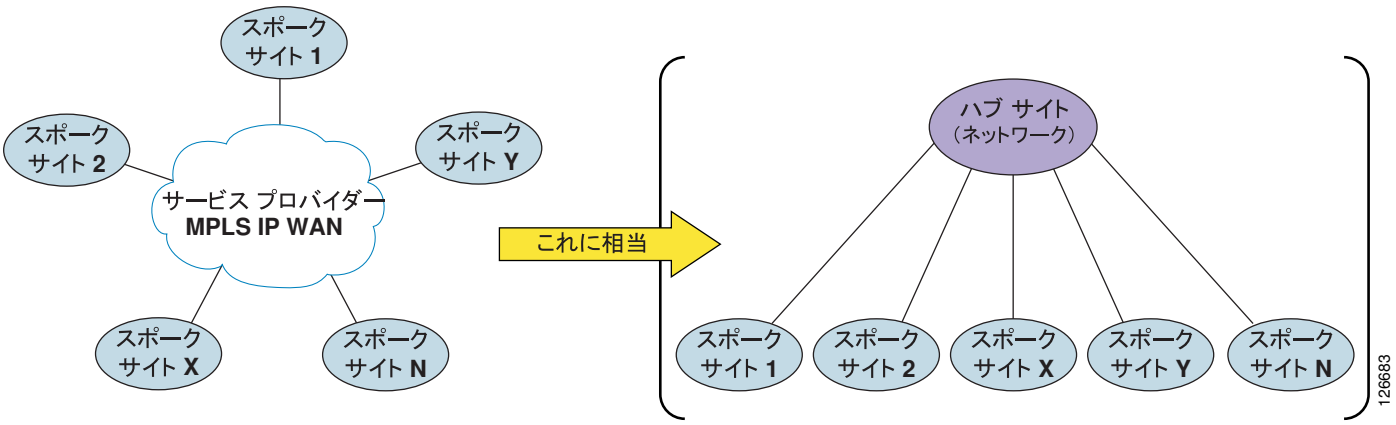
（注）　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.11-83）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することを推奨します。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.11-5）を参照してください。

単純な MPLS トポロジ

図 11-44 では、Multiprotocol Label Switching（MPLS）テクノロジー ベースの（サービス プロバイダーからの）IP WAN を示しています。サービス プロバイダーの提供する従来のレイヤ 2 WAN サービスと MPLS ベースのサービスのデザイン上の大きな違いは、MPLS を使用すると、IP WAN のトポロジはハブアンドスポークに準拠していないということです。すべてのサイト間の接続にはフルメッシュ接続方式を採用します。

このトポロジの違いは、ネットワークを企業側での IP ルーティングという観点から見たとき、各サイトが、他のどのサイトからも IP ホップ 1 つ分しか離れていないことを意味します。したがって、他のサイトに到達するためにハブ サイトを経由する必要はありません。事実上、「ハブ サイト」という概念が存在しません。すべてのサイトが対等と見なされ、各サイトで異なっているのは、IP WAN を介して使用することのできる帯域幅の量のみです。

図 11-44　サービス プロバイダーからの MPLS IP WAN、およびこれに相当するトポロジ



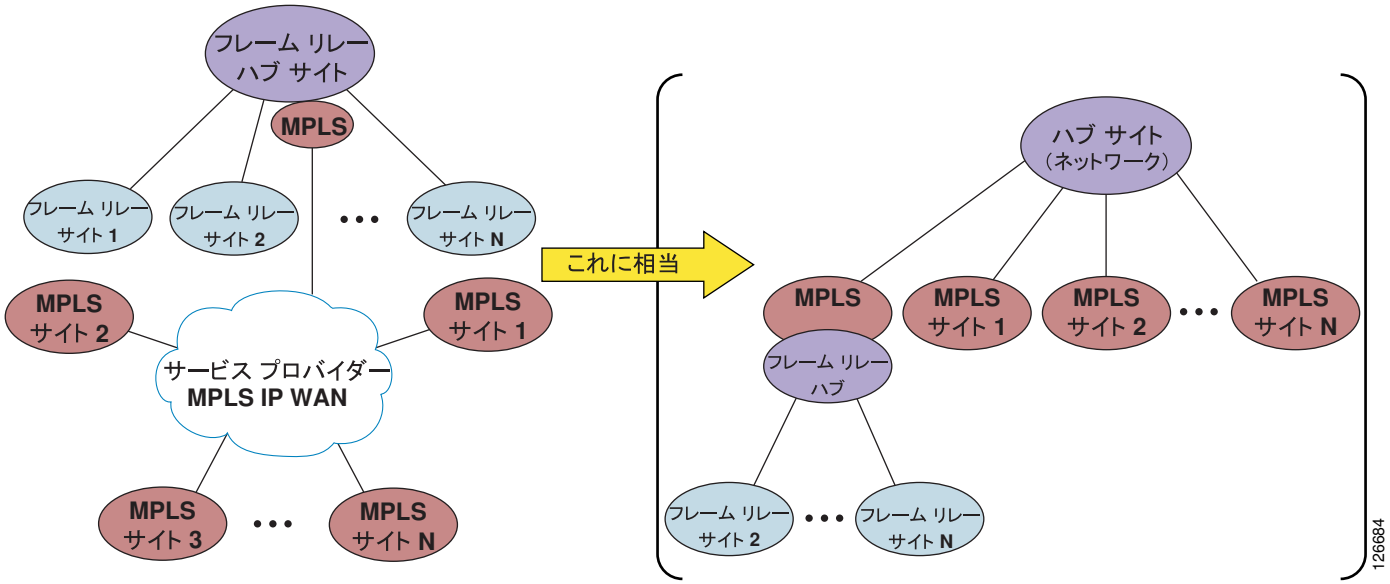
これまでに検討した内容に基づくと、コール アドミッション制御という観点から見たとき、MPLS に基づくサービス プロバイダー IP WAN サービスは、実質的には、ハブ サイトのないハブアンドスポーク トポロジに相当することが簡単にわかります（図 11-44 を参照）。事実上、ネットワーク自体をハブ サイトと見なすことができます。企業サイトは、いずれも（本社、つまり中央サイトを含めて）スポーク サイトに相当します。このように見方を変えると、コール アドミッション制御の実行方法も異なってきます。この方法については、以降で説明します。

上で検討した内容の中で、ここで例外として言及する価値があるのは、マルチサイト配置において、MPLS ベースの WAN がフレーム リレーや ATM などの従来のレイヤ 2 テクノロジー ベースの IP WAN と共存している場合です。このようなシナリオは、実際に発生する可能性があります。たとえば、ネットワークが移行の途中段階にある場合や、企業合併などの状況が発生した場合です。

図 11-45 に示すように、従来のレイヤ 2 テクノロジー（フレーム リレーなど）ベースのハブアンドスポーク IP WAN を MPLS ベースの IP WAN と統合すると、ネットワーク トポロジは単純なハブアンドスポークやフルメッシュではなく、2 層ハブアンドスポークになります。

この場合、MPLS ネットワークが第 1 層ハブ サイトを表し、MPLS 対応のフレーム リレー ハブ サイト、および MPLS ベースのサイトが第 2 層ハブ サイトを表し、フレーム リレー スポーク サイトがスポーク サイトを表します。したがって、このような配置での設計上の考慮事項については、「2 層ハブアンドスポーク トポロジ」（P.11-73）の項を参照してください。

図 11-45　MPLS サイトとフレーム リレー サイトの共存、およびこれに相当するトポロジ



以降では、採用する Unified CM 配置モデルごとに、MPLS ベースのトポロジに関する設計上のベストプラクティスを示します。

- 「集中型の Unified CM 配置」（P.11-79）

  1 つまたはそれ以上の Unified CM クラスタを 1 つのサイトだけに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 「分散型の Unified CM 配置」（P.11-81）

  Unified CM クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

（注） ここでは、サービス プロバイダーによって MPLS サービスが提供されている企業の配置を中心に説明します。MPLS ネットワークが企業自体によって配置される場合、次の 2 つのいずれかの条件が満たされる限り、コール アドミッション制御は効果的に実行できます。最初の条件は、MPLS ネットワークでのルーティングが、ネットワークがハブアンドスポークになるように設定されていること、2 番めの条件は、輻輳が末端部分でしか発生しないように、MPLS ネットワークの核の部分の帯域幅を非常に大きく設定していることです。

（注） 1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、「汎用トポロジ」（P.11-83）の項で説明しているように、トポロジ対応コール アドミッション制御を配置することを推奨します。ロード バランシング リンクが存在する場合は、対称的なルー

ティングを保証するために特に注意が必要です。詳細については、「トポロジ非対応コール アドミッション制御の制限」（P.11-5）および「MPLS ネットワークの特別な考慮事項」（P.11-11）を参照してください。また、シスコのアカウント チームにお問い合せください。

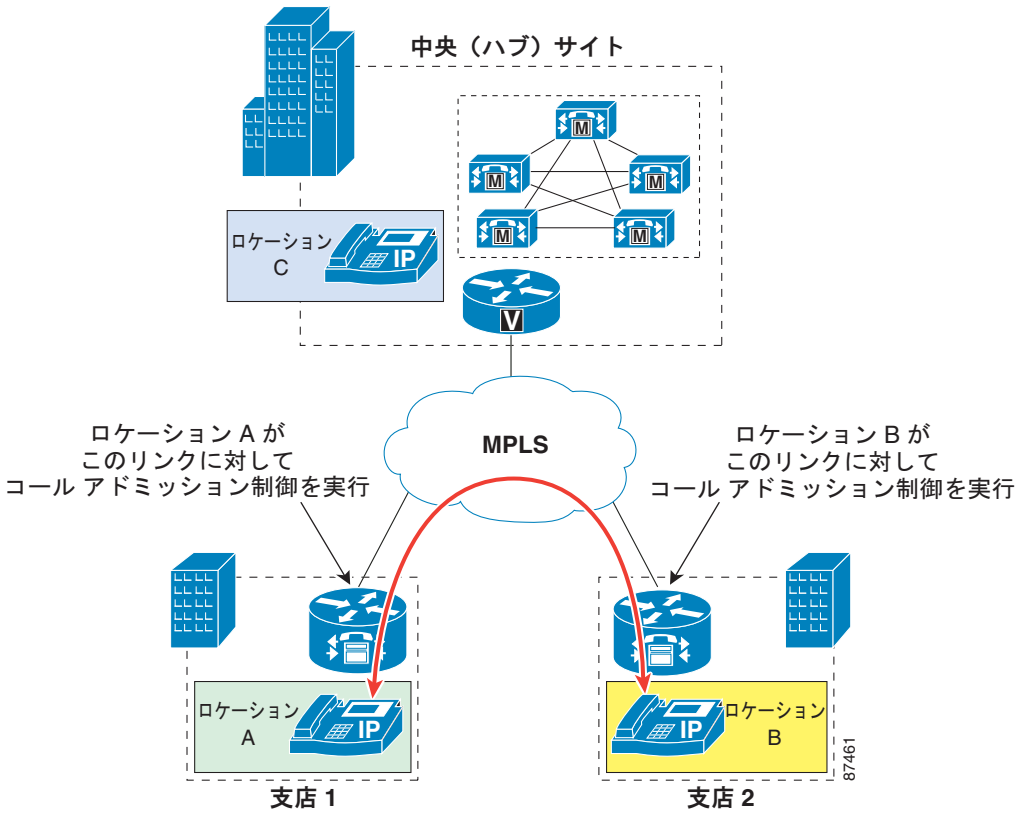
集中型の Unified CM 配置

MPLS トポロジ上で集中型コール処理を使用するマルチサイト WAN 配置では、Unified CM の静的ロケーションを使用してコール アドミッション制御を実装します。

ハブアンドスポーク WAN トポロジ（フレーム リレー、ATM など）では、支店サイトとのリンクはすべて、中央サイトで終端します。フレーム リレーを例にすると、支店ルータからのすべての PVC（Permanent Virtual Circuits; 相手先固定接続）は、中央サイトのヘッドエンド ルータに集約されています。この例では、帯域幅に対する課金は WAN リンクの支店エンドで行われているので、中央サイドではデバイスにコール アドミッション制御を適用する必要はありません。したがって、Unified CM ロケーションの設定では中央サイトのデバイスのロケーションは Hub_None のままにしておきます。一方、各支店のデバイスは適切なコール アドミッション制御を受けるために各支店のロケーションに指定される必要があります。

MPLS WAN ネットワークでは、すべての支店はレイヤ 3 で隣接していると見なされるため、中央サイトに接続する必要はありません。図 11-46 では、スポークツースポーク配置による 2 つの支店間のコールを説明しています。

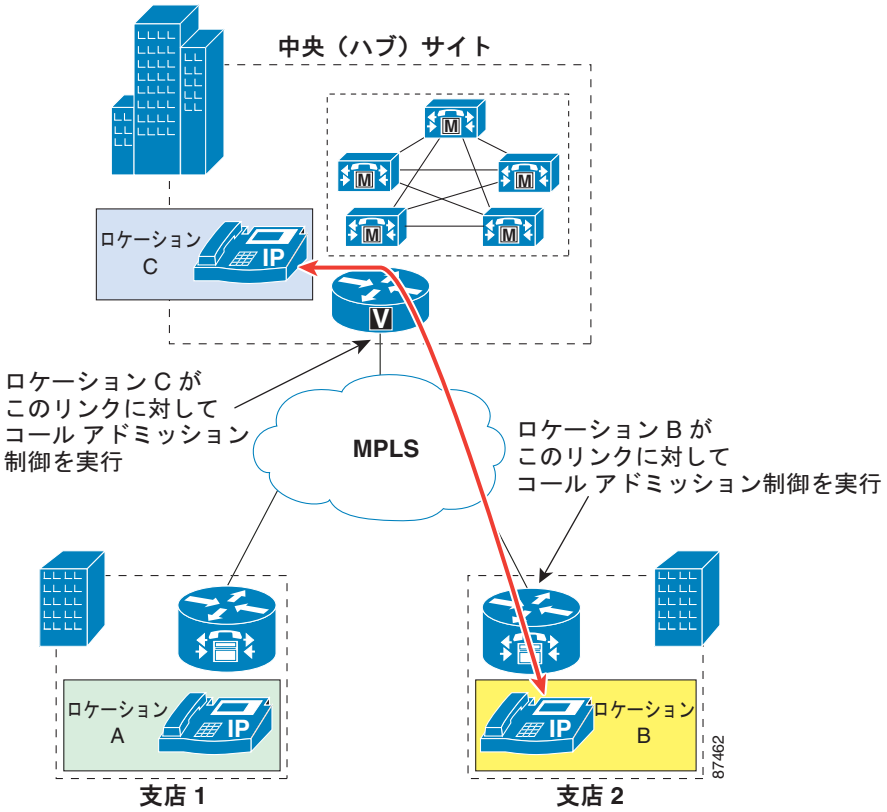
図 11-46　MPLS 配置におけるスポークツースポーク コール



また、MPLS WAN では、中央サイト WAN に接続しているリンクは支店の WAN リンクのすべてを集約していません。中央サイトに存在するすべてのデバイスは、個々のデバイスに対応するコール アドミッション制御ロケーション（つまり、Hub_None ロケーションではありません）に指定されています。したがって、このスポークツースポーク設定では支店のリンクとは無関係に、コール アドミッション制御は中央サイト リンク上で実行される必要があります（図 11-47 を参照）。

（注）　トランクなどの一部のデバイスはメディアを終端しないで、通常は Hub_None ロケーションのままにします。ただし、トランクで MTP が要求される場合にコール アドミッション制御のエラーを回避するためには、トランクは Hub_None 以外のロケーションに割り当てる必要があり、トランクの MRGL 内のすべての MTP は、そのロケーションに関連付けられたサイトに物理的に配置する必要があります。MTP はロケーションに直接割り当てることができず、その MTP を選択したデバイスのロケーションを継承するため、この設定が必要です。

図 11-47　MPLS 配置におけるハブとのコール

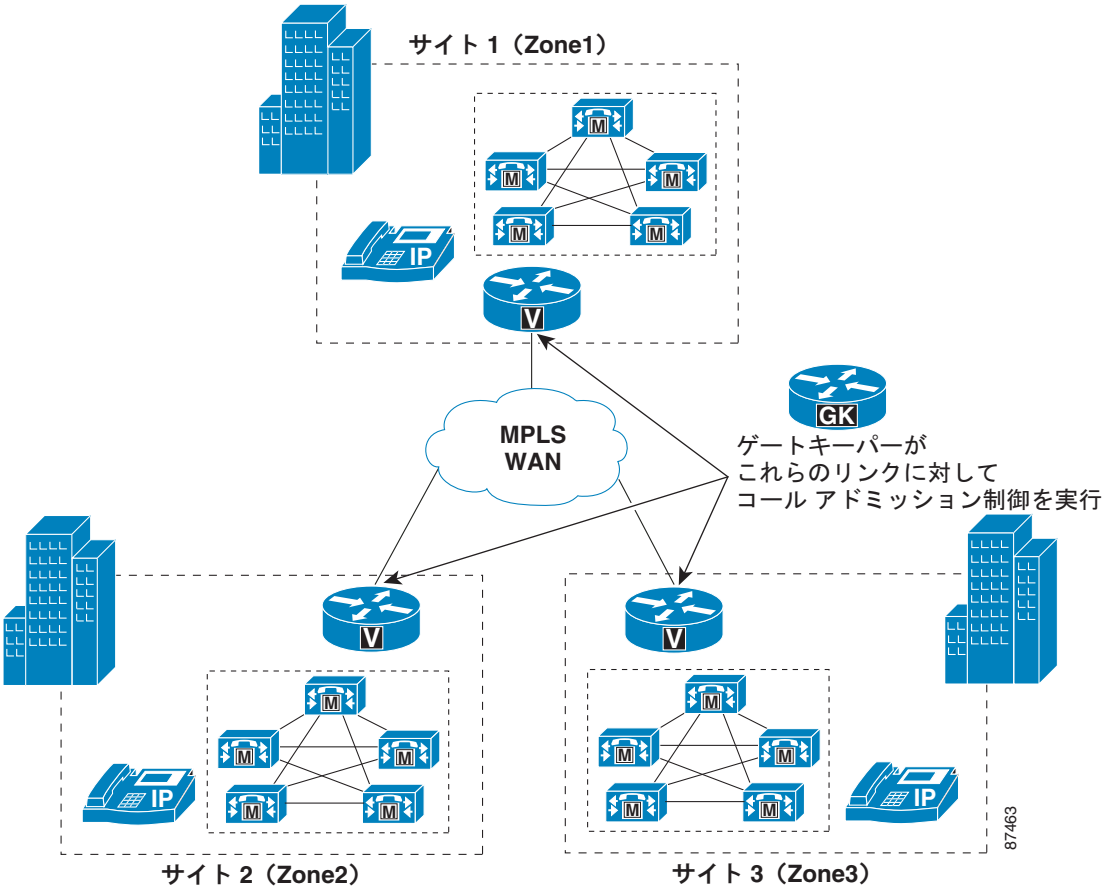


特定サイトに許されている帯域幅がすべて消費されてしまっている場合は、Unified CM が備えている Automated Alternate Routing（AAR）機能を使用して、公衆網へ自動的にフェールオーバーさせることができます（AAR の詳細については、「Automated Alternate Routing」（P.9-103）を参照してください）。

分散型の Unified CM 配置

支店ロケーションのない複数のサイトに Unified CM クラスタが設定されていて、どのサイト間も MPLS WAN でリンクされているマルチ サイト配置の場合は、ゲートキーパーがダイヤル プランを解決し、サイト間のコール アドミッション制御を行い、個々のサイトを異なるゲートキーパー ゾーンに格納します。この同様のメカニズムは、レイヤ 2 WAN テクノロジーをベースにしたハブアンドスポークトポロジにも適用されています（図 11-48 を参照）。

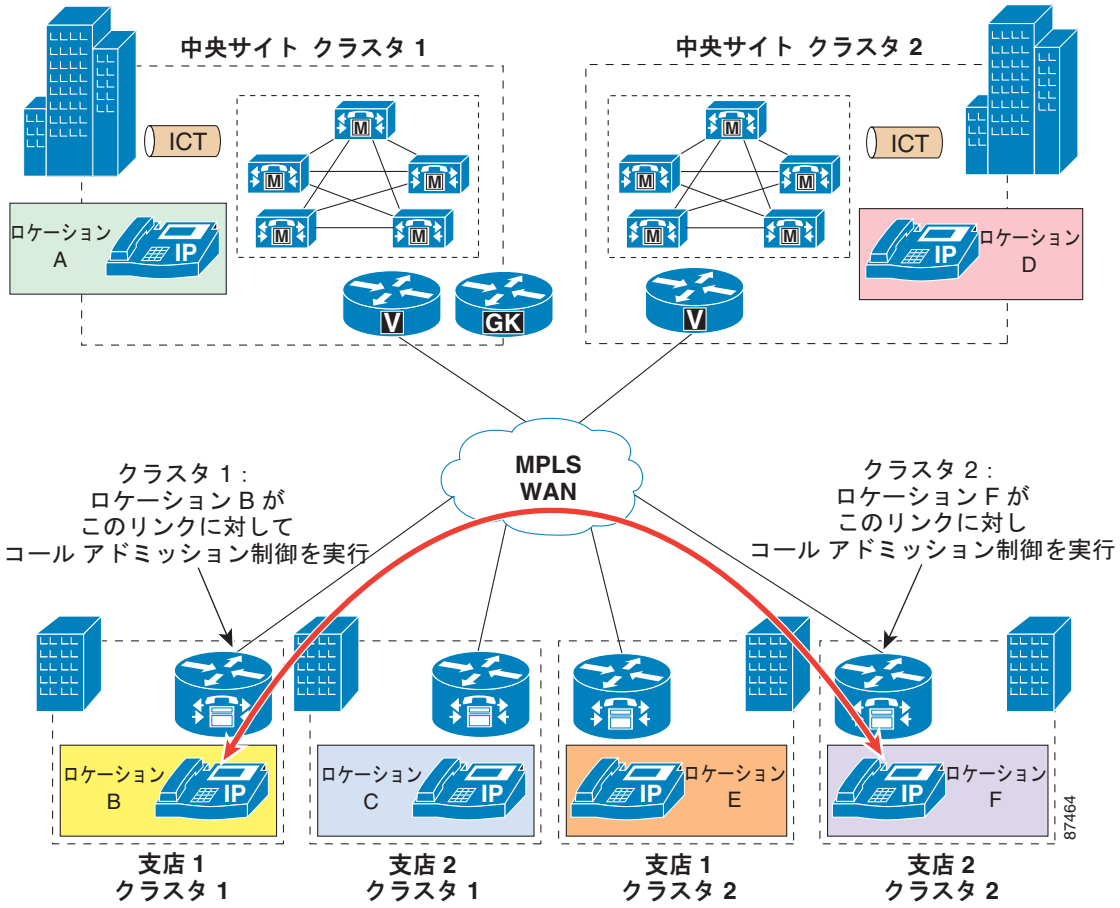
図 11-48　　MPLS を使用した分散型配置におけるゲートキーパー コール アドミッション制御



支店サイトが必要な配置では、クラスタ間のダイヤル プランの解決にゲートキーパーを使用することもできますが、コール アドミッション制御にはゲートキーパーを使用しないことを推奨します。

異なるクラスタに属している支店間にコールが発生した場合は、音声パスはその支店間で直接確立できるので、支店のクラスタから中央サイトへメディアを転送する必要はありません。したがって、コール アドミッション制御は各支店の WAN リンクに対してのみ必要です（図 11-49 を参照）。

図 11-49　クラスタ間トランク（ICT）によるマルチ クラスタ接続



Unified CM の集中型配置で見られるように、メディアを各サイトで終端するデバイス（各クラスタに対する中央サイトを含む）は、適切に設定されているロケーションに指定されている必要があります。

クラスタ間トランクで重要なことは、これは単なるシグナリング デバイスであって、クラスタ間トランクのメディアを転送する役目をもたないということです。したがって、クラスタ間トランクのロケーションの指定は、Hub_None のままにしておきます。トランクが MTP を必要とする場合は例外です。この場合は、トランクと MTP の両方を、それらが存在するサイトのロケーションに配置する必要があります。

特定のサイトに許されている帯域幅を消費してしまっている場合は、次の 2 つの方式を組み合せて、公衆網へ自動的にフェールオーバーできます。

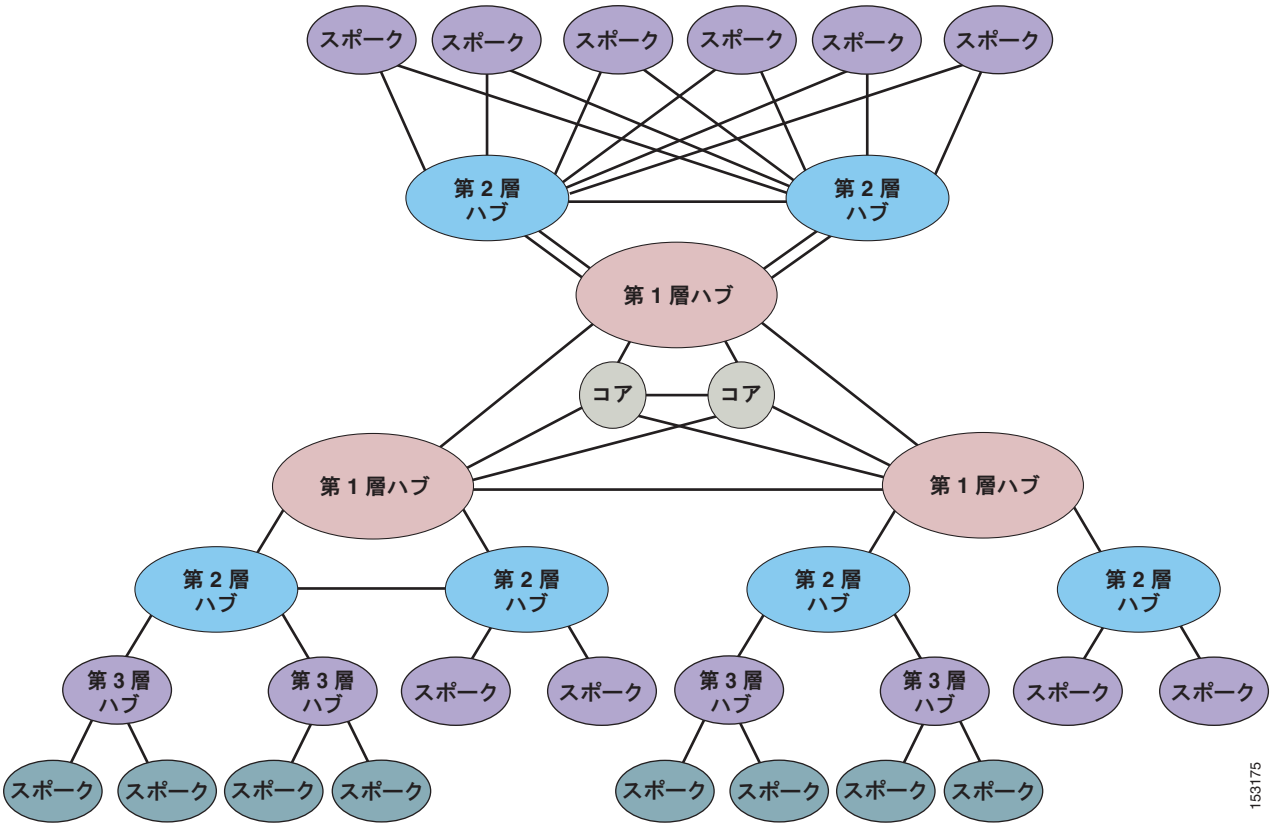
- マルチ Unified CM クラスタに対するコールには、ルート リストおよびルート グループで対応
- Unified CM クラスタ内のコールには、Automated Alternate Routing（AAR）機能で対応（AAR の詳細については、「Automated Alternate Routing」（P.9-103）を参照してください）

汎用トポロジ

この章の説明における汎用トポロジとは、単純なハブアンドスポーク、2 層ハブアンドスポーク、または単純な MPLS ベースのネットワークに変換できないネットワーク トポロジです。

図 11-50 に示すように、汎用トポロジでは、フルメッシュの機能、ハブアンドスポークの機能、部分メッシュの機能、またはこれらのすべての組み合せを 1 つのネットワーク内で実現できます。これは、サイト間の二重接続、および 1 つのサイトから別のサイトへのマルチ パスを表すこともあります。

図 11-50　　汎用トポロジ



このようなネットワークは複雑な性質を持つため、RSVP に基づくトポロジ対応コール アドミッション制御メカニズムを採用する必要があります。このメカニズムは、特にトポロジの形態が次のような場合に、帯域幅を適切に制御できます。

- さまざまなハブ サイトにデュアル ホーム接続されたリモート サイト
- プライマリ/バックアップ設定またはアクティブ/アクティブ ロード バランシング設定のいずれかによる、任意の 2 つのサイト間の複数の IP WAN リンク
- 冗長ハブまたは専用接続を備えたデータ センター
- フル メッシュ構造のコア ネットワーク
- 任意の 2 つのサイト間の複数の等コスト IP パス
- 多層アーキテクチャ

以降では、採用する Unified CM 配置モデルごとに、汎用ネットワーク トポロジに関する設計上のベスト プラクティスを示します。

- 「集中型の Unified CM 配置」（P.11-84）

  1 つまたはそれ以上の Unified CM クラスタを特定のサイトに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 「分散型の Unified CM 配置」（P.11-71）

  Unified CM クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

- 「分散型混在コール処理配置」（P.11-89）

  さまざまなトポロジに呼制御アプリケーションが分散します。

集中型の Unified CM 配置

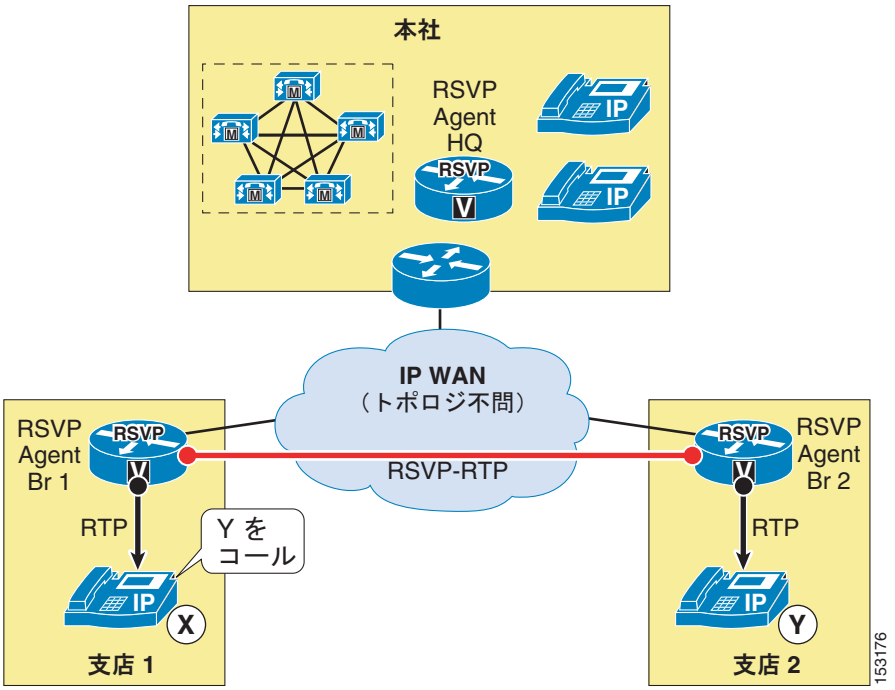
汎用トポロジを使用した Unified CM の集中型配置は、次の 2 つのサブタイプに分類できます。

- 「単一の Unified CM クラスタ」（P.11-84）
- 「同じ場所にある Unified CM クラスタ」（P.11-85）

単一の Unified CM クラスタ

この項の推奨事項は、図 11-51 に示すように、汎用ネットワーク トポロジで採用される単一の Unified CM クラスタに適用されます。

図 11-51　汎用トポロジにおける単一の Unified CM クラスタ



このタイプの配置には、次の考慮事項が適用されます。

- Unified CM が存在する中央サイトなど、各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Unified CM で、各サイトのロケーションを定義し、すべての帯域幅の値を [Unlimited] のままにします。
- 各サイトにあるすべてのデバイスを適切なロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスの Media Resource Group List（MRGL; メディア リソース グループ リスト）の Media Resource Group（MRG; メディア リソース グループ）に属するようにします。
- Unified CM サービス パラメータで、[Default inter-location RSVP Policy] を [Mandatory] または [Mandatory (video desired)] に設定し、[Mandatory RSVP mid-call error handle option] を [Call fails following retry counter exceeded] に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（「RSVP 設計上のベスト プラクティス」（P.11-33）を参照）。
- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします。

同じ場所にある Unified CM クラスタ

この項の推奨事項は、複数の Unified CM が同じ LAN または MAN にある配置に適用されます。ただし、Unified CM クラスタが存在するサイトが低帯域幅リンクで接続されている場合には、考慮事項も同じものが有効です。仕様のため、クラスタからクラスタへのコールでは各クラスタのエンドポイントに RSVP Agent を使用します。

図 11-52 では、所定のサイト（本社）にある 2 つの Unified CM クラスタ、およびエンドポイントとゲートウェイを持つ複数のリモート サイトの配置を示しています。これらのリモート サイトは、クラスタ 1（たとえば支店 1）またはクラスタ 2（たとえば支店 2）のいずれかによって制御されます。

図 11-52　汎用トポロジにおける同じ場所にある Unified CM クラスタ

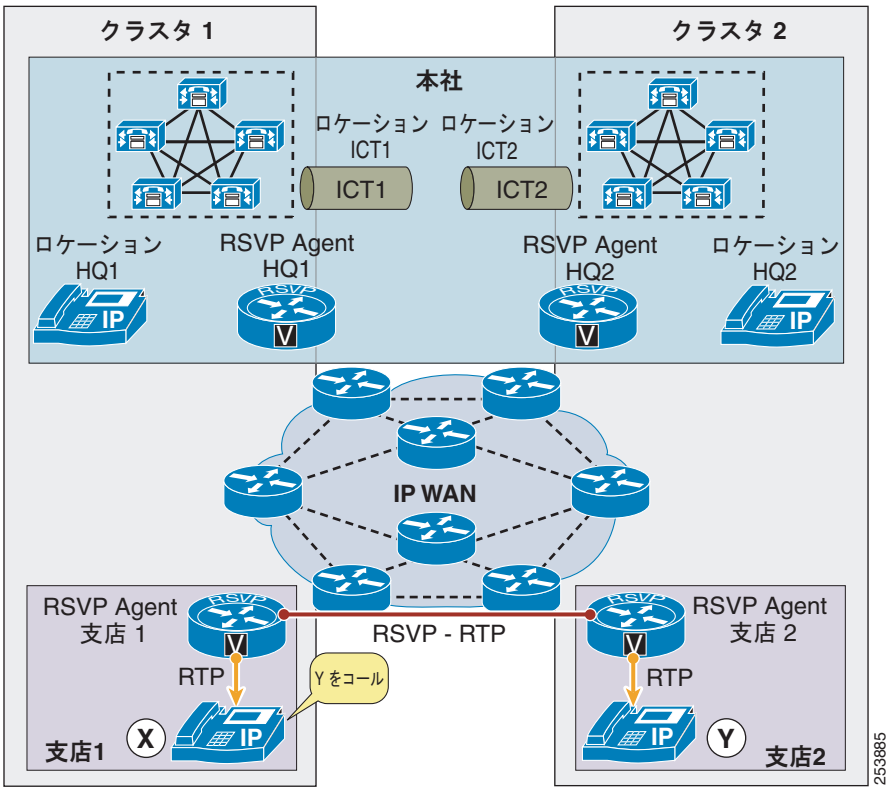


図 11-52 に示す配置には、次のガイドラインが適用されます。

- Unified CM が存在する中央サイトなど、各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- 中央サイトとリモート サイト間およびクラスタ間を流れるコール トラフィックの量に応じて、中央サイトの両クラスタの RSVP Agent とも、1 つまたは複数の Cisco Integrated Services Router（ISR; サービス統合型ルータ）に配置することを検討してください。1 つの ISR に異なるクラスタで制御される複数の RSVP Agent をホストできます。
- 各 Unified CM クラスタで、各サイトのロケーションを定義し、すべての帯域幅の値を無制限のままにします。
- 各サイトにあるすべてのデバイスを適切なロケーションに割り当てます。これには、エンドポイント、ゲートウェイ、会議リソース、Cisco RSVP Agent 自体などが含まれています。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスの Media Resource Group List（MRGL; メディア リソース グループ リスト）の Media Resource Group（MRG; メディア リソース グループ）に属するようにします。
- Unified CM サービス パラメータで、両クラスタに [Default inter-location RSVP Policy] を [Mandatory] または [Mandatory (video desired)] に設定し、[Mandatory RSVP mid-call error handle option] を [Call fails following retry counter exceeded] に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（「RSVP 設計上のベスト プラクティス」（P.11-33）を参照）。

- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします。
- SIP クラスタ内トランクで RSVP SIP プレコンディションを有効にします（手順については、「ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションへの移行」（P.11-54）を参照してください）。
- SIP クラスタ間トランク ロケーションと自らを含めたすべてのロケーションとの間に、[Mandatory] または [Mandatory (Video Desired)] のロケーション間 RSVP ポリシーを設定します（次のロケーション内 RSVP ポリシーを参照）。
- SIP クラスタ間トランクに [Mandatory] または [Mandatory (Video Desired)] のロケーション内 RSVP ポリシーを設定します。ロケーション内 RSVP ポリシーを設定するには、ロケーションを選択し、そのロケーションのポリシーを設定します。これにより、このロケーション内のコールでは RSVP コール アドミッション制御が効率よく使用されるようになります。これは、発信元クラスタへのコールの転送または自動転送からコールがトランクにヘアピンされる場合に重要です。
- 中央サイト内でのクラスタ間のコールには、RSVP Agent が使用されます。これは仕様であり、付加サービスをクラスタ全体で機能させて、クラスタ全体でエンドツーエンド RSVP を保持できるようにしています。サポートできるバリエーションがいくつかあります。同じロケーションにあるクラスタに最善のコール アドミッション制御設計については、シスコ営業担当にお問い合せください。

分散型の Unified CM 配置

RSVP SIP プレコンディションにより、汎用ネットワーク トポロジで Unified Communication Manager クラスタを分散配置した環境でコール アドミッション制御を機能させることができます。ここでは、クラスタ間での RSVP SIP プレコンディションのサポートを使用したデュアル クラスタ配置の例を示します（図 11-53 を参照）。このモデルにはハイブリッドおよびバリエーションがいくつか考えられます。これは簡単な設計の概要を示した例にすぎませんが、ベスト プラクティスおよび設計上の考慮事項を踏まえたものです。

図 11-53　分散型の Unified CM 配置

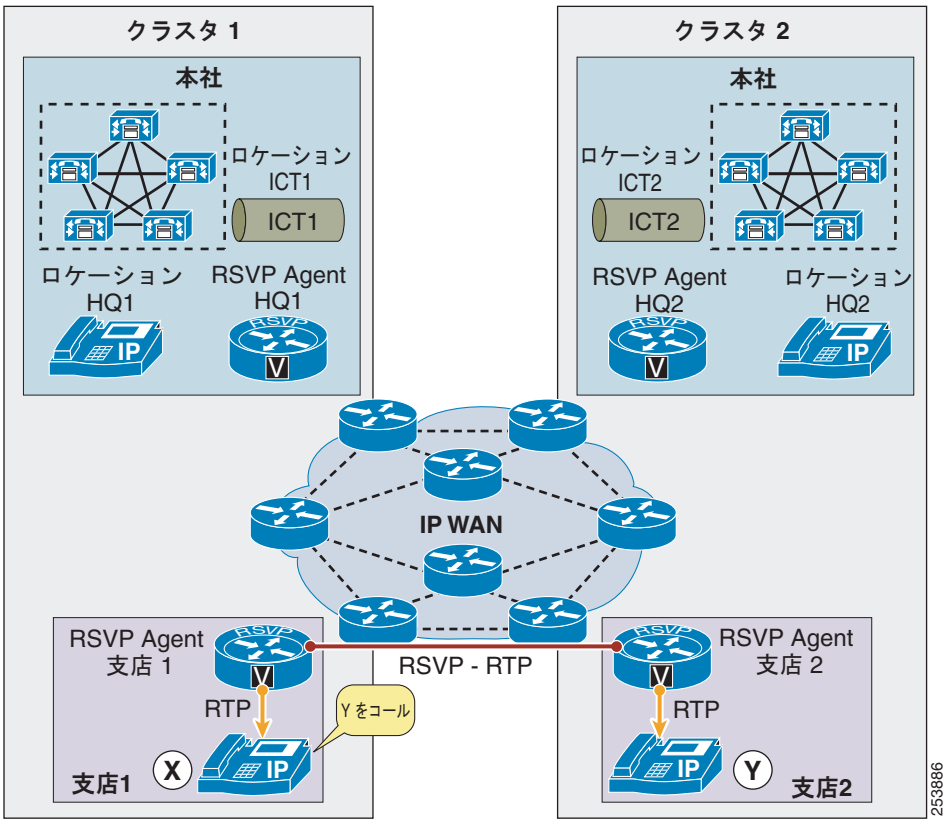


図 11-53 に示す配置には、次のガイドラインが適用されます。

- Unified CM が存在する中央サイトなど、各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- 各 Unified CM クラスタで、各サイトのロケーションを定義し、すべての帯域幅の値を無制限のままにします。
- 各サイトにあるすべてのデバイスを適切なロケーションに割り当てます。これには、エンドポイント、ゲートウェイ、会議リソース、Cisco RSVP Agent 自体などが含まれています。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスの Media Resource Group List（MRGL; メディア リソース グループ リスト）の Media Resource Group（MRG; メディア リソース グループ）に属するようにします。
- Unified CM サービス パラメータで、両クラスタに [Default inter-location RSVP Policy] を [Mandatory] または [Mandatory (video desired)] に設定し、[Mandatory RSVP mid-call error handle option] を [Call fails following retry counter exceeded] に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（「RSVP 設計上のベスト プラクティス」（P.11-33）を参照）。
- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします。

- SIP クラスタ内トランクで RSVP SIP プレコンディションを有効にします（手順については、「ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションへの移行」（P.11-54）を参照してください）。
- SIP クラスタ間トランク ロケーションと自らを含めたすべてのロケーションとの間に、[Mandatory] または [Mandatory (Video Desired)] のロケーション間 RSVP ポリシーを設定します（次のロケーション内 RSVP ポリシーを参照）。
- SIP クラスタ間トランクに [Mandatory] または [Mandatory (Video Desired)] のロケーション内 RSVP ポリシーを設定します。ロケーション内 RSVP ポリシーを設定するには、ロケーションを選択し、そのロケーションのポリシーを設定します。これにより、このロケーション内のコールでは RSVP コール アドミッション制御が効率よく使用されるようになります。これは、発信元クラスタへのコールの転送または自動転送からコールがトランクにヘアピンされる場合に重要です。

分散型混在コール処理配置

RSVP SIP プレコンディションにより、汎用ネットワーク トポロジで Unified Communications 呼制御アプリケーションを分散配置した環境でコール アドミッション制御を機能させることができます。

ここでは、サポートされている RSVP SIP プレコンディションの配置モデルのリストを示します。これらのモデルにはハイブリッドおよびバリエーションがいくつか考えられます。いずれも有効な設計の概要を示した例にすぎませんが、ベスト プラクティスおよび設計上の考慮事項を踏まえたものです（このような機能の設定の詳細については、特定の製品マニュアルを参照してください）。

図 11-54 に示す配置には、次のガイドラインが適用されます。

- 配置では、音声専用コールの Unified CME SCCP 統合をサポートします。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（「RSVP 設計上のベスト プラクティス」（P.11-33）を参照）。
- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- 「Unified CM と SIP Cisco IOS TDM ゲートウェイおよび Unified CME との相互運用に関する設計の考慮事項」（P.11-64）に記載されている推奨事項に従います。

図 11-54　Unified CM から Cisco IOS ゲートウェイ（TDM）および Unified CME（SCCP）

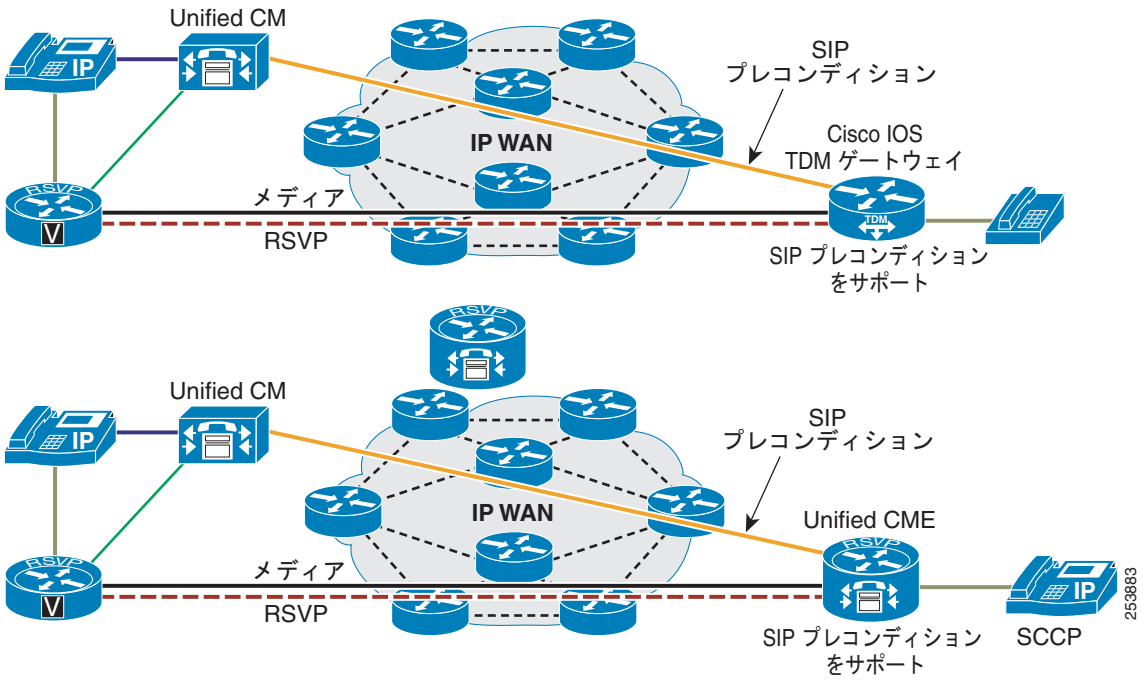


図 11-55 に示す配置には、次のガイドラインが適用されます。

- 次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』に記載されている SIP Cisco IOS TDM ゲートウェイと Unified CME との相互運用性に関するガイドライン、ベスト プラクティス、制限、および制約事項に従います。

  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

- コールが失敗したり、保護されなかったりするのを避けるために、各 Unified CME または SIP Cisco IOS TDM ゲートウェイに一貫性のある RSVP ポリシーを設定します。SIP Cisco IOS TDM ゲートウェイまたは Unified CME に対して RSVP 予約を有効にする場合は、**ダイヤル ピア**設定で次のオプションを使用します。

  ```
  req-qos guaranteed-delay audio
  acc-qos guaranteed-delay audio
  ```

  この設定を行うと、各音声コールに対して、SIP Cisco IOS TDM ゲートウェイは遅延保証付きのサービスを使用して RSVP 予約を要求します。要求された QoS と許容可能な QoS の両方がこの RSVP サービスを指定している場合、コールが成功するためには RSVP 予約が必須になります（予約を確立できない場合はコールが失敗します）。

- アプリケーション ID を使用する場合は、ソリューションの全製品（SIP Cisco IOS TDM ゲートウェイおよび Unified CME）で一貫性を確保します。

- SIP プレコンディションとともに設定した適切なダイヤル ピアが使用されるように、着信と発信のダイヤル ピアを正確に一致させます。詳細については、次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』を参照してください。

  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

図 11-55　Unified CME から Unified CME、Unified CME から Cisco IOS ゲートウェイ、および Cisco IOS ゲートウェイから Cisco IOS ゲートウェイ

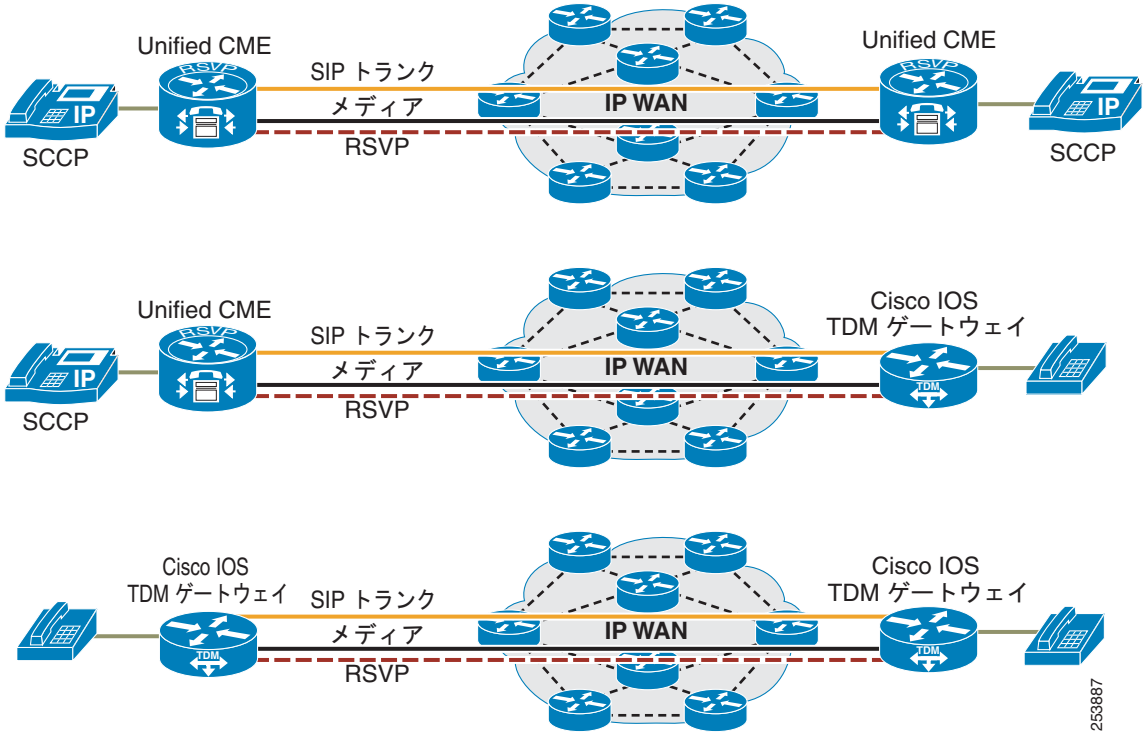


図 11-56 に示す配置には、次のガイドラインが適用されます。

- 分散型コール処理配置の Unified CM の場合は図 11-54 に記載されたガイドラインに従い、Unified CME および SIP Cisco IOS TDM ゲートウェイの場合は図 11-55 に記載されたガイドラインに従います。
- 各 Unified CM クラスタには、一般に Cisco Unified SIP Proxy に向かうトランクが 1 つあります。そのトランクでは、RSVP SIP プレコンディション（エンドツーエンド RSVP）を有効にします。
- Cisco Unified SIP Proxy への SIP トランクで RSVP SIP プレコンディションを有効にします（手順については、「ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションへの移行」（P.11-54）を参照してください）。
- IP Phone ロケーションと SIP トランク ロケーションとの間の各 Unified CM クラスタにロケーション間 RSVP ポリシーを設定します。これにより、Cisco Unified SIP Proxy への SIP トランクを経由するすべてのコールに対して SIP プレコンディションが有効になります。
- RSVP SIP プレコンディションをサポートしない SIP 宛先が存在する可能性がある場合は、ローカル RSVP への RSVP SIP プレコンディションのフォールバックを SIP トランクに設定して、そのコール フロー用の RSVP Agent を割り当てます。また、RSVP SIP プレコンディション フォールバックを有効にする場合は、SIP トランクに関連付けられた RSVP Agent を物理的なサイトに配置して、そのコール フローで RSVP パスが保護されるようにします。
- Unified CME および SIP Cisco IOS TDM ゲートウェイには、一般に Cisco Unified SIP Proxy に向けた SIP ダイヤル ピアが 1 つあります。次の Web サイトで入手可能な『*Cisco IOS SIP Configuration Guide*』の記載に従って、そのダイヤル ピアに RSVP SIP プレコンディション（SIP プレコンディションサポート）を設定します。

  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

- Cisco Unified SIP Proxy に関する設定、ガイドライン、ベスト プラクティス、制限、および制約事項の詳細については、次の Web サイトで入手可能なドキュメントを参照してください。

  http://www.cisco.com/en/US/prod/collateral/modules/ps2797/data_sheet_c78-521390_ps2797_Products_Data_Sheet.html

図 11-56　Cisco Unified SIP Proxy 経由の RSVP SIP プレコンディションに対応したすべてのコンポーネント

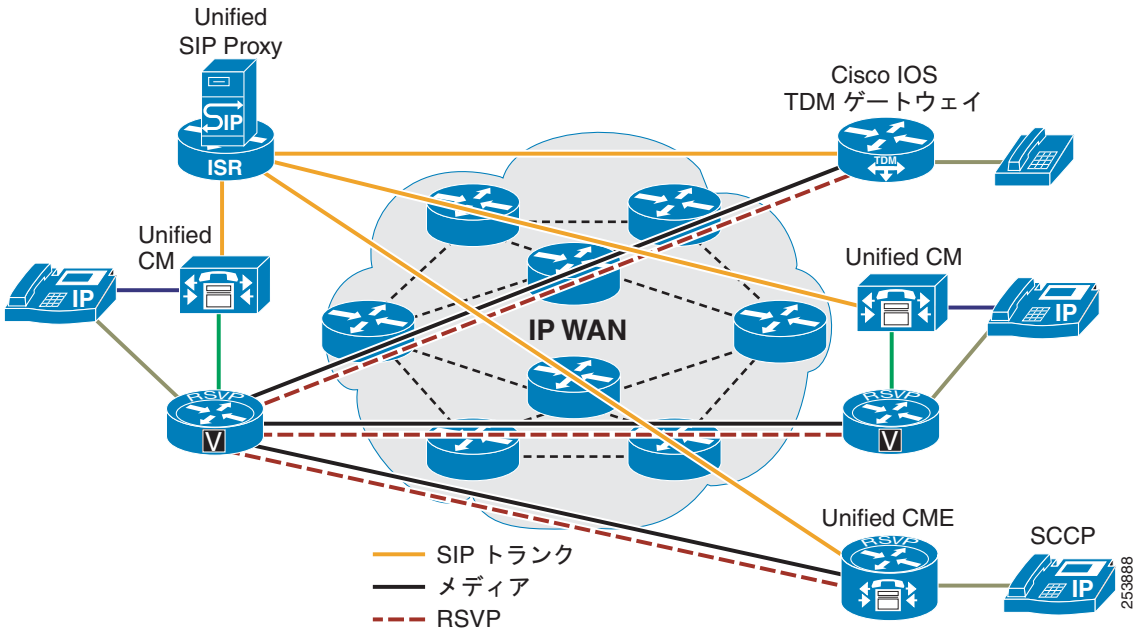


図 11-57 に示す配置には、次のガイドラインが適用されます。

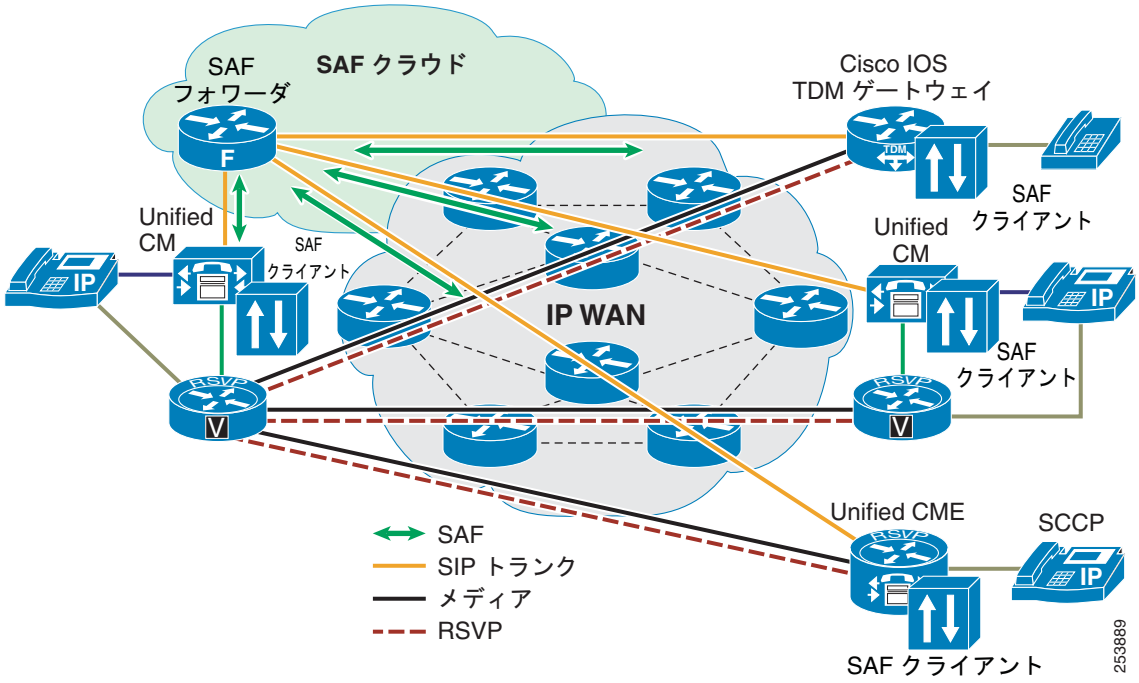
- 分散型コール処理配置の Unified CM の場合は図 11-54 に記載されたガイドラインに従い、Unified CME および SIP Cisco IOS TDM ゲートウェイの場合は図 11-55 に記載されたガイドラインに従います。
- Service Advertisement Framework（SAF）および Call Control Discovery（CCD; コール制御ディスカバリ）をネットワークで有効にし、配置した製品全体で機能させます。SAF 設定の詳細については、次のドキュメントを参照してください。
  - *Cisco IOS Service Advertisement Framework Configuration Guide*

    http://www.cisco.com/en/US/docs/ios/saf/configuration/guide/15_0/saf_15_0_book.html
  - *Cisco Unified Communications Manager Features and Services Guide*

    http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- SAF 対応 SIP トランクで RSVP SIP プレコンディションを有効にします（手順については、「ロケーションベースのコール アドミッション制御から RSVP SIP プレコンディションへの移行」（P.11-54）を参照してください）。
- SAF 対応 SIP トランクで RSVP SIP プレコンディションを有効にします。RSVP SIP プレコンディションの配置のコール制御ディスカバリでは、SAF 対応 SIP トランクだけを使用します。RSVP SIP プレコンディションの配置では、SAF 対応 H.323 トランクは機能しません。

- SAF 対応 SIP トランク ロケーションと自らを含めたすべてのロケーションとの間に、[Mandatory] または [Mandatory (Video Desired)] のロケーション間 RSVP ポリシーを設定します（次のロケーション内 RSVP ポリシーを参照）。これにより、SIP トランク経由で SAF ネットワークを発着するすべてのコールに対して SIP プレコンディションが有効になります。
- SAF 対応 SIP トランクに [Mandatory] または [Mandatory (Video Desired)] のロケーション内 RSVP ポリシーを設定します。ロケーション内 RSVP ポリシーを設定するには、ロケーションを選択し、そのロケーションのポリシーを設定します。これにより、このロケーション内のコールでは RSVP コール アドミッション制御が効率よく使用されるようになります。これは、発信元クラスタへのコールの転送または自動転送からコールがトランクにヘアピンされる場合に重要です。
- RSVP SIP プレコンディション環境で SAF 対応 SIP トランクを使用する場合は、CCD 自動フェールオーバーを有効にし、コール アドミッション制御に失敗したコールをローカル ルート グループにルーティングすることを推奨します。詳細については、「コール制御ディスカバリ自動公衆網フェールオーバー」の項と「ダイヤル プラン」の章の「ローカル ルート グループ」を参照してください。

図 11-57　Service Advertisement Framework（SAF）および Call Control Discovery（CCD; コール制御ディスカバリ）経由の RSVP SIP プレコンディションに対応したすべてのコンポーネント



コール アドミッション制御の設計上の推奨事項

ここでは、さまざまな Cisco Unified Communications Manager（Unified CM）配置でコール アドミッション制御を提供するためのベスト プラクティスについて、簡単に概要を示します。

次の推奨事項は、単一の Unified CM クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Unified CM 静的ロケーションを使用します。ハブ サイト デバイスは Hub_None ロケーションのままにします。
- デュアル リンクのない Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）トポロジでは、（中央サイトを含む）すべてのサイトのデバイスを 1 つのロケーションに割り当てて、Unified CM 静的ロケーションを使用します。
- その他のトポロジでは、Unified CM RSVP 対応ロケーションを使用します。サイト間のデフォルト RSVP ポリシーには、[Mandatory] または [Mandatory (video desired)] ポリシーを推奨します。Cisco RSVP Agent 機能は、比較的小さなサイトでは IP WAN ルータで有効化されている場合もあります。また、比較的大きなサイトではスタンドアロン プラットフォームで実行される場合もあります。

次の推奨事項は、複数の Unified CM クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Unified CM クラスタが存在するサイト間の Cisco IOS ゲートキーパー ゾーンを使用します。
- Unified CM クラスタが第 1 レベルおよび第 2 レベルのハブ サイトに配置された、デュアル リンクのない 2 層ハブアンドスポーク トポロジでは、第 1 レベルと第 2 レベルのハブ サイト間のリンクに Cisco IOS ゲートキーパー ゾーンを使用し、第 2 レベルのハブ サイトとスポーク サイト間のリンクには Unified CM 静的ロケーションを使用します。
- デュアル リンクのない MPLS トポロジでは、すべてのサイトを 1 つのロケーションに配置し、ゲートキーパー ゾーンなしで、Unified CM 静的ロケーションを使用します。MTP が必要な場合を除いて、クラスタ間トランクは Hub_None ロケーションのままにします。クラスタ間コール ルーティング用にはゲートキーパーを使用できますが、コール アドミッション制御では必要ありません。
- それ以外のトポロジには、RSVP を使用します。

CHAPTER 12

IP ビデオ テレフォニー

企業は、Unified Communication システムを導入することで、外部接続に対する公衆網へのコールに加え、企業内のポイントツーポイント コールや会議などの音声サービスを幅広く使用できます。そのようなネットワークにビデオを追加すると、次のアプローチを使用できます。

ビデオ コールをサポートするために音声デバイスを有効にする

企業は、カメラをサポートするために既存の IP 電話を有効にしたり、PC ベース システム上のソフトウェアを使用して IP 電話と組み合わせたビデオ機能を提供したりすることがあります。可能な場合は、ビデオをサポートする新しいデバイスを配置できるため、既存の呼制御インフラストラクチャはそのまま保持されます。

このアプローチには、次の利点があります。

- 既存のダイヤル プラン：企業は、既存のダイヤル プランと既存のコール エージェントを使用してネットワークでビデオ コールをサポートできます。
- コール アドミッション制御：企業内の 1 つのコール アドミッション制御エンティティは、ネットワーク帯域幅の使用を最適化する方法を提供します。
- 既存のネットワーク：企業は、企業のネットワーク上でビデオに対応するために必要な帯域幅を追加することで、既存のネットワーク トポロジを使用できます。
- ユーザ：企業は、既存のすべてのユーザによるビデオ コールの発信を有効にできます。
- ビデオ コーデック：ビデオ コーデックを標準化すると、企業はビデオ コールの帯域幅使用量を最適化できるため、必要なトランスコーディング リソースまたはトランスレーティング リソースを減らすことができます。
- 既存の IP 電話：企業は、ビデオを追加するためにソフト クライアントを追加するか、カメラと IP 電話を接続することで、既存の IP 電話を利用できます。

音声ネットワークを既存のビデオ ネットワークと統合する

会議室のビデオ コールまたは経営幹部用ビデオ デバイスに既存のビデオ ネットワークを使用している企業は、ビデオ ネットワークと音声ネットワークを統合できるため、企業のユーザがビデオ デバイスを呼び出すことができるようになります。

このアプローチには、次の利点があります。

- 別個のダイヤル プラン：ビデオ ネットワークの別個のダイヤル プランを使用すると、企業はビデオ カンファレンス ブリッジ、ビデオ PSTN ゲートウェイなどのビデオ リソースのプランを作成できます。ユーザは、プレフィックスをダイヤルして他のネットワークのリソースにアクセスできます。

- 既存のネットワーク：企業は、既存の重複したネットワーク トポロジを別個のビデオ ネットワークと音声ネットワークとして使用できます。
- 管理とモニタリング：音声およびビデオの別個の管理とモニタリングにより、トラブルシューティングおよび問題の解決がさらに容易になります。
- トランク プロトコル：企業は、音声とビデオのコール エージェント間で相互作用する必要なプロトコルを選択できます。これにより、企業はコール転送、DTMF、MWI、他の機能に同様の方法を使用できます。
- コール エージェント機能に依存しない：企業は、コールのビデオ トラフィックのビット レートの最適化など、ビデオ コール エージェントがビデオ エンドポイントに提供する機能を活用できます。これらの機能は音声コール エージェントの機能に依存しません。

企業は、上記のアプローチのいずれかを選択したり、上記のアプローチを組み合わせて企業のユーザがビデオ コールを発信したりできます。

ビデオは Cisco Unified Communications Manager（Unified CM）に完全に統合され、シスコおよびシスコの戦略パートナーから多くのビデオ エンドポイントも入手できるようになりました。たとえば、Cisco Unified Video Advantage は、Cisco Unified IP Phone と同様に簡単に配置、管理、および使用できます。

この章の新規情報

表 12-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

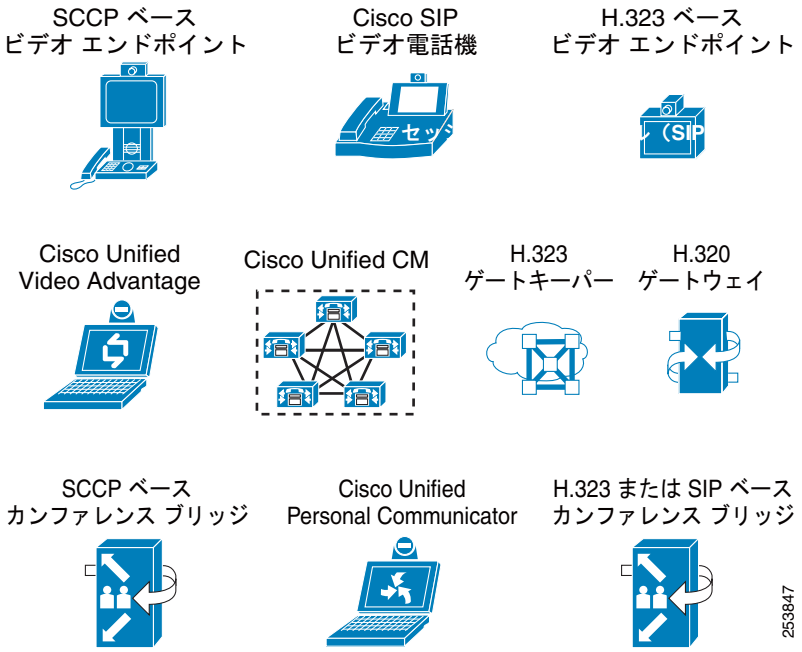
表 12-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 6 月 2 日
SIP クライアント	「エンドポイント」（P.12-5）	2010 年 11 月 15 日
ビデオ コール用トランク	「トランク」（P.12-15）	2010 年 11 月 15 日
ビデオ エンドポイント	「エンドポイント」（P.12-5）	2010 年 11 月 15 日
Cisco Unified IP Phone 9900 シリーズ	この章の各項で説明	2010 年 4 月 2 日

IP ビデオ テレフォニー ソリューションのコンポーネント

Cisco IP ビデオ テレフォニー ソリューションは、Cisco Unified Communications Manager（Unified CM）、H.323 電話会議、セッション開始プロトコル（SIP）電話会議、および Skinny Client Control Protocol（SCCP）電話会議に対応する Cisco Unified Videoconferencing 3500 および 5000 シリーズ Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、Cisco Unified Videoconferencing 3500 シリーズ H.320 ゲートウェイ、Cisco IOS H.323 ゲートキーパー、Cisco Unified IP Phone 9900 シリーズ、Cisco IP Video Phone E20、Cisco Unified Personal Communicator、Cisco Unified Video Advantage、Cisco Unified IP Phone 7985、サードパーティ製の SCCP ビデオ エンドポイント ソリューション、および Polycom、Lifesize、Sony などのパートナーが取り扱っている既存の H.323 または SIP 準拠製品で構成されます（図 12-1 を参照）。

図 12-1　IP ビデオ テレフォニーのコンポーネント



管理に関する考慮事項

この項では、ビデオ テレフォニーに関係する Unified CM Administration の次の構成要素について説明します。

- 「プロトコル」（P.12-3）
- 「エンドポイント」（P.12-5）
- 「リージョン」（P.12-5）
- 「トポロジ対応ロケーション」（P.12-8）
- 「Retry Video Call as Audio」（P.12-10）
- 「Wait for Far-End to Send TCS」（P.12-13）
- 「トランク」（P.12-15）

プロトコル

Unified CM は、多くのプロトコルをサポートします。任意のデバイスから任意の別のデバイスを呼び出すことができますが、ビデオは SCCP、H.323、および SIP デバイスでのみサポートされます。具体的には、Cisco Unified CM Release 8.*x* において、次のプロトコルではビデオがサポートされません。

- コンピュータ テレフォニー インテグレーション（CTI）アプリケーション（TAPI および JTAPI）
- メディア ゲートウェイ コントロール プロトコル（MGCP）

したがって、現在 Unified CM でサポートされるコールのタイプは、表 12-2 に示すとおりです。

表 12-2　Unified CM Release 8.x でサポートされるコールのタイプ

発信デバイス タイプ	着信デバイス タイプ				
	SCCP	H.323	MGCP	TAPI/JTAPI	SIP
SCCP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ
H.323	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ
MGCP	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
TAPI/JTAPI	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
SIP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ

表 12-3 は、現在 Unified CM でサポートされている音声とビデオのアルゴリズムおよびプロトコルを示しています。

表 12-3　Unified CM Release 8.x でサポートされる機能

H.323	SCCP	SIP
H.261	H.261	H.261
H.263、H.263+	H.263、H.263+	H.263、H.263+
H.264	H.264	H.264
G.711 A-law および mu-law	G.711 A-law および mu-law	G.711 A-law および mu-law
G.723.1	G.723.1	G.723.1
G.728	G.728	G.728
G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab
G.722	G.722	G.722
G.722.1		
		iLBC
		iSAC
		AAC-LD
H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし	H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません）プロトコル インターワーキングなし	H.224 遠端カメラ制御（Unified CM でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし
アウトオブバンド DTMF（H.245 英数字） RFC2833 AVT Tones（SIP コールへの H.323 クラスタ間トランクの場合のみ）	アウトオブバンド DTMF RFC2833 AVT Tones	RFC2833 AVT Tones Unsolicited SIP Notify KPML

エンドポイント

IP 電話は、Cisco Unified Communications システムにおける最も一般的なビデオ エンドポイントです。ユーザ用にビデオを IP 電話に追加するために、企業は Cisco Unified IP Phone 9971 にカメラを使用したり、Cisco E20 Video Phone などのエンドポイントを使用したり、Cisco Unified Video Advantage を実行する PC に IP 電話を接続したりできます。また、企業は Cisco Unified Personal Communicator などのソフト クライアントを配置することもできます。

さらに、Cisco Unified CM を使用して H.323 や SIP などのプロトコルをサポートするエンドポイントを配置することもできます。H.323 の使用は、主にデータ共有（たとえば、ビデオ コール時に PC 画面を共有する）に H.239 を使用するかどうか、あるいはエンドポイント間にセキュア メディアがあるビデオ コールのエンドポイント間でセキュア トークンを渡すために H.235 を使用するかどうかで決定されます。SIP は、主にセキュア ビデオ コールおよび会議に Secure RTP（SRTP）が必要である場合に使用されます。プレゼンスなどのユーザ機能のタイプにより、エンドポイントで使用されるプロトコルのタイプが決定されます。プロトコル選択は主にエンドポイントで必要な機能のサポートに依存します。

Cisco Unified CM によりサポートされる SIP ビデオ デバイスには、Cisco 9900 Series IP Phone、Cisco E20 Video Phone、Cisco Cius、サードパーティ製 SIP デバイス（拡張）、または汎用デスクトップおよびルーム システムのビデオ デバイスがあります。Cisco 9900 Series IP Phone では、そのデバイスのビデオ機能設定によってビデオを有効にできます。Cisco E20 Video Phone の設定は、その電話自体にあります。Cius は、前面にカメラがあるコールのためのビデオをサポートします。サードパーティ製 SIP デバイス（拡張）の電話タイプや汎用ビデオ デバイスは、Polycom 社製、Lifesize 社製、Sony 社製および他の製造業者のエンドポイントに対する追加オプションです。これらのエンドポイントに関して Unified CM の設定は以前のバージョンから変更されていませんが、Cisco E20 Video Phone、Cisco Cius、Tandberg 社製のエンドポイントとサードパーティ製のエンドポイントをより効率的にサポートするために Unified CM の動作が最適化されています。それらのエンドポイントからのアーリー オファーを処理して MTP リソースを使用せずに SIP トランクを介してそれらのエンドポイントを処理する機能などの機能により、コール シグナリングが最適化され、コールのメディアを確立する時間が短縮されます。また、2 つのデバイス間の最適なビデオ コールを実現するために追加のシグナリング（エンドポイント間で渡される RTCP やパラメータなど）が処理および送信されるように、Unified CM では、それらのエンドポイントの HD コールもサポートしています。Cius は、結合された場合はビデオ電話機として、また分離された場合は Wi-Fi タブレットとして柔軟に使用できるため、追加の考慮事項が必要ですが、音声には Wi-Fi ネットワークが推奨され、またコールには適切な帯域幅を使用する必要があります。無線の展開の詳細については、「モバイル ユニファイド コミュニケーション」（P.25-1）の章を参照してください。

各種 IP 電話と Cisco Unified Video Advantage の詳細については、「Unified Communications エンドポイント」（P.18-1）の章を参照してください。Cisco Unified Personal Communicator、Client Services Framework などのソフトウェア クライアントの詳細については、「Cisco Collaboration クライアントおよびアプリケーション」（P.24-1）の章を参照してください。

ユーザがビデオ コールを発信するための適切な IP 電話とエンドポイントの選択は、目的の機能とビデオ コールに必要な機能によって異なります。使用可能なオプションにより、さまざまなタイプのユーザにクライアントを柔軟に設計および配置できます。

リージョン

リージョンを設定するときは、Unified CM Administration の 2 つのフィールド、[Audio Codec] と [Video Bandwidth] を設定します。オーディオ設定ではコーデック タイプを指定し、ビデオ設定ではコールごとの帯域幅の量を指定します。ただし、表記は異なりますが、[Audio Codec] フィールドと [Video Bandwidth] フィールドは、実際には似た機能を実行します。[Audio Codec] フィールドは、音声のみのコールおよびビデオ コールの音声チャネルに許可される最大ビット レートを定義します。たとえば、リージョンの [Audio Codec] を G.711 に設定した場合、Unified CM はそのリージョンの音声

チャネルに許可される最大帯域幅として 64 kbps を割り当てます。この場合、Unified CM は G.711、G.722、G.728、iLBC、または G.729 を使用するコールを許可します。ただし、[Audio Codec] を G.729 に設定すると、Unified CM は、音声チャネルに許可される帯域幅の最大量として 8 kbps だけを割り当てます。この場合、iLBC、G.728、G.711、および G.722 はすべて 8 kbps より多く帯域幅を使用するため、G.729 を使用するコールだけが許可されます。

（注）　両方のエンドポイントが G.711 と G.722 をサポートしている場合、ワイドバンド コーデックである G.722 がネゴシエートされます。

[Video Bandwidth] フィールドは、コールのビデオ チャネルに許可される最大ビット レートを定義します。ただし、従来のビデオ会議製品での慣例に従い、このフィールドに使用する値には、音声チャネルの帯域幅も含めます。たとえば、G.711 の音声を使用する 384 kbps のコールを許可するには、[Video Bandwidth] フィールドに 320 kbps ではなく 384 kbps を設定します。

（注）　[Audio Codec] 設定は、ビデオ コールの音声チャネルにも適用されます。

つまり、[Audio Codec] フィールドは音声のみのコールおよびビデオ コールの音声チャネルに使用する最大ビット レートを定義し、[Video Bandwidth] フィールドは、ビデオ コールに許可される最大ビット レート（コールの音声部分を含む）を定義します。

各デバイスは、表 12-4 で示すように、特定の音声コーデックのみをサポートするため、正しい音声コーデックの帯域幅制限を選択することが重要です（特定のエンドポイントでサポートされるコーデックの最新リストについては、そのエンドポイントの製品マニュアルを参照してください）。

表 12-4　エンドポイント デバイスでサポートされている音声コーデックのタイプ

コーデック タイプ	Cisco 7900 および 9900 シリーズ IP Phone	SCCP サードパーティ製ビデオ エンドポイント	一般的な H.323 または SIP エンドポイント	Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイ	Cisco Unified Videoconferencing 3500 および 5000 シリーズ MCU
G.729	あり	あり、モデルによる	なし	なし	あり、モデルによる
G.728	なし	あり、モデルによる	あり	あり	あり、モデルによる
G.711	あり	あり	あり	あり	あり
G.722	あり、モデルによる	あり	あり	あり	あり、モデルによる

表 12-4 で示すように、リージョンを G.729 に設定した場合、ビデオ会議デバイスによっては、このタイプのコーデックをサポートできないものがあります。たとえば、Cisco Unified Video Advantage エンドポイントと Tandberg T1000 エンドポイントとの間のコールは失敗します。または、このコールに Unified CM が音声変換リソースを割り当てます。

Cisco Unified CM Release 5.0 では、Cisco IOS Enhanced Media Termination Point に基づく音声変換リソースが導入されました。これによって、パススルー コーデックによるビデオ ストリームのサポートを継続しながら、ビデオの音声ストリームのトランスコーディングができます。パススルー コーデックは、トランスコーディングが必要なストリームには使用できないため、ビデオ ストリームにのみ使用されます。パススルー コーデックを使用するには、次の 3 つの条件をすべて満たす必要があります。

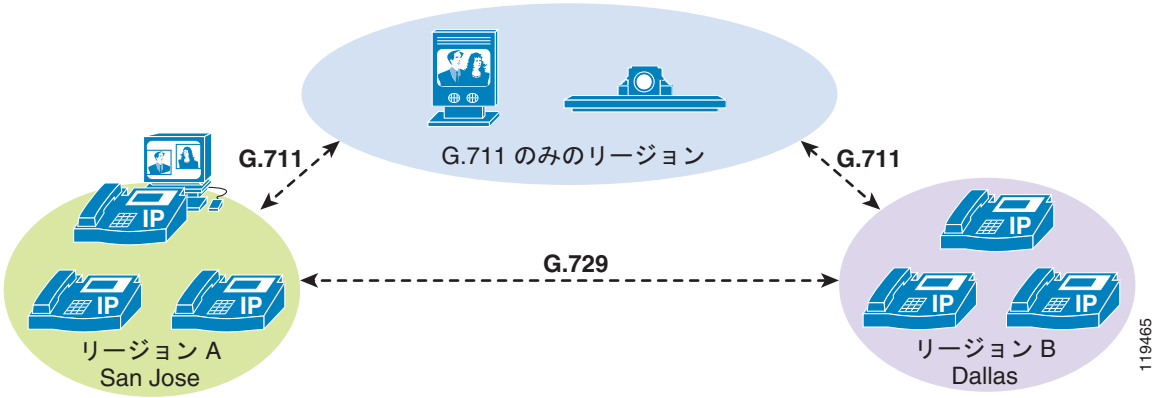
- 2 つのエンドポイント デバイスのコーデック能力が一致している。

- どちらのエンドポイントでも、[MTP Required] がオフになっている。
- すべての中間リソース デバイス（MTP およびトランスコーダ）がパススルー コーデックをサポートしている。

従来のトランスコーダは、現在、パススルー機能をサポートしていません。そのため、コールは音声のみとして接続され、G.729 と G.711 の間でトランスコーディングされます。Cisco IOS Enhanced Transcoder を使用せずにこの状態を防止するには、G.711 を使用するようにリージョンを設定する必要があります。ただし、G.711 に設定されたリージョンは、2 つの IP Phone 間の音声コールにも G.711 を使用します。この場合、WAN で消費される帯域幅が増えます。

帯域幅を節約するために音声のみのコールに G.729 を使用し、ビデオ コールに G.711 を使用する場合は、G.729 をサポートしないビデオ エンドポイント用に G.711 を使用するリージョンを設定し、IP Phone 用に G.729 を使用する別のリージョンを設定する必要があります（図 12-2 を参照）。この方式を使用すると、必要なリージョンの数が増えますが、望ましいコーデックと帯域幅の割り当てが得られます。

図 12-2　ビデオ コールに G.711 を使用し、音声のみのコールに G.729 を使用



（注） ビデオを禁止するリージョンのペアを設定できます。このリージョン ペアにある 2 つのビデオ対応デバイスが相互に通話しようとした場合、[Retry Video Call as Audio] がオンになっていれば、音声のみとして接続されます。オフになっている場合は、AAR 再ルーティング ロジックが実行されます。

表 12-5 は、設定例とその結果を示しています。

表 12-5　さまざまなリージョン設定のシナリオ

リージョン設定	[Retry Video as Audio] の設定	結果
リージョンでビデオを許可する。	有効	ビデオ コールは許可される。
リージョンでビデオを許可する。	無効	ビデオ コールは許可される。
リージョンでビデオを許可しない。	有効	ビデオ コールは音声として処理される。
リージョンでビデオを許可しない。	無効	AAR が設定されていない場合、ビデオ コールは失敗する（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）。

[Video Call Bandwidth] フィールドには、1 ～ 32,256 kbps の値を指定できます。ただし、H.323 および H.320 ビデオ会議デバイスとの互換性を維持するために、このフィールドには常に、56 または 64 kbps の倍数の値を入力することを推奨します。したがって、このフィールドの有効な値としては 112 kbps、128 kbps、224 kbps、256 kbps、336 kbps、384 kbps などがあります。

エンドポイントで要求されるコール速度がリージョンに設定されている帯域幅値を超えた場合、Unified CM は自動的に、リージョン設定で許可された値に適合するようにコールをネゴシエートします。たとえば、H.323 エンドポイントが別の H.323 エンドポイントを 768 kbps で呼び出しているが、リージョンは最大 384 kbps を許可するように設定されていたとします。発信側からの着信 H.225 セットアップ要求はコール速度として 768 kbps を提示しますが、Unified CM は、着信側への発信 H.225 セットアップ メッセージで、この値を 384 kbps に変更します。そのため、着信側エンドポイントは、開始するコールが 384 kbps であると認識し、このレートでコールがネゴシエートされます。発信側エンドポイントは、要求した帯域幅として 768 kbps を提示しますが、ネゴシエートされた帯域幅は 384 kbps になります。

ただし、リージョンの [Video Bandwidth] を「None」に設定した場合は、着信側デバイスの [Retry Video Call as Audio] が有効かどうかに応じて、Unified CM はコールを終了するか（この場合、H.225 Release Complete メッセージを発信側に送信）、音声のみのコールとして通過を許可します（「Retry Video Call as Audio」（P.12-10）を参照）。

コールのビデオ解像度が高くなるにつれて、必要な帯域幅も大きくなります。リージョン設定のビデオ帯域幅には、CIF ビデオ解像度が必要な場合は 384 kbps を、VGA 解像度が必要な場合には 768 kbps を、720p 解像度のビデオ コールが必要な場合には 1.5 Mbps を設定することを推奨します。ほとんどのビデオ エンドポイントには可変ビット レート エンコーダが備えられていますが、Cisco Unified IP Phone 9900 シリーズなどのビデオ電話機には固定ビット レートのビデオ用エンコーダが備えられています。固定ビット レートのエンコーダでは、より良いモーション ビデオおよびエラー復元性が提供されます。

Cisco Unified Video Advantage などのいくつかのエンドポイントでは、コールの CIF 解像度が使用されます。そのようなデバイスからのビデオ コールの CIF 解像度を制限するために、ビデオ コール帯域幅のリージョン設定を 384 kbps にして、デバイスをこのリージョンに関連付けることができます。この結果、高解像度のエンドポイントへのコールまたは MCU への会議では、ビデオの CIF 解像度がネゴシエートされます。

トポロジ対応ロケーション

ロケーション間のコールで使用できる帯域幅の量を制限する方式は、2 種類あります。Cisco Unified CM 4.0 では、ロケーションでのビデオ コールのサポートが導入されました。具体的には、Cisco Unified CM のロケーション オプションによって、あるロケーションと別のロケーションの間のすべてのコールに許可される合計帯域幅が定義されます。この合計帯域幅の値は、従来のハブアンドスポーク ネットワーク トポロジに十分に対応します。Cisco Unified CM Release 5.*x* では、リソース予約プロトコル（RSVP）に基づくトポロジ対応ロケーションを使用して、2 つのサイト間のパスに十分な帯域幅があるかどうかを判断するオプションが用意されています。RSVP を使用すると、複雑なトポロジに対応するホップ単位のチェックが可能になり、RSVP アプリケーション ID を使用して音声帯域幅とビデオ帯域幅を個別にサポートできます。

（注）　静的ロケーションと RSVP ベースのロケーションは、異なるモデルを使用して、音声コールとビデオコールを区別します。詳細については、「コール アドミッション制御」（P.11-1）を参照してください。

RSVP ベースのロケーションでは、RSVP ポリシーの概念が採用されています。多くのポリシー オプションがありますが、主に次の 2 つのカテゴリに分けられます。

- コールを完了するために、ビデオ ストリームの RSVP 予約が必須。コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます。
- ビデオ ストリームの RSVP 予約が望ましい。

最初に、リージョンに設定された音声コーデックとビデオ帯域幅で、ビデオ コールの最大速度（ビット レート）が定義されます。予約要求として、最大ビット レートを使用してコールのオーディオ ストリームとビデオ ストリームの RSVP 予約が Cisco RSVP Agent から送信されます。ビデオ ストリームの RSVP 予約が失敗した場合、Unified CM は RSVP ポリシーの設定をチェックし、このコールの処理方法を決定します。オーディオ ストリームのポリシーがオプションの場合、コールは音声のみとして継続します。オーディオ ストリームの RSVP ポリシーが必須の場合は、オーディオ ストリームも RSVP 予約の取得に失敗した場合を除いて、コールは音声のみとして継続します。予約に失敗した場合、コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます（トポロジ対応ロケーションの詳細については、「コール アドミッション制御」（P.11-1）を参照してください）。

（注） ビデオ優先ポリシーを使用しているときに、ビデオ予約に失敗した場合、コールは音声のみとして完了します。ただし、ユーザはビデオが失敗した原因を示す、視覚的な表示または音声によるフィードバックを受けることができません。

静的ロケーションを設定するときも、Unified CM Administration の 2 つのフィールド、[Audio Bandwidth] と [Video Bandwidth] を設定します。ただし、リージョンと異なり、静的ロケーションの Audio Bandwidth は音声のみのコールにのみ適用され、Video Bandwidth はビデオ コールの音声チャネルとビデオ チャネルの両方に適用されます。音声帯域幅とビデオ帯域幅は、別々に維持されます。これは、両方のタイプのコールが帯域幅の単一割り当てを共有すると、音声コールが使用可能な帯域幅のすべてを使用してビデオ コール用の帯域幅が残らなくなる（または、その逆になる）可能性が高いためです。また、音声とビデオの個別の帯域幅プールは、ネットワーク上のスイッチおよびルータでのキューの設定方法に対応します。通常、音声トラフィック用のプライオリティ キューと、ビデオ トラフィック用の独立したプライオリティ キューまたはクラスベース WFQ があります。詳細については、「WAN の QoS」（P.3-40）を参照してください。

[Audio Bandwidth] フィールドと [Video Bandwidth] フィールドのどちらにも、[None]、[Unlimited]、または数値を指定する 3 つのオプションがあります。ただし、これらのフィールドに入力する値は、2 つの異なる計算モデルを使用します。[Audio Bandwidth] フィールドに入力する値には、コールに必要なレイヤ 3 ～ 7 のオーバーヘッドを含める必要があります。たとえば、ロケーションとの間で単一の G.729 コールを許可する場合は、値として 24 kbps を入力します。G.711 コールの場合は、値として 80 kbps を入力します。一方、[Video Bandwidth] フィールドには、オーバーヘッドを含めない値を入力する必要があります。たとえば、128 kbps コールの場合は 128 kbps を入力し、384 kbps コールの場合は 384 kbps を入力します。リージョンの [Video Bandwidth] フィールドで使用する値と同様に、ロケーションの [Video Bandwidth] フィールドにも、56 kbps または 64 kbps の倍数の値を使用することを推奨します。

たとえば、企業に 3 サイトのネットワークがあるとします。San Francisco ロケーションには、San Jose メイン キャンパスに接続された 1.544 Mbps T1 回路があります。システム管理者は、このロケーションとの間で、4 つの G.729 音声コールと 1 つの 384 kbps（または 2 つの 128 kbps）ビデオ コールを許可します。Dallas ロケーションには、San Jose メイン キャンパスに接続された 2 つの 1.544 Mbps

T1 回路があります。管理者は、このロケーションとの間で、8 つの G.711 音声コールと 2 つの 384 kbps ビデオ コールを許可します。この例で、管理者は、San Francisco ロケーションと Dallas ロケーションに次の値を設定します。

ロケーション	必要な音声コールの数	[Audio Bandwidth] フィールドの値	必要なビデオ コールの数	[Video Bandwidth] フィールドの値
San Francisco	4、G.729 を使用	96 kbps（4 * 24 kbps）	1、384 kbps	384 kbps
Dallas	8、G.711 を使用	640 kbps（8 * 80 kbps）	2、384 kbps	768 kbps

エンドポイントで要求されるコール速度がロケーションに設定されている値を超えた場合、リージョンの場合とは異なり、Unified CM がロケーション設定で許可された値に適合するように、*自動的にコール速度をネゴシエートすることはありません*。コールは拒否されるか、音声のみのコールとして再試行されます（着信側デバイスで [Retry Video as Audio] 設定が有効の場合）。そのため、リージョンのビデオ帯域幅は、ロケーションのビデオ帯域幅の値よりも低い値に設定する必要があります。たとえば、2 つのリージョン（リージョン A とリージョン B）があり、これら 2 つのリージョン間のビデオ帯域幅が 768 kbps に設定されている場合、リージョン A のデバイスがビデオ帯域幅が 384 kbps に設定されているロケーションにあると、これら 2 つのリージョン間のすべてのコールが失敗するか、音声のみのコールになります（[Retry Video Call as Audio] の設定による）。

Retry Video Call as Audio

このチェックボックスは、Cisco Unified IP Phone 7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、7975、および Cisco IP Video Phone 7985、サードパーティ製の SCCP ビデオ エンドポイント、すべての H.323 および SIP デバイス（クライアント、ゲートウェイ、およびすべてのタイプの H.323 トランク）など、ビデオをサポートするすべての SCCP エンドポイント タイプで使用できます。このオプションがアクティブ（オン）のときに、デバイスに到達できるだけの帯域幅がない場合（たとえば、Unified CM リージョンまたはロケーションで、そのコールのビデオが許可されない場合）、Unified CM はそのコールを音声のみのコールとしてリトライします。このオプションが非アクティブ（オフ）のときは、Unified CM はコールを音声のみとして再試行することなく、コールを失敗させるか、Automated Alternate Routing（AAR; 自動代替ルーティング）パスが設定されている場合は可能な限り再ルーティングします。デフォルトでは、このリトライ オプションは有効（オン）です。

この機能は、次のシナリオだけに適用されます。

- ビデオを許可しないようにリージョンが設定されている。
- ビデオを許可しないようにロケーションが設定されている。または、ロケーションが RSVP ポリシーを使用しない場合は、要求されたビデオ速度が、そのロケーションで使用可能なビデオ帯域幅を超えている。
- Unified CM クラスタ間のコールの場合、要求されたビデオ速度がゲートキーパーのゾーン帯域幅制限を超えている。

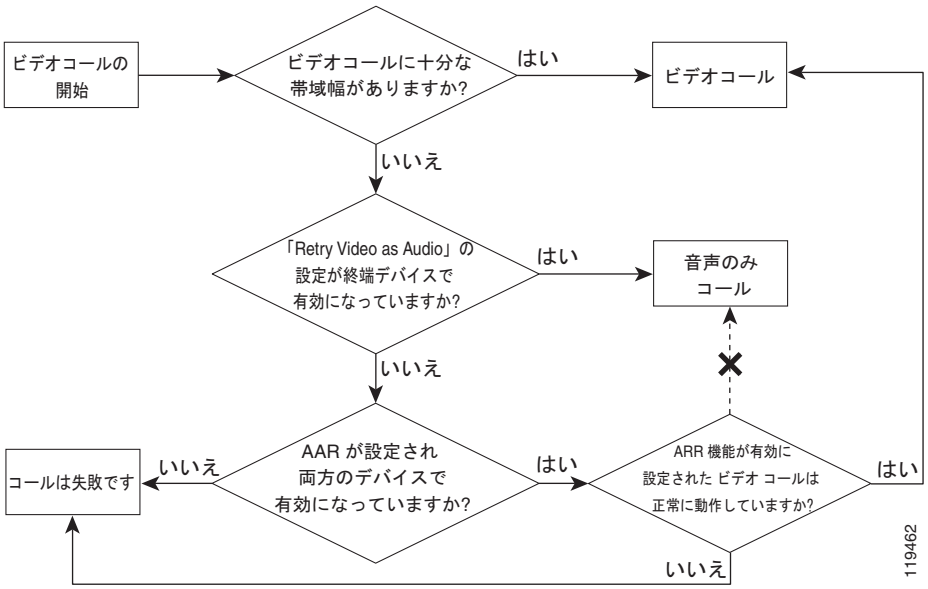
Retry Video Call as Audio オプションは、終端（着信側）デバイスでのみ有効です。そのため、発信側デバイスでは宛先ごとに異なるオプション（再試行または AAR）を使用できる柔軟性があります。

帯域幅の制限が原因でビデオ コールが失敗した場合、自動代替ルーティング（AAR）が有効であれば、Unified CM は失敗したコールをビデオ コールとして AAR の宛先に再ルーティングしようとします。AAR が有効でない場合、失敗したコールによって、発信者にビジー トーンとエラー メッセージが送信されます（図 12-3 を参照）。発信側のデバイスのタイプによって、失敗したコールは次のいずれかになります。

- 発信側デバイスが LCD 画面付き SCCP エンドポイントの場合、発信者にはビジー トーンが聞こえ、メッセージ「Bandwidth Unavailable」がデバイスに表示されます。

- 発信側デバイスが LCD 画面なしの SCCP エンドポイントの場合（Cisco Unified IP Phone 7902 など）、発信者にはビジー トーンが聞こえます。
- 発信側デバイスが H.323 または SIP デバイス、またはゲートウェイで接続された公衆網デバイスの場合、発信者にはビジー トーンが聞こえ、Unified CM が適切なエラー メッセージ（Q.931 Network Congestion 原因コードなど）を H.323、SIP、または MGCP デバイスに送信します。

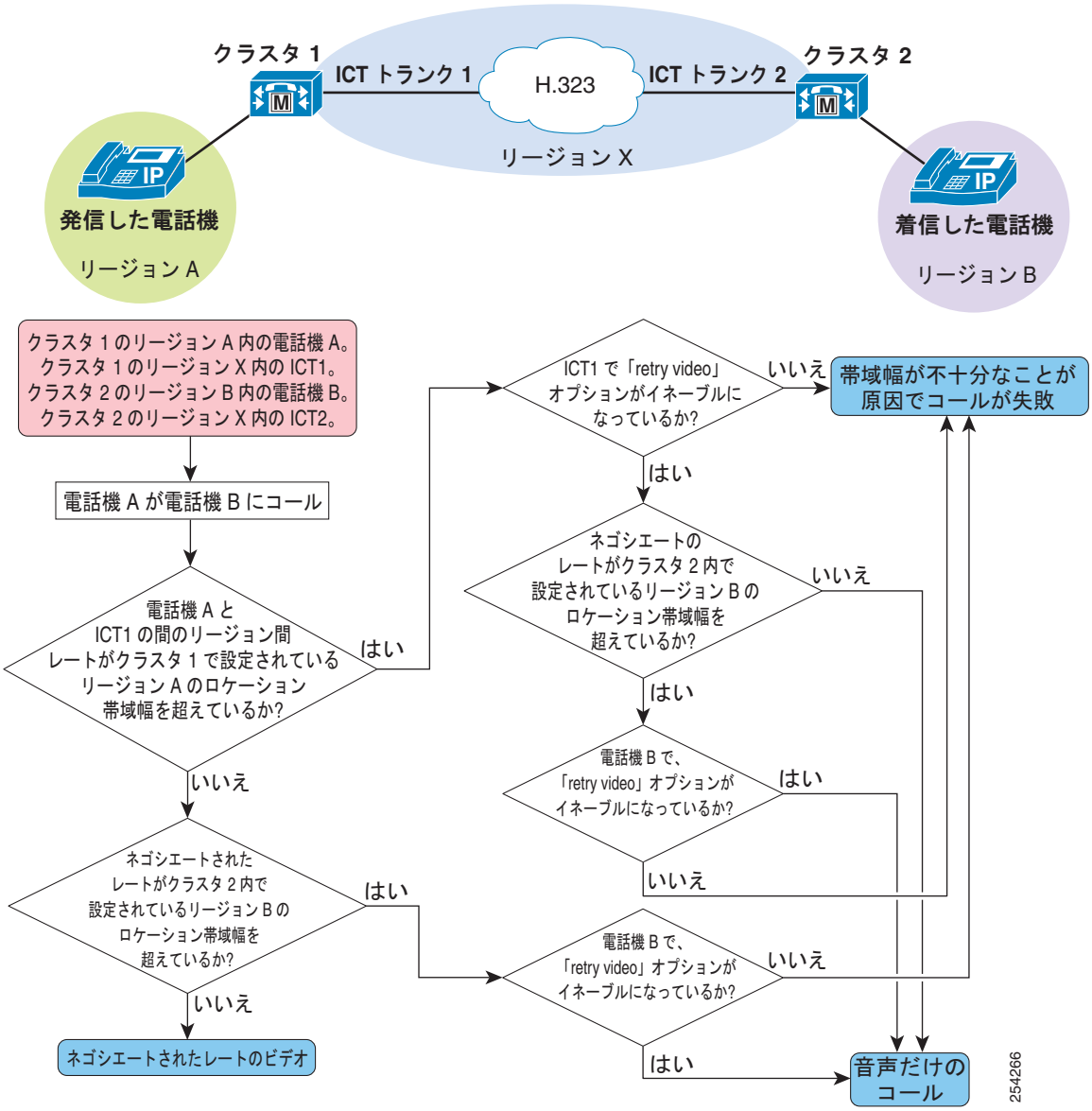
図 12-3　　ビデオ コールで起こり得るシナリオ



AAR の使用方法の詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください。

図 12-4 は、非ゲートキーパー制御クラスタ間トランクを使用する、2 つのクラスタ間のコールの手順を示しています。

図 12-4　非ゲートキーパー制御クラスタ間トランクを使用する 2 つのクラスタ間のコール フロー



Wait for Far-End to Send TCS

このチェックボックスは、H.323 クライアント、H.323 ゲートウェイ、H.225 ゲートキーパー制御トランクなど、すべての H.323 デバイスで使用できます。この機能は、H.323 コールの H.245 機能交換フェーズに関係します。この機能を有効にすると、Unified CM は、Unified CM が Terminal Capabilities Set（TCS; 端末機能セット）を H.323 デバイスに送信する前に、リモート H.323 デバイスが TCS を Unified CM に送信するまで待機します。このオプションが無効の場合、Unified CM は待機せず、すぐに TCS をリモート H.323 デバイスに送信します。

デフォルトでは、[Wait for Far-End to Send TCS] オプションが有効（オン）です。ただし、次の場合はオフ（無効）にする必要があります。

- Unified CM と通信する H.323 デバイスも、遠端が TCS を送信するまで待機する。

  この場合、どちらの側も TCS を送信しないためデッドロックが発生し、数秒後に H.245 接続がタイムアウトします。遠端が TCS を送信するまで待機するデバイスの例としては、一部の H.323 ルーテッドモード ゲートキーパー、H.320 ゲートウェイ、H.323 プロキシ（IP-to-IP ゲートウェイ）、一部の H.323 マルチポイント カンファレンス ブリッジがあります。これらのデバイスが遠端からの TCS の送信を待機する理由は、Unified CM が待機する理由と同じです。TCS を他方に転送する前に、接続の両端が TCS を送信するまで待機するためです。

- クラスタ間トランクを介して別の Unified CM クラスタと通信している。

（注）　クラスタ間トランクおよびゲートキーパー制御クラスタ間トランクでは、[Wait for Far-End to Send TCS] オプションは常に無効で、有効にはできません。

多くのシナリオで、Unified CM は、2 つのエンドポイント デバイス（相互に通話しようとする 2 つの H.323 クライアントなど）を接続するソフトウェア スイッチの役割を実行します。このような場合、両方のデバイスが TCS メッセージを送信するまで Unified CM が待機することが最良です。Unified CallManager が各デバイスの機能を認識することで、それぞれに送信する TCS に関して（特に、リージョンおよびロケーションの設定に応じて）最適な判断ができます。この場合、Wait for Far-End to Send TCS 機能は有効にする必要があります。

ただし、その他の H.323 デバイス（H.323 デバイスを H.320 デバイスに接続する H.320 ゲートウェイなど）が、複数の参加者を接続する機能を実行することもあります。また、ゲートウェイも、コールのセットアップ方法に関して最適な選択ができるように、両端が TCS メッセージを送信するまで待機します。Unified CM とゲートウェイの両方が、相手側から TCS が送信されるまで待機すると、デッドロックが発生します。このデッドロック状態を防止するには、Wait for Far-End to Send TCS 機能を無効（オフ）にします。

たとえば、図 12-5 で示す次のコール シナリオについて考えます。

- シナリオ 1：Cisco Unified Video Advantage が H.320 エンドポイントを呼び出す。
- シナリオ 2：H.323 クライアントが H.320 エンドポイントを呼び出す。

これらのシナリオでは、どちらの場合も、Wait for Far-End to Send TCS 機能は、デフォルト設定である有効（オン）のままにします。

図 12-5　Wait for Far-End to Send TCS 機能が有効（オン）のシナリオ

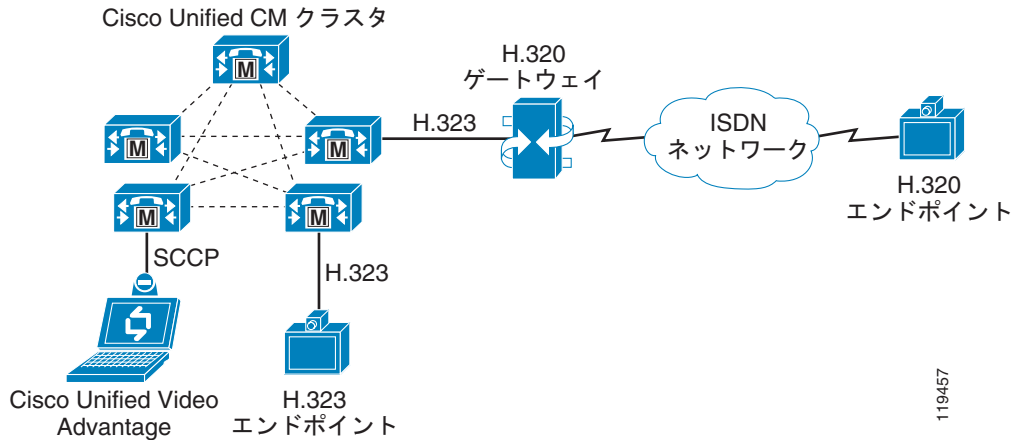


図 12-5 のシナリオ 1 では、登録時に SCCP デバイスがメディア機能を Unified CM に提供しているため、Unified CM はすでに Cisco Unified Video Advantage クライアントの機能を認識しています。しかし、ゲートウェイがコールの H.245 フェーズで TCS を Unified CM に送信するまで、Unified CM は H.320 ゲートウェイの機能を認識しません。同様に、H.320 エンドポイントが TCS をゲートウェイに送信するまで、H.320 ゲートウェイは、Unified CM に送信する TCS を判断できません。この場合、H.320 エンドポイントがゲートウェイに TCS を送信し、ゲートウェイが Unified CM に TCS を送信し、判断に使用できる両端のエンドポイントからの TCS を Unified CM が受信するため、Wait for Far-End to Send TCS 機能は有効のままにしておく方が適切です。

図 12-6 は、次のコール シナリオを示しています。これらのシナリオでは、Wait for Far-End to Send TCS 機能を無効にしないとコールが失敗します。

- シナリオ 1 : Cisco Unified Video Advantage が、ISDN ネットワークを介してリモート クラスタにある別の Cisco Unified Video Advantage を呼び出す。
- シナリオ 2 : H.323 クライアントが、ISDN ネットワークを介してリモート クラスタにある別の H.323 クライアントを呼び出す。

図 12-6　Wait for Far-End to Send TCS 機能が無効（オフ）のシナリオ

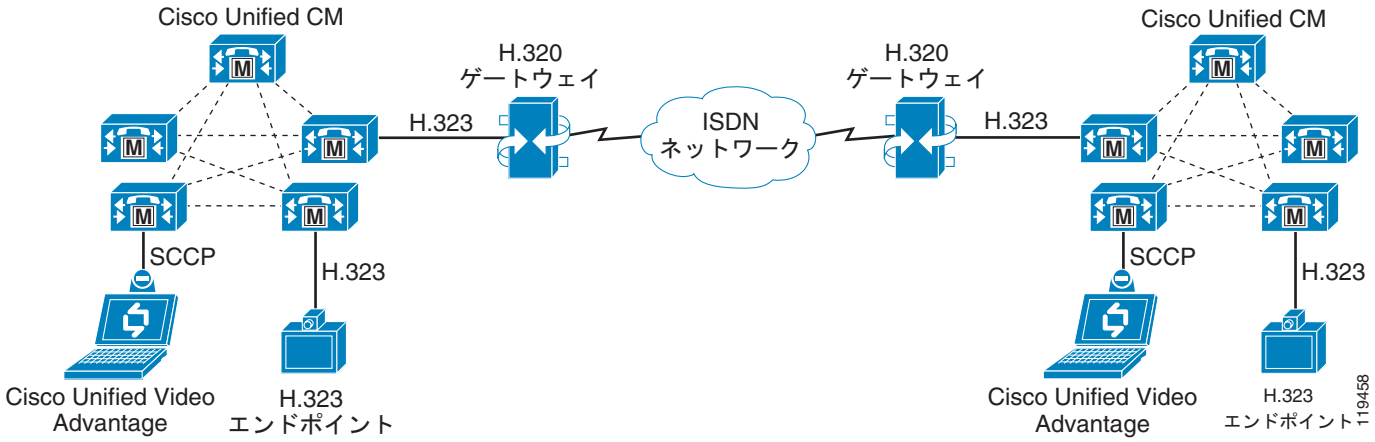


図 12-6 のどちらのシナリオでも、両方の Unified CM がゲートウェイから TCS を受信するまで待機し、両方のゲートウェイも ISDN 側からの TCS を受信するまで待機するため、デッドロックが発生します。コールは数秒後にタイムアウトし、失敗します。ユーザから見ると、発信者にはコールが進行中であることを示すリングバック トーンが聞こえ、着信側には着信コールを示す呼び出し音が聞こえます。着信側がコールに応答しようとすると、デッドロックのために H.245 フェーズが失敗し、コールは両方で切断されて失敗します。

このようなシナリオの問題の回避策としては、Unified CM で H.320 ゲートウェイを表すデバイスで、[Wait for Far-End to Send TCS] オプションを無効（オフ）にすることを推奨します。H.320 ゲートウェイに到達するように Unified CM を設定した方法に応じて、このデバイスは H.225 ゲートキーパー制御トランクまたは H.323 ゲートウェイ デバイスになります。

ただし、[Wait for Far-End to Send TCS] オプションを無効にすると、交換された初期機能がリモート デバイスで機能しなくなることがあります。たとえば、Unified CM リージョンが 768 kbps ビデオに設定されていても、H.320 デバイスが 384 kbps しかサポートしないことがあります。また、選択された音声コーデックがリモート側で機能しないことがあります。この場合、初期ネゴシエートされた論理チャネルを切断し、正しい速度とコーデックで再開する必要があります。多くのレガシー H.323 および H.320 デバイスは、この状態を正しく処理せず、Unified CM が CloseLogicalChannel メッセージを送信して異なる値でチャネルと再ネゴシエートすると、コールを切断します。そのため、[Wait for Far-End to Send TCS] オプションを無効にする場所とタイミングには注意が必要です。

トランク

Cisco Unified CM は、さまざまなタイプのトランクをサポートしています。H.323 エンドポイントの配置が非常に多く、コールをビデオ エンドポイントおよびゲートウェイにルーティングする H.323 ゲートキーパーとの相互作用に使用できるため、H.323 トランクがビデオ配置に最も一般的に使用されています。H.323 トランクには、H.239、H.235 などの H.323 ビデオ ポイントで使用される数多くのビデオ機能のパススルー機能もあります。RASAggregator トランクにより、Unified CM は Cisco IOS ゲートキーパーに登録されているエンドポイントのコールのコール制限および帯域幅拡張などの機能を提供できます。

SIP トランクは、SIP ネットワークとの相互接続を提供できます。これらのトランクは、トランク間でのビデオおよび SRTP をサポートしています。Unified CM は、Cisco TelePresence Video Communication Server（VCS）などのビデオ通信サーバのより緊密な統合を可能にします。この機能により、高解像度のコールのサポートが拡張され、Cisco VCS、Cisco Video デバイス、およびサードパーティ製ビデオ エンドポイントで必要となる高度なシグナリングも Unified CM 経由で動作できるようになります。さらに、Cisco Unified CM SIP トランクは、Media Termination Point（MTP; メディア ターミネーション ポイント）がなくてもビデオ コールのアーリー オファーをサポートします。これが重要となるのは、コールが複数の呼制御サーバを通過する配置、または双方向メディア パスを確立するためのコールのカットスルー時間が重要となる配置の場合です。詳細については、「Cisco Unified CM トランク」（P.14-1）の章を参照してください。

展開方法によっては、ネットワークで DNS SRV を使用する場合があります。DNS SRV を使用する Cisco TelePresence VCS 展開の場合、Unified CM SIP トランクも DNS SRV を使用できます。そのような展開では、DNS サーバのスケーラビリティおよび冗長性を考慮する必要があり、またロード バランシングおよび冗長性の機能は、要求を処理する DNS サーバに依存することにも注意する必要があります。このように、Unified CM トランクのロード バランシングおよび冗長性は、DNS サーバのロード バランシングおよび冗長性に追加されます。

マルチポイント会議

3 者以上が同じビデオ コールに同時に参加するには、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）が必要です。MCU は、次のメイン コンポーネントで構成されています。

- Multipoint Controller（MC）
- Multipoint Processor（MP）

MC は、メディア ネゴシエーション、コール シグナリング、コールに使用する MP の選択など、会議のコール セットアップと切断のすべての面を処理します。MP は、すべての音声パケットおよびビデオ パケットを処理します。MC が MP を制御し、1 つの MC で複数の MP を制御できます。MP は、ソフトウェアベースのものも、ハードウェアベースのものもあります。ソフトウェアベースの MP は、通常、高度なトランスコーディング、レート変換（複数の速度）、構成機能は実行できません。

Cisco MCU では、Skinny Client Control Protocol（SCCP）もサポートされています。これにより、Cisco IOS カンファレンス ブリッジがオーディオ会議に統合できるように、MCU がビデオ カンファレンス ブリッジとして Unified CM に統合可能になります。

Cisco Unified Videoconferencing 製品では、Multipoint Conference Unit（MCU; マルチポイント カンファレンス ユニット）に、Multipoint Controller（MC; マルチポイント コントローラ）機能と Multipoint Processor（MP; マルチポイント プロセッサ）機能が統合デバイスとして組み込まれています。シャーシ ベースの MCU では、ビデオ会議を実行する Enhanced Media Processor（EMP）モジュールを管理および制御する MCU モジュールを使用することによって、柔軟性とスケーラビリティが提供されます。

（注） Cisco 3545 および 5200 MCU には、ソフトウェア ベースの MP が備えられていないため、EMP が必要です。MCU モジュールは、MCU シャーシの EMP を制御するために必要です。

Cisco Unified CM では、SCCP、H.323、および SIP モードで Cisco Unified Videoconferencing MCU がサポートされています。各プロトコルにはさまざまな機能が用意され、さまざまな理由で使用されます。そのため、3 つのプロトコルすべてを実行するように、これらの各 MCU が搭載されています。Cisco Unified Videoconferencing MCU は 3 つすべてのプロトコルを実行し、これら 3 つの間で利用可能な MP リソースの合計数を分割するように設定できます。

シグナリング プロトコルに関係なく、MCU は、音声ストリームとビデオ ストリームを各参加者から受信し、これらのストリームをすべての他の参加者に、組み合せたビューで送信するという同じ基本機能を提供します。マルチポイント テレビ会議のビューには、次の 2 つのタイプがあります。

- Voice-Activated（音声起動）（切り替え）
- Continuous-Presence（連続表示）

Voice-Activated（音声起動）

Voice-Activated 会議は、すべての参加者の音声ストリームとビデオ ストリームを取得し、主要な発言者を決定し、主要な発言者のビデオ ストリームだけをすべての他の参加者に送信します。参加者には、主要な発言者の全画面イメージが表示されます（現在の発言者には、前の主要な発言者が表示されます）。すべての参加者からの音声ストリームが混合され、全員が他の全員の発言を聞くことができますが、ビデオは主要な発言者のものだけが表示されます。

次のいずれかの方法で、主要な発言者を選択できます。

- Voice-Activated モード

  このモードを使用すると、MCU は、最も声が大きく、発言が長い会議参加者を判断して、主要な発言者を自動的に選択します。声の大きさを判断するために、MCU は各参加者の音声信号の強さを計算します。会話中に条件が変わると、MCU は自動的に新しい主要な発言者を選択し、その参

加者が表示されるようにビデオを切り替えます。ホールド タイマーによって、ビデオの頻繁な切り替えが防止されます。主要な発言者になるには、指定された秒数以上発言し、他のすべての参加者よりも際立つ必要があります。

- MCU の Web ベースの会議制御ユーザ インターフェイスによる主要な発言者の手動選択

  会議コントローラ（議長）は MCU の Web ページにログインし、参加者を強調表示することで、その参加者を主要な発言者として選択できます。この処理によって音声アクティビティ検出は無効になり、議長が新しい主要な発言者を選択するか、Voice-Activated モードを再度有効にするまで、主要な発言者は固定されます。

- 参加者リストを自動的に 1 人ずつ循環するように MCU を設定

  この方式を使用すると、MCU は設定された時間だけ各参加者で止まり、リスト上の次の参加者に切り替えます。会議コントローラ（議長）は、Web インターフェイスでこの機能をオンまたはオフにできます（オフにすると、Voice-Activated モードが再度有効になります）。

Continuous-Presence（連続表示）

Continuous-Presence 会議では、一部の参加者またはすべての参加者が合成ビューで同時に表示されます。ビューには 2 ～ 16 の長方形（参加者）をさまざまなレイアウトで表示できます。各レイアウトには、長方形の 1 つを Voice-Activated にする機能があり、合成ビューに表示できる長方形の数よりも参加者の方が多い会議で役立ちます。たとえば、4 画面のビューを使用していて、コールの参加者が 5 人のとき、同時に表示される参加者は 4 人だけです。この場合、長方形の 1 つを Voice-Activated にすると、主要な発言者に応じて参加者 4 と参加者 5 をその長方形で切り替えることができます。他の 3 つの長方形に表示される参加者は固定で、すべての長方形は、会議制御 Web ベース ユーザ インターフェイスで操作できます。

（注）　Continuous-Presence には、Cisco Unified Videoconferencing MCU の Enhanced Media Processor（EMP）が必要です。

MP リソース

どちらのタイプの会議でも、MP リソースによって、MCU がサポートできるビデオ形式、トランスレーティング、およびトランスコーディング機能が決まります。エンドポイントが異なる速度で会議に接続している場合は、レート変換対応 MP が必要です。RM モジュールと EMP モジュールは、どちらも速度間のレート変換に対応しています。レート変換対応 MP が使用できない場合、MCU はすべてのエンドポイントにフローコントロール メッセージを送出し、最も遅いエンドポイントの最大受信レートに合せて転送速度を下げるように指示します。たとえば、3 人の参加者が 384 kbps の会議に接続し、4 番めの参加者が 128 kbps で参加した場合、MCU は他の 3 人の参加者にフローコントロール メッセージを送信し、128 kbps の参加者に合せて転送速度を下げるように指示します。この方式を使用すると、1 人の参加者の性能が低いことで、すべての参加者の品質が低下します。レート変換対応 MP を使用した場合、128 kbps のストリームが 384 kbps に（および、その逆に）変換され、各参加者がそれぞれの接続で許可される最大の品質を使用できます。

Continuous-Presence 会議でも、レート変換対応 MP は非常に重要です。MCU に内蔵されたソフトウェアベースの MP は、すべての入力ストリームを組み合せ、得られた組み合せを各参加者に送信します。たとえば、4 人の参加者が 384 kbps で G.711 音声を使用して Continuous-Presence 会議に接続している場合、各参加者は 320 kbps のビデオと 64 kbps の音声を MCU に転送します。MCU は 4 つの入力ビデオ ストリームを取得し、4 画面の合成ビューに組み合せます。MCU は混在する 64 kbps の音声と共に、1280 kbps のビデオを各エンドポイントに転送します。その結果、エンドポイントごとに合計 1344 kbps になります。この方式は Asynchronous Continuous Presence と呼ばれ、帯域幅要件、コール アドミッション制御メカニズム、一部のデバイスとの相互運用性に悪影響を与えることがあります。

（注）　Asynchronous Continuous Presence は使用しないことを強く推奨します。

RM モジュールまたは EMP モジュールを使用すると、MCU は各入力ストリームを組み合せる前に、合計出力帯域幅が入力帯域幅と一致するようにレート変換できます。たとえば、MCU が 4 画面のレイアウトを使用し、各参加者が 320 kbps のビデオと 64 kbps の音声を MCU に転送する場合、MCU は原則として各入力ストリームを 80 kbps にレート変換し、4 画面のビューが 320 kbps のビデオになるように組み合せ（4 X 80 kbps）、混合された 64 kbps 音声とこのビデオを組み合せて、最終的な組み合せを各参加者に転送します。この方式は、Synchronous Continuous Presence と呼ばれます。すべての Continuous-Presence 会議で、Synchronous Continuous Presence モードを使用することを強く推奨します。ただし、このモードを使用するには、各 MCU にレート変換対応 MP（RM、EMP など）が必要で、MCU のコストが上がります。

（注）　MCU が内蔵された H.323 および SIP クライアントの場合、Unified CM は、H.323 クライアントで別のコールの生成を許可しません。そのため、内蔵 MCU の機能は無効になります。

Ad-Hoc 会議用の MCU リソース

すでに説明したように、Cisco Unified Videoconferencing MCU では、これらのモデルのソフトウェア バージョン 3.2+ および Cisco Unified CM Release 4.0 から SCCP をサポートしています。SCCP モードで設定すると、Unified CM が MC 機能を提供し、MCU が MP 機能を提供します。SCCP MCU は、Unified CM で完全に制御されます。Cisco Unified CM 8.6 以降のリリースは、カンファレンス ブリッジ経由の SIP ベースの TelePresence MCU をサポートします。その結果、より高い解像度をサポートできる Ad-Hoc 会議用の MCU 統合の方法も提供します。

Ad-Hoc MCU リソースを呼び出すのは、次のイベントだけです。

- SCCP エンドポイントまたは SIP エンドポイント（IP Phone やサードパーティ製 SCCP ビデオ エンドポイントなど）のユーザが、[Conf] ソフトキー、[Join] ソフトキー、または [cBarge] ソフトキーを押して Ad-Hoc 会議を呼び出した。
- SCCP エンドポイントまたは SIP エンドポイント（IP Phone やサードパーティ製 SCCP ビデオ エンドポイントなど）のユーザが、[MeetMe] ソフトキーを押して、予約なしの Meet-Me 会議を呼び出した。
- ソフトフォン モードの Cisco Cius または Cisco Unified Personal Communicator のユーザが、参加機能または会議機能を使用して会議に複数のコールを参加させた。

これらのタイプの会議の参加者には、任意のタイプのエンドポイント（サポートされる任意のゲートウェイ タイプを介して Unified CM がサポートする任意のシグナリング プロトコルを使用するビデオ デバイスおよび非ビデオ デバイス）が含まれます。ただし、Ad-Hoc MCU リソースを呼び出せるのは、SCCP エンドポイント、SIP Cisco IP Phone、または Cisco Unified Personal Communicator だけです。つまり、H.323 ビデオ エンドポイントは Ad-Hoc MCU リソースを呼び出せませんが、SCCP ビデオ エンドポイントがリソースを呼び出し、H.323 ビデオ参加者をコールに参加させることはできます。たとえば、SCCP エンドポイントのユーザは、[Conf] ソフトキーを押し、H.323 クライアントのディレクトリ番号をダイヤルして、もう一度 [Conf] ソフトキーを押すと、トランザクションを完了できます。H.323 クライアントは、参加者として SCCP MCU 会議に参加します。

ただし、[Conf]、[Join]、または [cBarge] ソフトキーで開始された Ad-Hoc 会議の場合、他の参加者が使用するシグナリング プロトコルは、保留機能および MCU に音声チャネルとビデオ チャネルを転送する機能をサポートしている必要があります。H.323 デバイス（H.323 クライアント、H.323 ゲートウェイ、H.320 ゲートウェイ、およびすべてのタイプの H.323 トランク）の場合、Unified CM は、H.245 仕様で定義されている Empty Capabilities Set（ECS）方式を使用してこの機能を実現しています。H.323 エンドポイントが Unified CM からの ECS メッセージの受信をサポートしていない場合、切断されるか、クラッシュしてリブートする可能性もあります。この問題の回避策としては、H.323 デバイスで [MTP Required] オプションを有効（オン）にして、MTP デバイスを含まないメディア リソース グループ リスト（MRGL）をこのデバイスに割り当て、Unified CM のサービス パラメータ

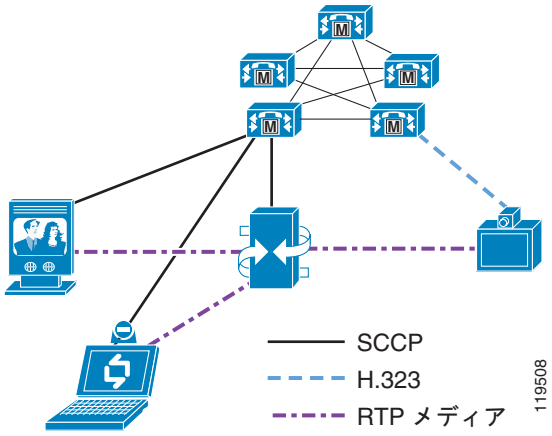
Fail Call if MTP Allocation Fails を **False** に設定します（詳細については、「メディア リソース グループとメディア リソース グループ リスト」（P.12-19）を参照してください）。この設定を行うと、電話機のソフトキーはグレーアウトされます。ユーザはこのエンドポイントで、保留、既存のコールとの会議、既存のコールへの参加、このエンドポイントを含む既存のコールへの割り込みなど、付加サービスを呼び出せなくなります。

（注）　ここで説明した回避策には MTP デバイスを含まない MRGL が必要になるため、RSVP ベースのコール アドミッション制御を使用している場合、この回避策は使用できません。

[MeetMe] ソフトキーによる予約なしの会議の場合は、他のエンドポイントで使用されているシグナリング プロトコルが保留および転送をサポートしている必要はありません。これらのタイプの会議では、各エンドポイントが、会議を開始した SCCP クライアントで割り当てられた [MeetMe] ダイヤルイン番号をダイヤルします。

図 12-7 は、H.323 エンドポイントと Cisco IP Phone を同じ Ad-Hoc 会議に参加させる方法を示します。この例では、SCCP エンドポイントで [Conf] ソフトキーによって会議が開始され、3 人のメンバーが招待されています。

図 12-7　SCCP エンドポイント、SIP エンドポイント、および H.323 エンドポイントの間の Ad-Hoc 会議



Ad-Hoc 会議は、使用されるカンファレンス ブリッジに応じて、Voice-Activated モードと Continuous-Presence をサポートします。

メディア リソース グループとメディア リソース グループ リスト

SCCP または SIP 電話機のユーザが [Conf]、[Join]、または [MeetMe] ソフトキーをアクティブにした場合、Unified CM では、メディア リソース マネージャを使用してカンファレンス ブリッジが選択されます。カンファレンス ブリッジまたは MCU リソースは、Media Resource Group（MRG; メディア リソース グループ）で設定されます。Media Resource Group List（MRGL; メディア リソース グループ リスト）は、優先順位順に並べられた MRG のリストを指定するものであり、エンドポイントと関連付けることができます。メディア リソース マネージャでは、エンドポイントの MRGL を使用して、カンファレンス ブリッジが選択されます。リソースをグループ化する方法は完全に自由ですが、地理的な配置（特定のサイトのすべてのエンドポイントで最も近いカンファレンス ブリッジが使用される

ようにする方法）、またはエンドポイントのタイプ（ビデオ対応エンドポイントがビデオ対応 MCU を使用し、音声だけのエンドポイントは別のカンファレンス ブリッジ リソースを使用するようにする方法）でグループ化することが一般的です。

Cisco Unified CM には、インテリジェント ブリッジ選択機能があります。この機能を使用すると、会議のエンドポイントの能力に基づいて、会議リソースを選択できます。ビデオ会議の起動時に複数のビデオ エンドポイントが存在し、ビデオ会議リソースが使用可能な場合、インテリジェント ブリッジ選択機能は、会議に使用するリソースを選択します。ビデオ会議リソースが 1 つも使用できない場合、またはビデオ会議にビデオ対応エンドポイントが 1 つも存在しない場合、インテリジェント ブリッジ選択機能は、会議で使用可能なオーディオ リソースを選択します。インテリジェント ブリッジ選択機能は、セキュア会議に対しセキュアなカンファレンス ブリッジを選択する付加機能を提供します。ただし、セキュアなカンファレンス ブリッジ接続は、デバイス機能に依存します。Unified CM は、ビデオまたはオーディオ カンファレンス ブリッジの代わりに、セキュアなカンファレンス ブリッジを割り当てることがあります。インテリジェント ブリッジ選択機能の動作は、Unified CM におけるサービス パラメータの設定によって、柔軟に変更できます。

インテリジェント ブリッジ選択機能では、次のタイプのエンドポイントがビデオ対応として扱われます。

- Cisco Unified Video Advantage（IP Phone の PC ポートに接続された PC 上で実行する必要があります）
- Cisco Unified IP Phone 7985G および 9900 シリーズ
- Cisco Unified Personal Communicator または Client Services Framework クライアント
- H.323 クライアント（サードパーティ製ビデオ エンドポイント）
- SIP Advanced エンドポイント（サードパーティ製ビデオ エンドポイント）
- ビデオ コール用メディア ターミネーション ポイント（MTP）のない SIP トランク
- ビデオ コール用 MTP のない H.323 トランク

インテリジェント ブリッジ選択機能は、カンファレンス ブリッジの他の選択方式と比べて、次のような利点があります。

- 会議タイプによるカンファレンス ブリッジ選択：セキュア、ビデオ、または音声会議
- メディア リソース設定の簡素化
- 他のブリッジ選択方式では音声のみの会議に占有されかねない、MCU ビデオ ポートの適正な使用

すべてのカンファレンス ブリッジ リソースおよび MCU を 1 つの MRGL に含めることができます。インテリジェント ブリッジ選択機能では、音声会議だけでよいのか、あるいはビデオ会議を行う必要があるのかに基づいて、カンファレンス ブリッジが選択されます。

Unified CM では、サービス パラメータ設定によって指定可能な、もう 1 つのカンファレンス ブリッジ選択方法がサポートされています。このモードでは、Unified CM において次の基準がここに示した順序で適用されて、使用するカンファレンス ブリッジ リソースが選択されます。

1. メディア リソース グループ リスト（MRGL）にリストされているメディア リソース グループ（MRG）の優先順位
2. 選択された MRG の中で、最も使用されていないリソース

電話機の MRGL の最上位に MCU を配置すると、ビデオ対応の参加者がいない音声だけの会議にも、この MCU が常に選択されます。このシナリオでは、音声のみの会議で MCU リソースが浪費され、ビデオ会議の要求が発生したときに使用できなくなることがあります。

（注）　Meet-Me 会議は、インテリジェント ブリッジ選択機能を使用しません。

インテリジェント ブリッジ選択機能

Cisco Unified CM には、インテリジェント ブリッジ選択機能があります。この機能を使用すると、会議のエンドポイントの能力に基づいて、会議リソースを選択できます。ビデオ会議の起動時に複数のビデオ エンドポイントが存在し、ビデオ会議リソースが使用可能な場合、インテリジェント ブリッジ選択機能は、会議に使用するリソースを選択します。ビデオ会議リソースが 1 つも使用できない場合、またはビデオ会議にビデオ対応エンドポイントが 1 つも存在しない場合、インテリジェント ブリッジ選択機能は、会議で使用可能なオーディオ リソースを選択します。

インテリジェント ブリッジ選択機能は、セキュア会議に対しセキュアなカンファレンス ブリッジを選択する付加機能を提供します。ただし、セキュアなカンファレンス ブリッジ接続は、デバイス機能に依存します。Unified CM は、ビデオまたはオーディオ カンファレンス ブリッジの代わりに、セキュアなカンファレンス ブリッジを割り当てることがあります。インテリジェント ブリッジ選択機能の動作は、サービス パラメータの設定によって、柔軟に変更できます。

インテリジェント ブリッジ選択機能では、次のタイプのエンドポイントがビデオ対応として扱われます。

- Cisco Unified Video Advantage（IP Phone の PC ポートに接続された PC 上で実行する必要があります）
- Cisco Unified IP Phone 7985G
- Cisco Unified Personal Communicator
- H.323 クライアント（サードパーティ製ビデオ エンドポイント）
- SIP Advanced エンドポイント（サードパーティ製ビデオ エンドポイント）
- ビデオ コール用メディア ターミネーション ポイント（MTP）のない SIP トランク
- ビデオ コール用 MTP のない H.323 トランク

インテリジェント ブリッジ選択機能は、カンファレンス ブリッジの他の選択方式と比べて、次のような利点があります。

- 会議タイプによるカンファレンス ブリッジ選択：セキュア、ビデオ、または音声会議
- メディア リソース設定の簡素化
- 他のブリッジ選択方式では音声のみの会議に占有されかねない、MCU ビデオ ポートの適正な使用

（注）　Meet-Me 会議は、インテリジェント ブリッジ選択機能を使用しません。

H.323 および SIP MCU リソース

H.323 または SIP モードで設定すると、MCU は MC 機能を提供し、Unified CM への H.323 または SIP ピアのように動作します。H.323 および SIP MCU 会議は多くの方法で呼び出せますが、それらの方法は主に次の 2 つのカテゴリに分類できます。

- スケジュール済み
- 予約なし

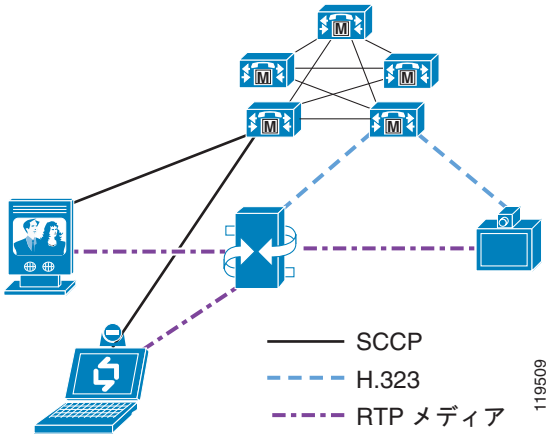
スケジュール済みの会議は、コールの前に、スケジューリング アプリケーションを使用して MCU リソースを予約します。スケジューリング機能は、通常、Cisco Unified MeetingPlace や Cisco Unified Video Conferencing Manager などの Web ベースのユーザ インターフェイスで提供されます。スケジューリング アプリケーションは、通常、会議の日付と時刻、会議用に予約されているポートの数、ダイヤルイン情報をユーザに提供する招待情報を生成します。または、会議の開始時に参加者の一部、またはすべてにダイヤル アウトするようにスケジューリング システムを設定できます。

予約なしの会議の場合、MCU には、オンデマンドで使用できる一定の数のリソースがあります。会議を作成するため、ユーザはいつでも MCU にダイヤルインするだけで済みます。そのユーザが最初にダイヤルした参加者である場合、MCU は、サービス テンプレートで定義された設定を使用して、動的に新しい会議を作成します（サービス テンプレートの詳細については、「サービス テンプレートとプレフィックス」（P.12-22）を参照してください）。同じ会議番号にダイヤルインした後続のユーザは、この会議に参加します。

スケジュール済みまたは予約なしの H.323 または SIP 会議の作成と参加は、任意のタイプのエンドポイントで実行できます。たとえば、SCCP エンドポイントが H.323 MCU にダイヤルインして、H.323 エンドポイントと同様に予約なしの会議を作成できます。

図 12-8 は、H.323 エンドポイントと SCCP エンドポイントを同じ H.323 会議に参加させる方法を示しています。この例では、H.323 MCU にダイヤルインして新しい予約なしの会議を作成した SCCP エンドポイントによって会議が開始され、他の 2 人の参加者が、後で会議にダイヤルインしています。

図 12-8　予約なしの会議の SCCP および H.323 エンドポイント



H.323 および SIP 会議は、Voice-Activated モードと Continuous-Presence モードの両方をサポートします。さらに、H.323 会議は、MCU に内蔵されたソフトウェアベースの MP、Rate Matching（RM）モジュール、および Enhanced Media Processor（EMP）モジュールなど、すべての MP タイプをサポートします。

サービス テンプレートとプレフィックス

MCU のサービスは、各会議に関係する設定を定義します。異なるタイプの会議に、異なるサービスを定義できます。各サービスは、少なくとも、次の設定を定義します。

- 会議の速度（ビデオ ビット レート）

  レート変換対応 MP を使用している場合、この設定に複数の速度が含まれることがあります。

- 参加者の最小数および最大数

  最小数は、会議の開始時に予約されるポートの数を定義します。最大数は、MCU がこの会議への参加を許可する参加者の最大数を定義します。

- ビデオ コーデック タイプ（H.261、H.263、または H.264）
- フレーム レート（15 または 30 fps）
- 解像度（QCIF または CIF）
- MP リソース（Auto、MP、RM、または EMP）

- 表示するビデオ レイアウト（Voice-Activated または Continuous-Presence）

  会議には複数のレイアウトを含めることができ、会議の参加者数が増減したときに変化する動的レイアウトもあります。

- H.323 と SIP、または SCCP

  [SCCP service] チェックボックスが有効（オン）の場合、サービスは SCCP 会議で使用されます。このボックスが無効（オフ）の場合、サービスは H.323 および SIP 会議で使用されます。

H.323 および SIP サービスでは、特定のサービスに到達するために、エンドポイントがダイヤルするサービス プレフィックスに各サービスが割り当てられます。サービス プレフィックスは会議番号の前半の番号を形成し、後半の番号で会議 ID を定義します。この形式によって、同じサービス プレフィックスで複数の会議を同時に実行できます。たとえば、サービス プレフィックスを 555 にして、会議の完全なダイヤル文字列を 7 桁にできます。この方式では、4 桁の会議 ID を使用でき、会議番号は 5550000 ～ 5559999 の範囲になります。ユーザは、会議にアクセスするために全文字列をダイヤルする必要があります。コールを受信すると、MCU はダイヤルされた番号を解析し、サービス プレフィックスとの照合を試行します。ダイヤルされたサービス プレフィックスを判断すると、MCU は残りの番号を会議 ID として使用します。会議 ID がまだ存在しない場合、MCU は、その ID で新しい予約なしの会議を作成します。会議がすでに存在する場合は、その会議にユーザが追加されます。

MCU で H.323 と SIP の両方を同時に有効にする場合は、両方のプロトコルでダイヤル プランを同じにする必要があります。H.323 と SIP の間には、SCCP との間にあるような区別がありません。会議が SIP で作成された場合、MCU はこの会議を H.323 を介して登録します。ゲートキーパーまたは SIP プロキシが登録を拒否した場合、会議は失敗します。

SCCP サービスでもサービス プレフィックスを定義する必要がありますが、ユーザは SCCP サービスに「ダイヤル」インしないため、番号自体に意味はありません。プレフィックスは、Unified CM と SCCP MCU リソースとの間の SCCP 登録メッセージでのみ使用されます。ユーザは、Conf、Join、または [cBarge] ソフトキーを使用して SCCP MCU 会議にアクセスするか（Ad-Hoc）、Unified CM で割り当てられた MeetMe 番号をダイヤルして会議に参加します（予約なし）。そのため、SCCP サービス プレフィックスに指定した番号は関係ありません。999999 など、任意の番号を自由に指定できます。このプレフィックスは、MCU と Unified CM との間の SCCP シグナリングの外側には公開されません（つまり、ダイヤルすることも、ゲートキーパーへの MCU の登録に含むこともできません）。

（注） Cisco MeetingPlace Express メディア サーバでは、SCCP がサポートされています。この統合を使用すると、Cisco Unified Videoconferencing MCU と同様に、Cisco MeetingPlace Express メディア サーバで Unified CM に Ad-Hoc カンファレンス ブリッジを提供できます。

MCU のサイジング

MCU がサポートできる会議のタイプと数の決定には、複数の要因が関与します。サイジングに関連するこれらの要因は、MCU のモデルによって異なります。また、MCU では、デスクトップ会議モードを使用する場合、High Definition（HD; 高品位）モードと比較してより多くのポートを使用できます。

MCU のサイズ計算は、次の要素で決まります。

- ビデオ会議の解像度のタイプ
- MCU がサポートできる合計ポート数
- MCU が各プロトコル専用に割り当てることができるポート数
- MCU 間または EMP カード間でカスケード化された会議が必要かどうか

（注）　1 つの SCCP 会議が複数の EMP にまたがることはできません。各 SCCP 会議は、最大 24 人の参加者をサポートします。

サポートされるポート数に関する特定の情報については、Cisco.com で入手可能な MCU ハードウェアの製品マニュアルを参照してください。可能なバリエーションの数は無限に近いため、具体的な設計ガイダンスをこのマニュアルで示すことは非常に困難です。多くのお客様では、最終的に、SCCP Ad-Hoc 会議、H.323 および SIP の予約なしの会議、および H.323 および SIP のスケジュール済み会議が混在することになります。MCU は、正しい速度とビデオ レイアウトでこれらのすべてのタイプの会議に対応できるサイズにする必要があります。言うまでもなく、この判断はとても複雑です。特定の環境での MCU のサイジングにあたっては、代理店にご相談ください。

ダイヤルイン会議の IVR

ダイヤルイン会議は、通常、Interactive Voice Response（IVR; 音声自動応答装置）システムを使用して、参加する会議の会議 ID とパスワード（設定されている場合）の入力をユーザに求めます。次のタイプの IVR と Cisco Unified Videoconferencing 3500 シリーズ MCU を使用できます。

- MCU に内蔵された IVR
- Cisco Unified IP IVR

MCU の内蔵 IVR には、次の特性があります。

- 会議の作成または会議 ID での参加のプロンプトを再生できる。
- 会議のパスワードのプロンプトを再生できる。
- インバンドとアウトオブバンド（H.245 英数字）の両方の DTMF をサポートする。
- より柔軟性の高いメニューまたは機能を提供するようにカスタマイズできない。

  カスタマイズできるのは、ユーザに対して再生される録音済み音声ファイルだけです。

ダイヤルイン番号を 1 つにして、会議 ID を入力するようにユーザに求めるには、Cisco Unified IP IVR と MCU を組み合せて使用します。

Cisco Unified IP IVR には、次の特性があります。

- （特に）会議 ID とパスワードのプロンプトを再生できる。
- アウトオブバンド DTMF だけをサポートする。

  つまり、発信側デバイスはアウトオブバンド DTMF 方式（H.323 デバイスの H.245 英数字など）をサポートしている必要があります。これらのアウトオブバンド DTMF メッセージは、次に、Unified CM によって Cisco IP IVR サーバにリレーされます。発信側デバイスがインバンド DTMF トーンだけをサポートしている場合、Cisco IP IVR サーバが発信側デバイスを認識しないため、そのデバイスは会議に参加できません。
- 高いカスタマイズ性があり、より柔軟性の高いメニューおよび他の高度な機能を提供できる。

  カスタマイズには、ユーザの会議への参加を許可する前にユーザのアカウントをバックエンド データベースで検証すること、議長が参加するまで参加者をキューに入れることなどが含まれます。

（注）　Cisco Unified IP IVR はアウトオブバンド シグナリングのみをサポートするため、インバンド DTMF トーンを使用する H.323 エンドポイントでは機能しません。

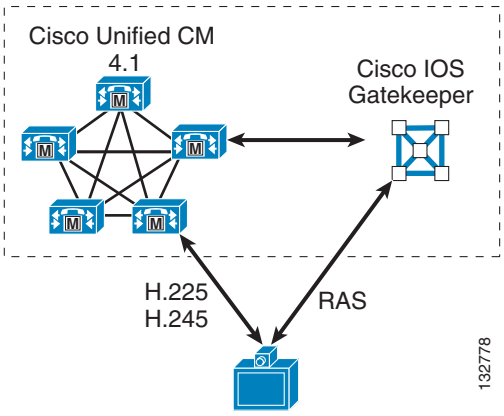
Cisco Unified IP IVR を使用する場合、ユーザは、MCU に直接ルーティングするルート パターンをダイヤルする代わりに、コールを Cisco Unified IP IVR サーバにルーティングする CTI ルート ポイントをダイヤルします。会議 ID の DTMF ディジットを収集した後、Cisco Unified IP IVR は、MCU にコールをルーティングするルート パターンにコールをルーティングします。この転送操作では、発信側デバイスがメディア チャネルの終了と新しい宛先への再開をサポートしている必要があります。たとえば、Cisco Unified IP IVR を呼び出す H.323 ビデオ デバイスは、最初に Cisco Unified IP IVR サーバへの音声チャネルをネゴシエートします。次に、適切な DTMF ディジットが入力された後、MCU に転送します。この時点で Unified CM が、エンドポイントと Cisco Unified IP IVR サーバとの間の音声チャネルを終了し、エンドポイントと MCU の間で新しい論理チャネルを開く Empty Capabilities Set（ECS）プロシージャを呼び出します。このプロシージャについては、この章ですでに説明しています。H.323 ビデオ エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、コールが切断されるか、最悪の場合、クラッシュしてリブートします。

ゲートキーパー

Unified CM にビデオ サポートが導入されるまで、H.323 ビデオ会議ネットワークは、デバイス登録管理、コール ルーティング、および帯域幅制御を実行するゲートキーパーに依存していました。以前は Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper が、これらの機能を提供します。ただし、シスコ製品を含むほとんどのゲートキーパーは、一般的なエンタープライズクラスの PBX で期待される機能と比較して、基本的なコール ルーティング機能だけを提供します。H.323 ビデオ コールのルーティングに使用する場合、Unified CM が基本的なゲートキーパー機能を補足し、完全なエンタープライズクラスの PBX 機能を H.323 ビデオ コールに提供します。

Unified CM とゲートキーパーはチームとして機能し、H.323 ビデオ エンドポイントを管理します。ゲートキーパーがすべての Registration, Admission, and Status（RAS）シグナリングを処理し、Unified CM がすべての H.225 コール シグナリングと H.245 メディア ネゴシエーションを処理します。そのため、図 12-9 で示すように、ネットワークの H.323 エンドポイントに RAS シグナリング プロシージャが必要な場合は、ゲートキーパーと Unified CM サーバを同時に配置する必要があります。

図 12-9　H.323 エンドポイントに RAS シグナリングを提供する Unified CM と Cisco IOS Gatekeeper



次のいずれかの条件が該当する場合、RAS シグナリングが常に必要になります。

- エンドポイントが固定 IP アドレスを使用しない。

  エンドポイントが静的 IP アドレスを使用する場合、Unified CM は、エンドポイントを探すために RAS プロシージャを必要としません。エンドポイントは静的 IP アドレスを使用して Unified CM Administration でプロビジョニングされ、この H.323 クライアントのディレクトリ番号へのコール

は、直接静的 IP アドレスにルーティングされます。エンドポイントが静的 IP アドレスを使用しない場合、Unified CM はこのエンドポイントにコールをルーティングするたびに、ゲートキーパーに照会してエンドポイントの現在の IP アドレスを取得する必要があります。

- E.164 アドレスへのコール発信のために、エンドポイントで RAS プロシージャを必要とする。

  ほとんどの H.323 ビデオ会議エンドポイントは、IP アドレスでダイヤルする場合に限り、別のエンドポイントに直接ダイヤルできます（ユーザが宛先エンドポイントの IP アドレスをドット付き 10 進表記で入力し、コール ボタンを押す）。ただし、ユーザが E.164 形式の番号（IP アドレスのドット付き 10 進表記ではない数値）または H.323-ID（*ユーザ名*または*ユーザ名@ ドメイン*の形式）をダイヤルする場合、ほとんどのエンドポイントは、現在、これらの宛先タイプを解決する方法としてゲートキーパーへの RAS 照会だけを提供します。ただし、E.164 アドレスへのコールが RAS プロシージャをスキップし、H.225 SETUP メッセージを指定された IP アドレスに直接送信するように設定できるエンドポイントの数が増えています。この操作方式は、ピアツーピア モードと呼ばれます。このモードを使用する例としては Tandberg 社製 H.323 エンドポイントがあり、登録するゲートキーパー アドレスを設定することも、使用する Unified CM サーバの IP アドレスを設定することもできます。後者の場合、エンドポイントはすべてのコールを指定された IP アドレスに直接送信し、ゲートキーパーの RAS プロシージャを必要としません。

H.323 ビデオ エンドポイントの RAS プロシージャの管理に加え、ゲートキーパーは、大規模なマルチサイト分散コール処理環境でのダイヤル プラン解決および Unified CM クラスタ間の帯域幅制限の管理において、重要な役割を果たしています。ゲートキーパーは、組織内の多数の H.323 VoIP ゲートウェイを統合できます。また、エンタープライズ IP Telephony ネットワークとサービス プロバイダー VoIP 転送ネットワークの間でセッション ボーダー コントローラとして機能します。

そのため、Cisco IP Video Telephony 配置に関しては、Cisco IOS Gatekeeper は次の役割の一方または両方を実行できます。

- エンドポイント ゲートキーパー

  エンドポイント ゲートキーパーは、H.323 クライアント、MCU、および H.320 ビデオ ゲートウェイを宛先または発信元とするコール、およびこれら相互間のコールのすべての RAS プロシージャを管理するように設定されます。エンドポイント ゲートキーパーは、Unified CM がすべての H.225 コール ルーティングおよび H.245 メディア ネゴシエーションを実行できるように、これらのすべてのコールを適切な Unified CM クラスタに転送します。

- インフラストラクチャ ゲートキーパー

  インフラストラクチャ ゲートキーパーは、Unified CM クラスタ間、Unified CM クラスタと H.323 VoIP ゲートウェイのネットワーク間、および Unified CM クラスタとサービス プロバイダーの H.323 VoIP 転送ネットワーク間のすべてのダイヤル プラン解決および帯域幅制限（コール アドミッション制御）を管理するように設定されます。

以前の Cisco Unified CM リリースでは、エンドポイント ゲートキーパーとインフラストラクチャ ゲートキーパーは別々のルータで実行する必要があり、各エンドポイント ゲートキーパーは単一の Unified CM クラスタだけにサービスを提供できました。企業内に複数の Unified CM クラスタがある場合は、Cisco Unified CM クラスタごとに、個別のエンドポイント ゲートキーパーを配置する必要がありました。現在のリリースの Cisco Unified CM では、これらの役割を単一のゲートキーパーに組み合せて、1 つ以上の Unified CM クラスタのエンドポイント ゲートキーパーとして使用しながら、クラスタ間またはクラスタと他の H.323 VoIP ネットワーク間のコールを管理するインフラストラクチャ ゲートキーパーとして使用できます。ただし、（特に）次の理由により、これらの役割は複数のゲートキーパーに分割することを推奨します。

- スケーラビリティ

  配置する Cisco IOS ルータ プラットフォーム、および煩雑時のコール量の概算によっては、負荷を処理するゲートキーパーが複数必要になることがあります。

- 地理的な復元性

  1 台のゲートキーパーでネットワーク全体をカバーすることは、大規模な国際 VoIP ネットワークにおいて、賢明な方法ではありません。複数のゲートキーパーをネットワーク全体に（一般的には地理的に）分散して配置すると、1 つのゲートキーパーが故障した場合に、より適切に障害を切り分けることができます。

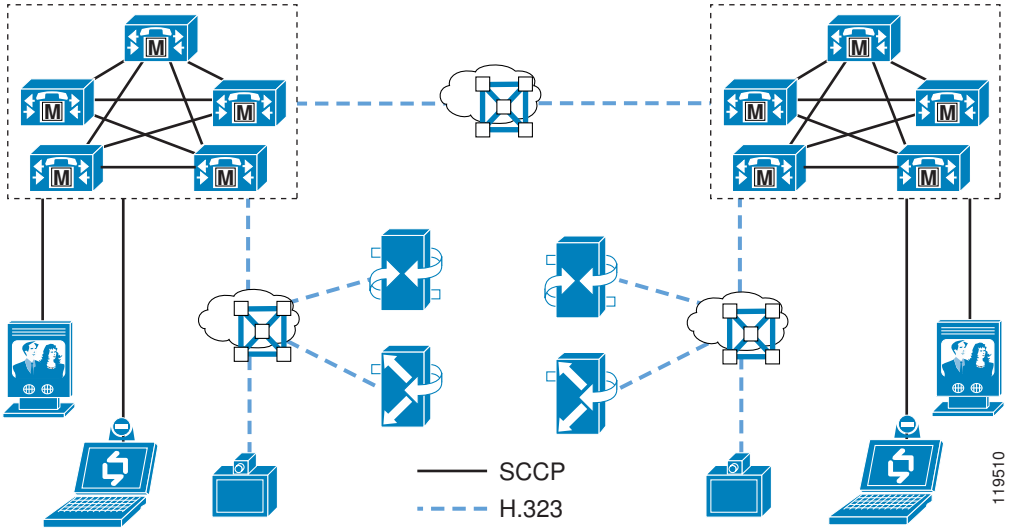
- 非互換性

  ゲートキーパーの設定の中には、グローバルな性質（そのゲートキーパーに登録されているすべてのエンドポイントに関連する性質）を持つものがあります。たとえば、コマンド **arq reject-unknown-prefix** は、一部の H.323 VoIP 転送環境では便利ですが、Unified CM へのコールをルーティングするエンドポイント ゲートキーパーで使用される **gw-type-prefix** < *プレフィックス*> **default-technology** コマンドと競合します。Cisco IOS では両方のコマンドを同じゲートキーパーで設定することは禁止されていませんが、**arq reject-unknown-prefix** コマンドが優先されるため、不明な番号へのコールは Unified CM にルーティングされず、拒否されます。この場合は、H.323 VoIP 転送ネットワーク用に 1 つのゲートキーパーを使用し、別のゲートキーパーを Unified CM クラスタに使用します。

  非互換性のもう 1 つの例は、冗長性のためにゲートキーパーを設定する際に発生することがあります。Cisco Voice Gateways や Unified CM など、ほとんどの Cisco H.323 音声デバイスは、Gatekeeper Update Protocol（GUP）を使用して相互に同期するゲートキーパー クラスタとしてゲートキーパーを設定可能な H.323v3 Alternate Gatekeeper 機能をサポートします。ただし、多くの H.323 ビデオ エンドポイントは Alternate Gatekeeper をサポートしないため、冗長性のために Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルータ プロトコル）を使用するようにゲートキーパーを設定する必要があります。これらの 2 つの冗長性方式を同じゲートキーパーに混在させ、組み合せることはできません。この場合、Alternate Gatekeeper をサポートするエンドポイント用にゲートキーパー クラスタを使用するか、サポートしないエンドポイント用にゲートキーパーの HSRP ペアを使用するかを決定します。

図 12-10 は、2 つの Unified CM クラスタがあるネットワーク シナリオを示しています。各クラスタは、SCCP クライアント、H.323 クライアント、H.323 MCU、および H.320 ゲートウェイで構成されています。H.323 クライアント、MCU、および H.320 ゲートウェイの RAS 部分を管理するために、エンドポイント ゲートキーパーを各クラスタに配置します。別のインフラストラクチャ ゲートキーパーが、クラスタ間のダイヤル プラン解決と帯域幅を管理します。この図ではゲートキーパーの冗長性は示されていませんが、これらの各ゲートキーパーは、実際には Alternate Gatekeeper または HSRP ベースの冗長性を持つように設定された複数のゲートキーパーです。

図 12-10　2 つの Unified CM クラスタと必要なゲートキーパー



エンドポイント ゲートキーパー

次の条件の両方が該当する場合は、エンドポイント ゲートキーパーが必要です。

- クラスタに H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ（集合的に H.323 エンドポイントと呼ぶ）が含まれている。これらのタイプのエンドポイントが存在しない場合（たとえば、すべてのクライアントが SCCP エンドポイントで、MCU も H.320 ゲートウェイもない場合）、エンドポイント ゲートキーパーは不要です。
- 次の条件のいずれかに当てはまる。
  - E.164 アドレスへのコール発信のために、H.323 エンドポイントで RAS プロシージャを必要とする。すでに述べたように、ピアツーピア コール シグナリングに対応するデバイスが増えています。これらのデバイスは、ゲートキーパーに登録する必要はありません。
  - H.323 エンドポイントが静的 IP アドレスを使用しない。

エンドポイント ゲートキーパーの役割は、これらの H.323 エンドポイントを登録する場所を提供し、エンドポイントとの通信の RAS 部分を処理するだけです。エンドポイント ゲートキーパーは、これらのエンドポイントが宛先または発信元となるコール、またはこれらのエンドポイント間のすべてのコール要求に対応して、Unified CM がすべてのコール ルーティング機能および帯域幅制御機能を実行できるように、コールを適切な Unified CM サーバに転送します。このコール ルーティング制御および帯域幅制御を実現するには、H.323 トランクをゲートキーパーに登録するように Unified CM を設定し、ゾーンへのコール、ゾーンからのコール、またはゾーン内のコールをすべてこれらのトランクにルーティングするようにゲートキーパーを設定します。

Cisco Unified CM では、RASAggregator トランクという H.323 トランクを使用してエンドポイント ゲートキーパーに登録する必要があります。このタイプのトランクは、すべての H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ ゾーンに使用されます。一方、ゲートキーパー制御クラスタ間トランクおよびゲートキーパー制御 H.225 トランクは、インフラストラクチャ ゲートキーパーとの統合に使用されます。

H.323 クライアントのプロビジョニング

H.323 クライアントは、他の電話機とほぼ同じ方法でプロビジョニングされます。新しい電話機（モデル タイプ = H.323 Client）を作成し、ディレクトリ番号を割り当て、コーリング サーチ スペース、デバイス プールなどを割り当てます。Unified CM で H.323 クライアントは、次のいずれかの方法で設定します。使用する方法は、クライアントが静的 IP アドレスを使用するかどうか、クライアントで E.164 アドレスをダイヤルする RAS プロシージャが必要かどうかによって異なります。

- ゲートキーパー制御

  このタイプの設定は、静的 IP アドレスが割り当てられていないクライアント（DHCP 割り当てアドレスを使用するクライアント）で、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。これらのクライアントとの通信には、RASAggregator トランクを使用します（図 12-11 および図 12-12 を参照）。

- 非ゲートキーパー制御、非同期

  このタイプの設定は、静的 IP アドレスが割り当てられているクライアントで、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。Unified CM はゲートキーパーを必要とせずに直接シグナルを送信して IP アドレスを解決できますが、クライアントは Unified CM に直接シグナルを送信できず、ダイヤルしようとしている E.164 アドレスを解決するためにゲートキーパーに照会する必要があります（非同期通信）。このタイプのクライアントをサポートするには、実際にはすべてのクライアントが静的 IP アドレスを使用していても、ゲートキーパーのゾーンごとに 1 つ以上のゲートキーパー制御クライアントを Unified CM で定義する必要があります。この場合、非ゲートキーパー制御クライアントは、実際には存在しない「ダミー」クライアントになります。定義する目的は、ゲートキーパーがクライアントから Unified CM へのコールをルーティングできるように、RASAggregator トランクを作成することだけです（図 12-13 および図 12-14 を参照）。

- 非ゲートキーパー制御、同期

  このタイプの設定は、クライアントが静的 IP アドレスを持ち、ピアツーピア シグナリングに対応している（E.164 番号をダイヤルする RAS プロシージャが必要ない）場合に使用します。Unified CM は直接シグナルを送信でき、クライアントは Unified CM に直接シグナルを送信できます（同期通信）。このタイプのクライアントには、ゲートキーパーまたは RASAggregator トランクが不要です（図 12-15 および図 12-16 を参照）。

図 12-11 から図 12-16 は、これら 3 つのシナリオで使用されるコール シグナリング フローを示しています。

図 12-11　Unified CM からゲートキーパー制御クライアントへのコール

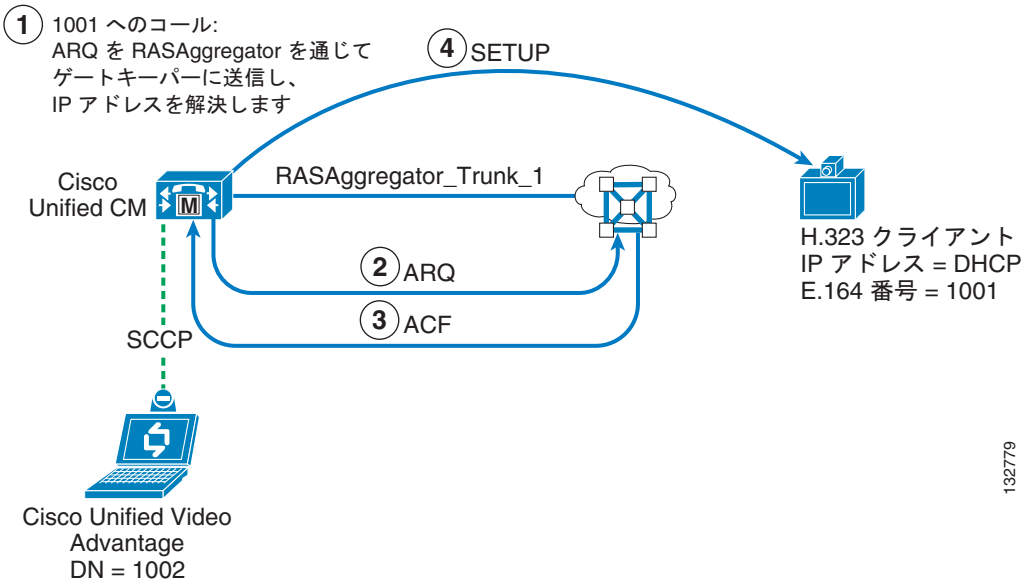


図 12-12　ゲートキーパー制御クライアントから Unified CM へのコール

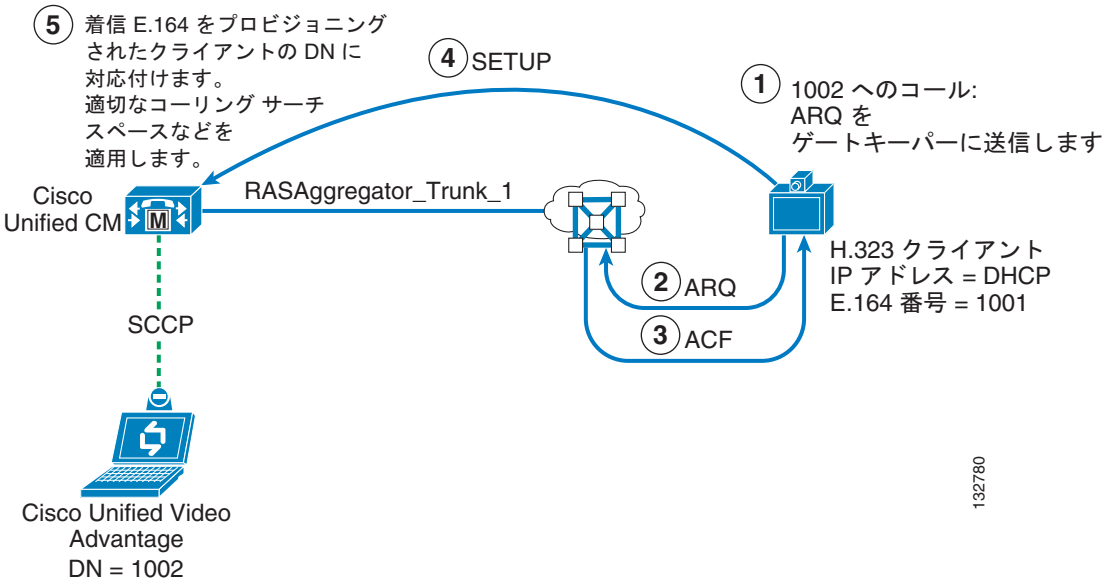


図 12-13　Unified CM から非ゲートキーパー制御クライアントへのコール（非同期）

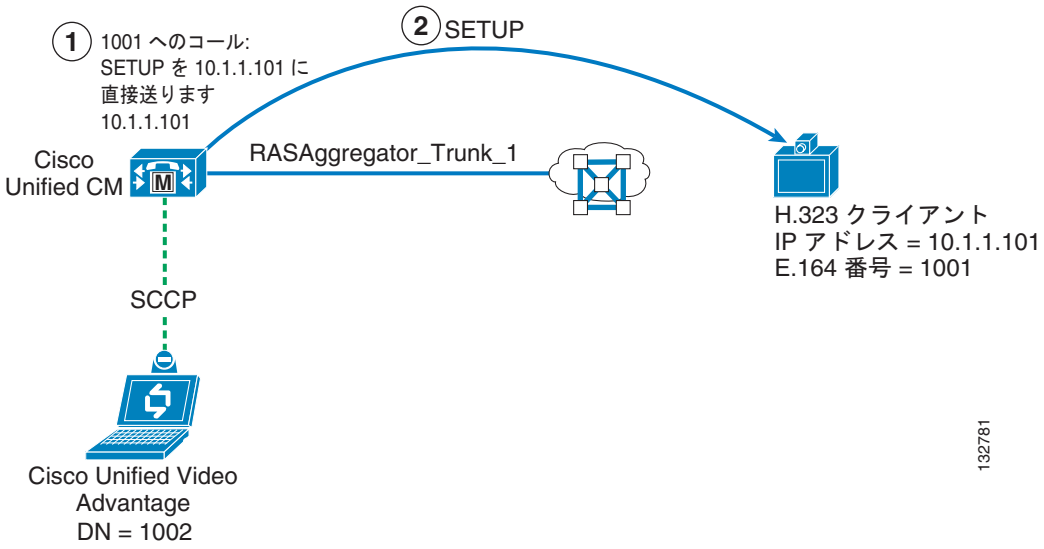


図 12-14　非ゲートキーパー制御クライアントから Unified CM へのコール（非同期）

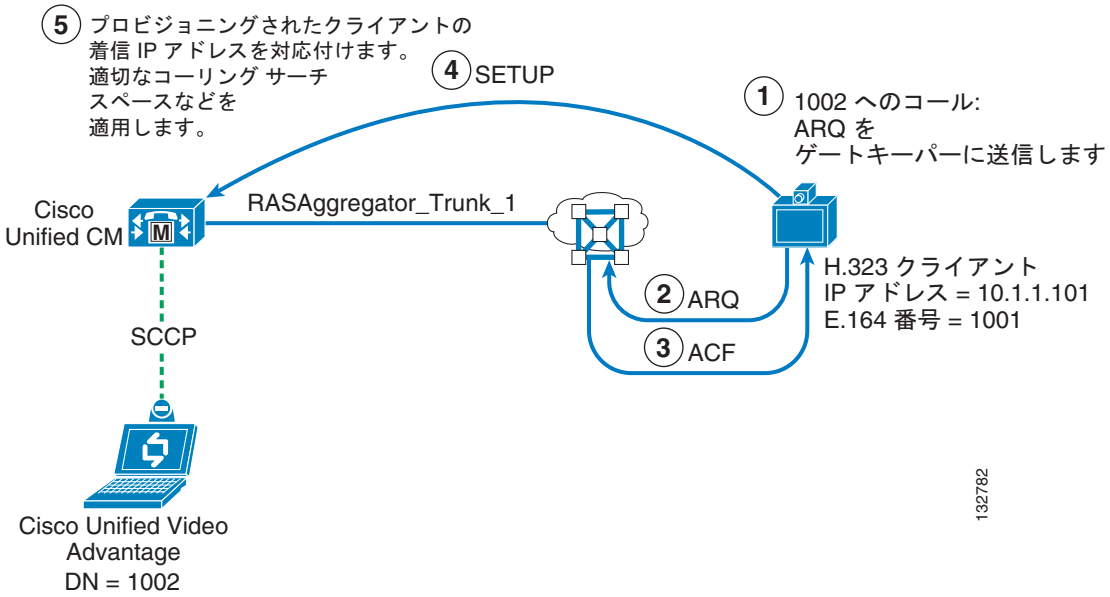


図 12-15　Unified CM から非ゲートキーパー制御クライアントへのコール（同期）

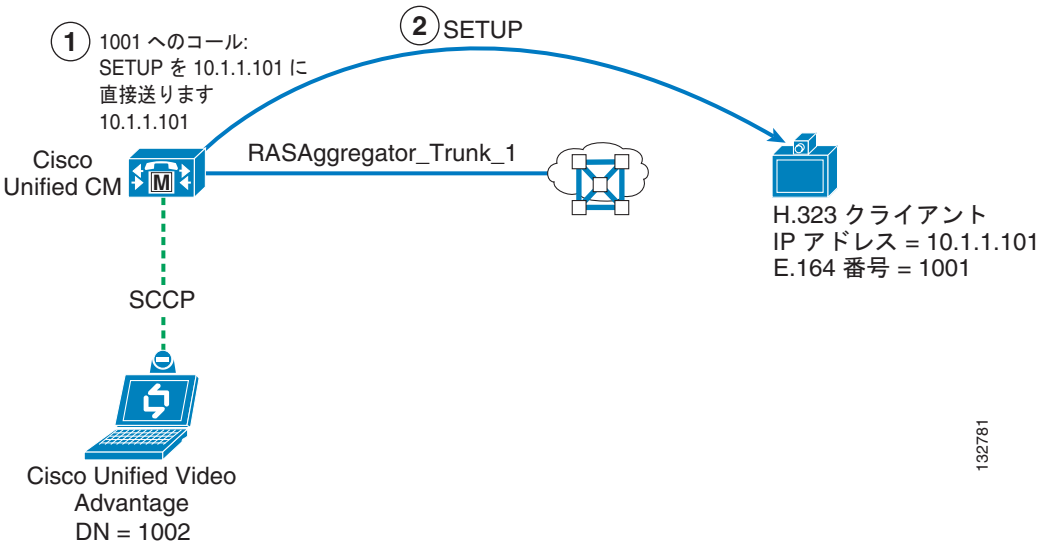
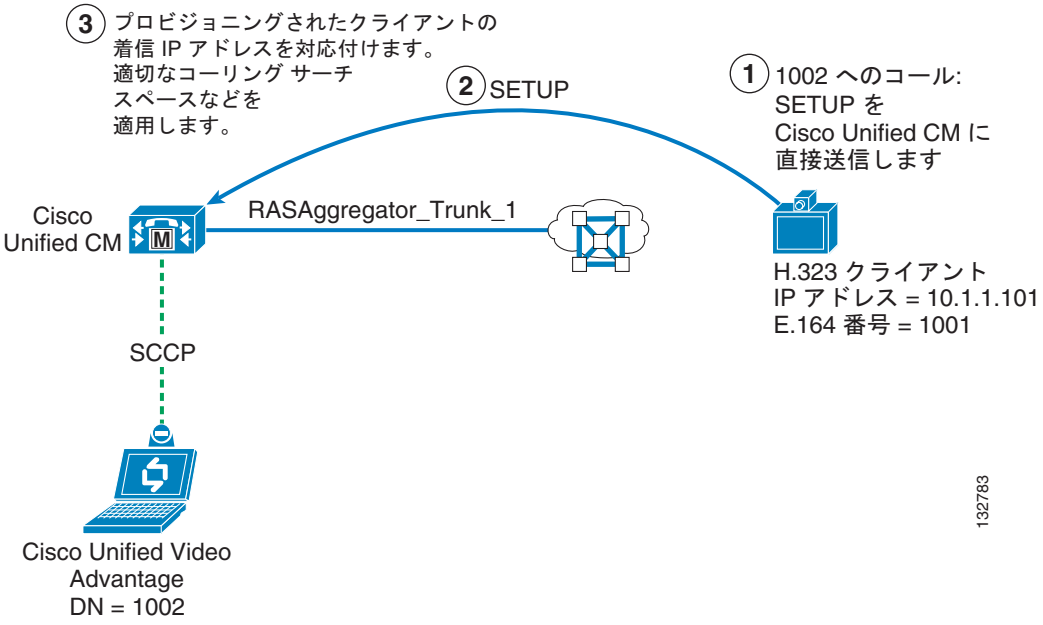


図 12-16　非ゲートキーパー制御クライアントから Unified CM へのコール（同期）



ゲートキーパー制御クライアント

H.323 クライアントをゲートキーパー制御として設定するときは、任意の英数字文字列（わかりやすい名前など）を [Device Name] フィールドに入力し、[Gatekeeper-controlled] ボックスをオンにして、次のフィールドに入力します。

- [Device Pool]

  クライアントで使用するデバイス プール。同じゾーンに登録されているすべての H.323 クライアント（ゲートキーパー制御と非ゲートキーパー制御の両方）が、同じデバイス プールを使用する必要があります。間違ってエンドポイントの間で異なるデバイス プールが割り当てられた場合、Unified CM は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じテクノロジー プレフィックスを使用する必要があります。間違ってエンドポイントの間で異なるテクノロジー プレフィックスが割り当てられた場合、Unified CM は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。このプレフィックスには **1#** を使用することを推奨します。

- [Zone Name]

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じゾーン名を使用する必要があります。間違ってエンドポイントの間で異なるゾーン名（このフィールドは大文字と小文字が区別されます）が割り当てられた場合、Unified CM は複数の RASAggregator トランクをゲートキーパーに登録しようとし（ただし、ゾーン名が不正なトランクは登録に失敗します）、着信コールが間違った RASAggregator トランクに転送されても、Unified CM で拒否されます。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。それによりゲートキーパーは、クライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できます。

非ゲートキーパー制御クライアント

H.323 クライアントを非ゲートキーパー制御としてプロビジョニングする場合は、クライアントの静的 IP アドレスを [Device Name] フィールドに入力し、[Gatekeeper-controlled] セクションの下のその他のすべての設定をブランク（オフ）のままにします。コールがこのディレクトリ番号にルーティングされると、Unified CM は静的 IP アドレスを使用してクライアントに転送します。

クライアントがピアツーピア モードを使用するように設定されている場合、これ以上の設定は不要です。クライアントで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- [Device Name]

  クライアント ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- [Device Pool]

  非ゲートキーパー制御 H.323 クライアントを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、実際のクライアントに割り当てられたデバイス プールと異なる場合、実際のクライアントからの着信コールが Unified CM で拒否されることがあります。

- [Gatekeeper]

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Unified CM でゲートキーパーを定義する必要があります。

- [Technology Prefix]

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することを推奨します。

- [Zone Name]

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。

また、Unified CM サービス パラメータの [Send Product ID and Version ID] を [True] に設定する必要があります。このパラメータによって、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。それによりゲートキーパーは、クライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できます。

H.323 MCU のプロビジョニング

H.323 MCU は、Unified CM で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、MCU の静的 IP アドレスおよび TCP シグナリング ポートを [Device Name] フィールドに入力する必要があります。コールが MCU に関連付けられたルート パターンと一致すると、Unified CM は静的 IP アドレスと TCP ポートを使用して、MCU に到達します。

（注） Cisco Unified Videoconferencing 3500 および 5000 シリーズ MCU は、デフォルトでは TCP ポート 1720 を監視しません（Cisco Unified Videoconferencing 3500 および 5000 シリーズ MCU は、デフォルトでポート 2720 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Unified CM でプロビジョニングする必要があります。

MCU がピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です（Cisco Unified Videoconferencing MCU は、現在、ピアツーピア モードをサポートしていませんが、一部のサードパーティ製 MCU がサポートしています）。MCU で E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、「非ゲートキーパー

制御クライアント」（P.12-33）に説明した [Device Name]、[Device Pool]、[Gatekeeper]、[Technology Prefix]、および [Zone Name] の各フィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

MCU サービス プレフィックス

H.323 MCU は、実行中の予約なしまたはスケジュール済みの H.323 会議に到達するダイヤルイン番号として、E.164 アドレスまたはテクノロジー プレフィックス（MCU ではサービス プレフィックスとも呼ばれる）を使用できます。MCU 管理画面で [MCU Mode] を [Gateway] ではなく [MCU] に設定して、E.164 アドレスを使用するように MCU を設定することを推奨します。使用している MCU のモデルで [MCU] 設定を使用できない場合は、次の特別な設定を使用して、他の H.323 エンドポイントから MCU に発信されたコールを適切にルーティングします。

MCU が [Gateway] モードに設定されている場合、または、別のベンダーの MCU で、（何らかの理由で）会議 ID を E.164 アドレスではなくテクノロジー プレフィックスとして登録する必要がある場合は、MCU のサービス プレフィックスの先頭を # 文字にする必要があります。たとえば、MCU サービス プレフィックスが 8005551212 の場合、MCU でサービス プレフィックスを #8005551212 としてプロビジョニングする必要があります。その結果、他の H.323 エンドポイントが 8005551212 とダイヤルすると、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、コールを発信したエンドポイントのゾーンでデフォルト テクノロジー プレフィックスとともに登録された RASAggregator トランクにコールをルーティングします。Unified CM は、コールを MCU にルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。この文字は、MCU を表す H.323 ゲートウェイに関連付けられたルート パターンに付加されます。そのため、SCCP クライアントから MCU へのコールでも、着信番号にこの # 文字が付加されます。

MCU が [MCU] モードで設定されている場合、または E.164 アドレスを会議 ID に使用する別のベンダーの MCU である場合、# 文字を付加する必要はありません。MCU がピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合もこの条件は当てはまらず、# 文字を付加する必要はありません。

H.320 ゲートウェイのプロビジョニング

H.323 MCU と同様に、H.320 ゲートウェイも、Unified CM で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、H.320 ゲートウェイの静的 IP アドレスおよび TCP シグナリング ポートを [Device Name] フィールドに入力する必要があります。コールがゲートウェイに関連付けられたルート パターンと一致すると、Unified CM は静的 IP アドレスと TCP ポートを使用して、ゲートウェイに到達します。

（注）　Cisco Unified Videoconferencing 3500 および 5000 シリーズ ゲートウェイは、デフォルトでは TCP ポート 1720 を監視しません（Cisco Unified Videoconferencing 3500 および 5000 シリーズゲートウェイは、デフォルトでポート 1820 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Unified CM でプロビジョニングする必要があります。

ゲートウェイがピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です。ゲートウェイで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、「非ゲートキーパー制御クライアント」（P.12-33）に説明した [Device Name]、[Device Pool]、[Gatekeeper]、[Technology Prefix]、および [Zone Name] の各フィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

ゲートウェイ サービス プレフィックス

H.320 ゲートウェイは、ユーザが ISDN の宛先に到達するためにダイヤルするプレフィックスとして、テクノロジー プレフィックス（ゲートウェイではサービス プレフィックスとも呼ばれる）を使用します。コールを正しくルーティングするには、ゲートウェイのサービス プレフィックスを # 文字で始まるように設定する必要があります。たとえば、ISDN 番号に到達するためにクライアントがダイヤルするゲートウェイのサービス プレフィックスが 9 の場合、#9 としてゲートウェイでサービス プレフィックスをプロビジョニングする必要があります。この場合、H.323 クライアントが 9 と公衆網番号をダイヤルした場合（918005551212 など）、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、デフォルト テクノロジー プレフィックスと共に登録された Unified CM トランクにコールをルーティングします。Unified CM は、コールをゲートウェイにルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。ゲートウェイがピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合は、この条件は当てはまらず、# 文字を付加する必要がありません。

ゲートキーパー ゾーンの設定

前の項では、Unified CM Administration でエンドポイントをプロビジョニングする方法について説明しました。適切なゾーン定義でエンドポイント ゲートキーパーを設定する必要もあります。Unified CM で、エンドポイントの各タイプ（クライアント、MCU、またはゲートウェイ）にゾーンを設定する必要があり、オプションとして、これらのエンドポイントに関連付けられている各デバイス プールにゾーンを設定します。

各ゾーンは、ゾーンを宛先または発信元とするコール、ゾーン内で発信されるコールのすべてを、ゾーンに登録されている RASAggregator トランクにルーティングするように設定されます。エンドポイント ゲートキーパーでゾーンを設定するには、次のコマンド構文を使用します。

```
zone local <zone_name> <domain_name> <ip_address> invia <zone_name>
outvia <zone_name> enable-intrazone
```

コマンド引数 **invia** は他のゾーンからこのゾーンに発信されたコールに適用され、**outvia** はこのゾーンから他のゾーンに発信するコールに適用されます。**enable-intrazone** は、ゾーン内で発信したコールに適用されます。次の項で、これらのコマンドの使用方法を示します。

クライアント ゾーン

各エンドポイント ゲートキーパー内で設定の必要なクライアント ゾーンの数は、次の要素で決まります。

- H.323 クライアントの関連付け先となるデバイス プール

  デバイス プールは、各 H.323 クライアントの 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべての H.323 クライアントを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるクライアント ゾーンは 1 つだけです。つまり、H.323 クライアントで使用するデバイス プールごとに、ゲートキーパーで個別のクライアント ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各クライアント ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のクライアント ゾーンを定義する必要があります。

説明のために、次の例でクライアント ゾーンの設定方法を示します。例 12-1 は、すべての H.323 クライアントが同じデバイス プールに関連付けられた単一の Unified CM クラスタに定義される、単一のクライアント ゾーンを示しています。例 12-2 は、H.323 クライアントが 2 つの異なるデバイス プールに分割された単一の Unified CM クラスタを示しています。

（注） 次の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 12-1　単一の Unified CM クラスタと単一のデバイス プールのクライアント ゾーン

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy clients default inbound-to terminal
no use-proxy clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 12-2　単一の Unified CM クラスタと 2 つのデバイス プールのクライアント ゾーン

```
gatekeeper
zone local dp1-clients domain.com invia dp1-clients outvia dp1-clients enable-intrazone
zone local dp2-clients domain.com invia dp2-clients outvia dp2-clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy dp1-clients default inbound-to terminal
no use-proxy dp1-clients default outbound-from terminal
no use-proxy dp2-clients default inbound-to terminal
no use-proxy dp2-clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

以前は Cisco Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper は、H.323 プロキシ機能を提供していましたが、廃止される予定です。この機能は Unified CM と互換性がありませんが、端末（クライアント）との間のすべてのコールにプロキシを使用するゲートキーパーのコマンドは、まだデフォルトで有効になっています。この機能はクライアント ゾーンごとに、次のコマンド構文で無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] terminals
```

Cisco MCM プロキシは、Cisco IOS Multiservice IP-to-IP Gateway と、それに関連付けられた中継ゾーン対応 Cisco IOS Gatekeeper というソリューションに置き換えられました。このマニュアルでは IP-to-IP ゲートウェイについては説明していませんが、Cisco Unified CM は、RASAggregator トラン

クをゲートキーパーに登録することで中継ゾーンと IP-to-IP ゲートウェイの構成を活用し、効果的に IP-to-IP ゲートウェイを模倣し、ゲートキーパーが IP-to-IP ゲートウェイであるかのように、すべての invia、outvia、および enable-intrazone コールを RASAggregator トランクにルーティングしています。

クライアント ゾーン プレフィックス

H.323 クライアント ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU ゾーン

各エンドポイント ゲートキーパー内で設定の必要な MCU ゾーンの数は、次の要素で決まります。

- MCU の関連付け先となるデバイス プール

  デバイス プールは、各 MCU の 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべての MCU を同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要がある MCU ゾーンは 1 つだけです。つまり、MCU で使用するデバイス プールごとに、ゲートキーパーで個別の MCU ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各 MCU ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別の MCU ゾーンを定義する必要があります。

MCU ゾーンのゲートキーパー設定は、例 12-1 および例 12-2 に示した設定と同様で、これらを MCU 用に設定したものです。

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper は MCU またはゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 MCU ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] [MCU | gateway]
```

MCU を MCU として登録する場合は、**no use-proxy** コマンドの最後で **MCU** 引数を使用します。MCU をゲートウェイとして登録する場合は、**gateway** 引数を使用します。

MCU ゾーン プレフィックス

H.323 MCU ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU が E.164 アドレスではなくテクノロジー プレフィックスとしてサービス プレフィックスを登録する場合は、すでに説明したように、# 文字を MCU のサービス プレフィックスに付加する特殊な設定を使用します（「MCU サービス プレフィックス」（P.12-35）を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントが MCU のサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プ

レフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

H.320 ゲートウェイ ゾーン

各エンドポイント ゲートキーパー内で設定の必要な H.320 ゲートウェイ ゾーンの数は、次の要素で決まります。

- H.320 ゲートウェイの関連付け先となるデバイス プール

  デバイス プールは、各 H.320 ゲートウェイの 1 次、2 次、および 3 次 Unified CM サーバを決定します。すべてのゲートウェイを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるゲートウェイ ゾーンは 1 つだけです。つまり、H.320 ゲートウェイで使用するデバイス プールごとに、ゲートキーパーで個別のゲートウェイ ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Unified CM クラスタにサービスを提供するのか、複数の Unified CM クラスタにサービスを提供するのか

  各ゲートウェイ ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Unified CM クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のゲートウェイ ゾーンを定義する必要があります。

ゲートウェイ ゾーンのゲートキーパー設定は、例 12-1 および例 12-2 に示した設定と同様で、これらをゲートウェイ用に設定したものです。

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper はゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 H.320 ゲートウェイ ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] gateway
```

ゲートウェイ ゾーン プレフィックス

H.320 ゲートウェイ ゾーンには、ゾーン プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

また、すでに説明したように、ゲートウェイのサービス プレフィックスに # 文字を付加する特殊な設定を使用する必要があります（「ゲートウェイ サービス プレフィックス」（P.12-36）を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントがゲートウェイのサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プレフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

ゾーン サブネット

すでに説明したように、H.323 仕様では、単一のゲートキーパーで複数のゾーンを管理できます。ただし、ゲートキーパーには、デバイスから Registration Request（RRQ）を受信したときに、そのエンドポイントをどのゾーンに配置するかを判断する手段が必要です。RRQ メッセージには、エンドポイン

トがどのゾーンへの登録を希望するかを示す Gatekeeper Identifier フィールドが含まれています。ただし、多くの H.323 ビデオ エンドポイントはこのフィールドを設定せず、ゲートキーパーに複数のゾーンが定義されている場合、ゲートキーパーはエンドポイントを配置するゾーンを認識できません。そのため、**zone subnet** コマンドを使用して、エンドポイントと関連付けられたゾーンをゲートキーパーに示す必要があります。このコマンドは、各ゾーンへの登録が許可される IP アドレスまたは IP の範囲を定義します。コマンド構文には、ネットワーク マスクの入力が必要です。そのため、32 ビット（/32）のネットワーク マスクを入力して特定のホスト アドレスを指定するか、それよりも小さなネットワーク マスクを指定してアドレスの範囲を指定します。

MCU、H.320 ゲートウェイ、および Unified CM サーバは通常、固定 IP アドレスを使用しますが、H.323 クライアントは DHCP アドレスを使用できます。そのため、**zone subnet** コマンドは MCU ゾーンおよびゲートウェイ ゾーンにのみ定義し、クライアント ゾーンは任意の IP アドレスを許可できるようにオープンのままにすることを推奨します。例 12-3 で示すように、Unified CM サーバが MCU ゾーンおよびゲートウェイ ゾーンに登録することも許可する必要があることに注意してください。

（注）　次の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 12-3　　ゾーン サブネットの定義

```
gatekeeper
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
```

例 12-3 の設定では、MCU ゾーンの MCU および RASAggregator を MCU ゾーンに登録することを明示的に許可しています。また、ゲートウェイ ゾーンのゲートウェイおよび RASAggregator をゲートウェイ ゾーンに登録することを明示的に許可しています。また、MCU およびゲートウェイをクライアント ゾーンに登録できないように明示的に拒否しています。その他のすべての IP アドレス（クライアント ゾーンの RASAggregator を含む）は、クライアント ゾーンに登録することが暗黙的に許可されています。

エンドポイントの存続可能時間

エンドポイントは、簡易な Registration Request（RRQ）をゲートキーパーに定期的に送信し、登録状態を維持します。これらの RRQ を送信する間隔は、Time to Live（TTL; 存続可能時間）値とも呼ばれます。エンドポイントは、使用する TTL を RRQ の本体で指定できます。ゲートキーパーは、エンドポイントが要求した TTL 値を受け入れて Registration Confirm（RCF）応答でエコーするか、異なる TTL 値を RCF で指定してエンドポイントの要求を上書きします。

TTL 値が RRQ で指定されていない場合は、ゲートキーパーが RCF 応答で指定する必要があります。この場合、エンドポイントはゲートキーパーが指定した TTL に従います。Cisco IOS Gatekeeper は、エンドポイントが指定したすべての TTL 値に従います。ただし、多くの H.323 ビデオ エンドポイントは、RRQ で TTL 値を指定しません。この場合、Cisco IOS Gatekeeper は、デフォルト値として 1800 秒（30 分）の TTL 値を指定します。Cisco IOS Gatekeeper は、エンドポイントからメッセージを受信せずに TTL 間隔の 3 倍の時間（3 X 30 分 = 90 分）が経過すると、そのエンドポイントの登録をフラッシュします。

TTL 値を大きくすると、静的 IP アドレスを使用しない H.323 クライアントで問題が発生することがあります。たとえば、デフォルト TTL 値の 1800 秒を使用した場合、クライアントをネットワークから切断し、別のロケーションに移動して異なる DHCP アドレスを受け取った場合、TTL 間隔の 3 倍が経過して、ゲートキーパーがそのエンドポイントの元の登録をフラッシュするまで、ゲートキーパーへの登録に失敗します（Registration Reject（RRJ）の理由値「duplicate alias」）。

したがって、ネットワークに悪影響が生じない範囲で、TTL 値はできるだけ小さくするようにしてください。Cisco IOS Gatekeeper では、60 秒から 3600 秒の任意の値に TTL 値を設定できます。ほとんどの場合、60 秒でうまく動作するはずです。ただし、すでにゲートキーパーの使用率が高い場合は、TTL をデフォルトの 1800 秒から 60 秒に調整すると、負荷が過大になることがあります。

TTL 値を設定するには、次のコマンド構文を使用します。

```
gatekeeper
endpoint ttl <seconds>
```

サポートされるゲートキーパー プラットフォーム

Cisco Unified CM を使用するエンドポイント ゲートキーパーとして機能するには、Cisco IOS Gatekeeper で Cisco IOS Release 12.3(11)T 以降を実行する必要があります。インフラストラクチャ ゲートキーパーの最小 Cisco IOS リリース要件については、次の Web サイトで入手可能な最新の『*Cisco Unified Communications System Release Notes for IP Telephony*』を参照してください。

http://www.cisco.com/go/unified-techinfo

ルータ プラットフォームで使用する必要があるリリースと機能を判断するには、次の URL にある Cisco Feature Navigator を使用します（Cisco.com ログイン アカウントが必要）。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

詳細については、次の Web サイトで入手可能な『*Cisco IOS H323 Gatekeeper Data Sheet*』も参照してください。

http://www.cisco.com/en/US/prod/collateral/voicesw/ps6788/vcallcon/ps4139/data_sheet_c78_561921.html

エンドポイント ゲートキーパーの要約

この項では、エンドポイント ゲートキーパーに関する重要なポイントを要約し、前の例で使用したテクニックを組み合せたいくつかの設定例を示します。

- エンドポイントのタイプ（クライアント、MCU、および H.320 ゲートウェイ）ごとに、エンドポイント ゲートキーパーに個別のゾーンを設定します。エンドポイントが複数のデバイス プールに関連付けられている場合は、エンドポイントのタイプごとに複数のゾーンを設定します。
- 各ゾーンに登録する RASAggregator トランクを設定します。このトランクは、Unified CM Administration でゲートキーパー制御 H.323 クライアントを設定したときに、自動的に作成されます。ただし、非ゲートキーパー制御 H.323 クライアント、H.323 MCU、および H.320 ゲートウェイに対しては、ゾーンの RASAggregator トランクを作成するために、ダミーのゲートキーパー制御 H.323 クライアントを設定する必要があります。
- RASAggregator トランクを IP-to-IP ゲートウェイとしてゲートキーパーに登録するには、デバイス パラメータ [Send Product ID and Version ID] を [True] に設定します。このように設定すると、ゲートキーパーは各ローカル ゾーン定義に適用される **invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** の各コマンドを使用することによって、ゾーンを宛先または発信元とするコール、またはゾーン内で発信されるコールのすべてについて、RASAggregator を選択できます。

- エンドポイント ゾーンにゾーン プレフィックスを関連付ける必要はありません。エンドポイントが何をダイヤルしても、ゲートキーパーは一致するゾーン プレフィックスまたはテクノロジー プレフィックスを見つけることなく、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングする必要があります。ゲートキーパーで、ダイヤルされた番号と MCU またはゲートウェイのテクノロジー プレフィックスが間違って一致することを防ぐために、すべての MCU およびゲートウェイ サービス プレフィックスを # 文字でマスクし、MCU またはゲートウェイに関連付けられているルート パターンに # 文字を付加します。
- Gatekeeper Identifier（ゾーン名）の指定機能をサポートしていない H.323 エンドポイントがある場合は、登録するゾーン サブネットを設定します。
- すべてのゾーンで、古い MCM プロキシの使用を無効にします。
- ゲートキーパーの負荷が過大にならない範囲で、できるだけ低い値でエンドポイント登録の存続可能時間（TTL）を設定します。ゲートキーパーが数百のエンドポイント登録を処理するような極端なケースでは、TTL を 60 秒に設定すると、管理できない量の RAS トラフィックが発生することがあります。小規模な環境では、60 秒でうまく動作するはずです。

例 12-4 は、単一の Unified CM クラスタにサービスを提供するエンドポイント ゲートキーパーの設定を示しています。このクラスタは、単一のデバイス プールを使用して、すべての H.323 ビデオ エンドポイント タイプにサービスを提供します。

（注）　次の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 12-4　単一のクラスタと単一のデバイス プールのエンドポイント ゲートキーパー設定

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
zone local MCUs domain.com invia MCUs outvia MCUs enable-intrazone
zone local gateways domain.com invia gateways outvia gateways enable-intrazone
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
no use-proxy clients inbound-to terminals
no use-proxy clients outbound-from terminals
! no use-proxy MCUs inbound-to [MCU | gateway]
! no use-proxy MCUs outbound-from [MCU | gateway]
! no use-proxy gateways inbound-to gateway
! no use-proxy gateways outbound-from gateway
gw-type-prefix 1# default-technology
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

アプリケーション

Cisco Unified Communications には、Unified CM の機能を拡張し、高度な機能と他の通信メディアとの統合を提供する幅広いアプリケーションのポートフォリオが用意されています。これらの多くのアプリケーションは、特にビデオをサポートしていなくても、IP ビデオ テレフォニー デバイスと組み合せて使用できます。たとえば、Cisco Unified CM は、TAPI/JTAPI プロトコルを使用する CTI アプリケーションのビデオ チャネルのネゴシエーションをサポートしていませんが、CTI アプリケーションをビデオ コールと組み合せて使用する妨げにはなりません。この項では、シスコおよびサードパーティ製のアプリケーションのいくつかについて検討し、ビデオ コールに対して高度なコール トリートメントを提供できるかどうかについて説明します。

CTI アプリケーション

次のアプリケーションは、Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）インターフェイスに基づいています。

Cisco Emergency Responder

Cisco Emergency Responder（ER）は、緊急コール（911）を適切な Public Safety Answering Point（PSAP）にルーティングします。また、PSAP が事故のあった物理的な正しい場所に応答し、コールが切断された場合はコールバックできるように、発信元デバイスの正しい発信元回線 ID を PSAP に提供します。Cisco ER は、JTAPI を使用して Unified CM に統合されています。緊急コールは CTI ルートポイント経由で Cisco ER にルーティングされ、Cisco ER は、コールの転送先 PSAP および表示する発信元回線 ID を判断します。Cisco ER は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）と Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を使用して、エンドポイントが接続されている物理ポートと特定の Cisco Catalyst Ethernet スイッチを検出することによって、ネットワークの各エンドポイントを追跡し、物理的な場所を判断します。CDP を使用できない場合は、代わりに IP サブネットを使用してエンドポイントを探すように Cisco ER を設定できます。Cisco ER は、この情報をスイッチの物理的な場所に関連付け、データベースに情報を格納します。

Cisco Unified Video Advantage と Cisco IP Video Phone 7985 はどちらも、Cisco ER 検出の目的で CDP をサポートしています。Cisco Unified Video Advantage は、スイッチに CDP メッセージを直接送信しませんが、このサポート用として、関連付けられた Cisco Unified IP Phone を利用します。その結果、Video Telephony ユーザが 911 をダイヤルすると、Cisco ER は正しい PSAP にコールをルーティングできます。

サードパーティ製の SCCP ビデオ エンドポイントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。

H.323 ビデオ会議クライアントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。ただし、H.323 デバイスのコールを Cisco ER でルーティングするには、H.323 デバイスが Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Cisco ER が処理する 911 へのコールは失敗します。

Cisco Unified Communications Manager Assistant

Cisco Unified Communications Manager Assistant を使用すると、アシスタントが、関連するマネージャに対応できます。Unified CM Assistant は、JTAPI を使用して Unified CM に統合されています。Unified CM Assistant は特にビデオ対応というわけではありませんが、ビデオ対応の電話機でも

Unified CM Assistant は問題なく使用できます。Unified CM Assistant がコールを処理し、コールが最終的な宛先デバイスに転送されると、コールの 2 つのデバイスが互いに直接通信し、この時点でビデオ チャネルを確立できます。たとえば、ビデオ対応エンドポイントがマネージャのディレクトリ番号をダイヤルし、アシスタントが Unified CM Assistant アプリケーションを使用してコールをカバーした場合、コールの最初の処理ではビデオは確立されていないことがあります。しかし、アシスタントが発信者をマネージャに転送すると、Unified CM がビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Unified CM Assistant と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Unified CM Assistant が代行受信したコールは、アシスタントがマネージャにコールを転送しようとしたときに失敗します。

Cisco Unified IP Interactive Voice Response と Cisco Unified Contact Center

Cisco Unified IP Interactive Voice Response（Unified IP IVR）および Cisco Unified Contact Center（Unified CC）は、JTAPI を使用して Unified CM に統合されています。ビデオ対応デバイスが IVR アプリケーション（ヘルプ デスクなど）にコールを発信した場合、発信者がアプリケーション サーバに接続している間（発信者が IVR メニューをブラウズしている間、またはヘルプデスクのメンバーがコールを受け付けるまでキューで待機している間）、通信は音声のみになります。ただし、IVR アプリケーションがコールを最終的な宛先に転送すると、その時点でビデオ チャネルをネゴシエートできるようになります。H.323 デバイスを Cisco Unified IP IVR および Unified CC と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Cisco Unified IP IVR または Unified CC が代行受信したコールは、アプリケーションが最終的な宛先に発信者を転送しようとしたときに失敗します。

IVR アプリケーションは、多くの場合、DTMF トーンを使用して IVR メニューのオプションを選択します。別の方法としては音声認識があり、電話機のキーを押す代わりに、発信者が IVR サーバに向かってコマンドを発音します。Cisco Unified IP IVR と Unified CC はどちらも、JTAPI を使用して Unified CM に統合されているため、アウトオブバンド シグナリング メッセージで DTMF トーンを渡します。現在、市販されている多くの H.323 デバイスは、インバンド DTMF トーンを使用しています。このような H.323 クライアントでは、DTMF を使用して IP IVR または Unified CC メニューをナビゲートできません。ただし、これらの H.323 クライアントは、IVR サーバが対応していれば、音声認識を使用できます。Cisco Unified Video Advantage などのビデオ対応デバイス、サードパーティ製の SCCP ビデオ デバイス、および DTMF に H.245 英数字アウトオブバンド シグナリングを使用する H.323 エンドポイントは、DTMF トーンを使用して IVR メニューをナビゲートできます。

Cisco Unified Enterprise Attendant Console

Cisco Unified Enterprise Attendant Console は、JTAPI を使用して Unified CM に統合されています。Unified Enterprise Attendant Console は、着信コールを処理する管理用デバイスとして使用されます。Unified Enterprise Attendant Console は、特にビデオをサポートしているわけではありませんが、コールが最終的な宛先に転送されると、ビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Unified Enterprise Attendant Console と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Unified CM からの ECS の受信をサポートしていない場合、Unified Enterprise Attendant Console が代行受信したコールは、コンソール担当者が最終的な宛先に発信者を転送しようとしたときに失敗します。

Cisco IP Communicator

Cisco IP Communicator は SCCP ソフトフォンであり、ビデオはサポートでていません。Cisco Unified Video Advantage クライアントを Cisco IP Communicator に関連付けることによって、ビデオを提供できます。バージョン 2.0 では、両方のアプリケーションが同じ PC 上に存在する場合、Cisco IP Communicator を Cisco Unified Video Advantage 2.0 に関連付けることができます。詳細については、「Unified Communications エンドポイント」（P.18-1）の章を参照してください。

Cisco IP Communicator 2.1 以降のリリースではまた、Cisco IP Communicator デバイスを作成または追加する際のデバイス プロトコルとして、SIP を選択できます。ただし、SIP プロトコルを使用した Cisco IP Communicator では、Cisco Unified Video Advantage はサポートされていません。

コラボレーション ソリューション

エンドポイント間のビデオ通信を提供するために、次のテクノロジーが使用されることがあります。

T.120 アプリケーション共有

T.120 プロトコルを使用して、ドキュメント、ホワイトボード、およびテキストを会議の参加者で共有するビデオ会議エンドポイントがあります。Unified CM は、T.120 チャネルのネゴシエートをサポートしません。T.120 の代わりに、Cisco MeetingPlace やサードパーティのコラボレーション ソリューションのような Web ベースのコラボレーション ソリューションを使用することを推奨します。

Cisco Unified MeetingPlace

Cisco Unified MeetingPlace は、ハイエンドな音声およびビデオ会議ソリューションと、会議のスケジューリングおよび参加に使用する Web ベースのフロントエンドを結合します。詳細については、「Cisco Unified MeetingPlace」（P.22-13）を参照してください。

無線ネットワーキング ソリューション

ビデオは帯域幅に大きな影響を与えるため、802.11b/g などの共有無線メディアをビデオ エンドポイントに使用することは*推奨しません*。

ビデオ エンドポイントが、実稼動中の IP Phone と無線帯域幅を共有しないように注意する必要があります。ビデオは帯域幅の大半を消費するため、ビデオ、音声、およびデータを同じ無線メディアでサポートすることは困難です。

Cisco Unified Video Advantage は、関連付けられた物理 IP Phone への物理イーサネット接続に依存します。ユーザが物理イーサネット インターフェイスと、Aironet 802.11b Wireless Adapter の両方を同じ PC にインストールすることはよくあります。このような設定は、無線インターフェイスがネットワークへの優先パスになった場合に、Cisco Unified Video Advantage がこのインターフェイス経由では関連付けられないため、Cisco Unified Video Advantage で問題が発生する原因になります。常に、物理イーサネット インターフェイスを優先パスにすることを推奨します。また、ユーザが IP Phone の背面の PC ポートに接続するときは、間違って優先されないように Aironet Adapter を無効にするように指示してください。

Cisco Unified Wireless IP Phone 7925G および 7921G

Cisco Unified Wireless IP Phone 7925G および 7921G は、ビデオをサポートしません。ビデオ エンドポイントからも Cisco Unified Wireless IP Phone にコールを発信できますが、音声のみのコールとしてネゴシエートされます。ワイヤレス IP Phone ユーザは、コールの保留、転送、または会議への参加ができます。発信者が H.323 ビデオ エンドポイントの場合、これらの付加サービスを機能させるには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。

XML サービス

現在、特に Cisco Unified Video Advantage クライアント ソリューション、Cisco IP Video Phone 7985、またはサードパーティ製の SCCP ビデオ エンドポイント用に作成された XML アプリケーションはありません。ただし、これらのエンドポイントのうち、少数のサードパーティ製エンドポイント以外は、XML アプリケーションをサポートします。Cisco Unified Video Advantage は Cisco Unified IP Phone を使用するため、これらの電話機モデルでサポートされる XML アプリケーションは Unified Video Advantage でも動作します。

ほとんどのサードパーティ製 SCCP ビデオ エンドポイントは XML をサポートしますが、現在、すべての XML アプリケーションがそれらのエンドポイントで動作するわけではありません。たとえば、Cisco エクステンション モビリティおよび Berbee InformaCast 製品は、現在、サードパーティ製の SCCP エンドポイントで動作しない代表的な 2 つの XML アプリケーションです。これらのアプリケーションをサポートするには、エンドポイントのファームウェア アップグレードと、場合によっては Unified CM Administration の変更が必要になります。

CHAPTER 13

ゲートウェイ

ゲートウェイは、IP テレフォニー ネットワークを Public Switched Telephone Network（PSTN; 公衆電話交換網）、従来型の PBX、またはキー システムに接続するための複数の方法を提供します。ゲートウェイには、特殊なエントリレベルのスタンドアロン音声ゲートウェイから、機能が豊富なハイエンド統合ルータや Cisco Catalyst ゲートウェイまで、さまざまなものがあります。

この章では、IP テレフォニー ネットワークに適切なプロトコルと機能サポートを提供するために Cisco ゲートウェイを選択する際に、考慮すべき重要な要素について説明します。この章は、次の項で構成されています。

この章の新規情報

表 13-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 13-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
ビデオ テレフォニー ゲートウェイ	「ビデオ テレフォニー用のゲートウェイ」（P.13-32）	2010 年 11 月 15 日
FAX とモデムのサポート	「FAX とモデムのサポート」（P.13-19）	2010 年 4 月 2 日
T.37 Store-and-Forward FAX	「T.37 Store-and-Forward FAX」（P.13-32）	2010 年 4 月 2 日

トラフィック パターンとゲートウェイのサイジング

この項では、さまざまなトラフィック モデルまたはトラフィック パターンの違いと、それらが音声ゲートウェイの選定にどのように影響するかについて、詳しく説明します。ここでは、トラフィック集約型配置におけるトラフィック パターンとゲートウェイのサイジングに重点を置きます。

定義と用語

この項では、次の用語と定義を使用します。

- 同時コール

  システム内ですべてが同時にアクティブになるコールの数。

- 最大同時コール

  システムで処理可能な、アクティブ（通話）状態にある同時コールの最大数。1 日の*最煩雑時間*に同時にアクティブになると予測されるコールの数がこの数を超えないようにする必要があります。

- コール数/秒（cps）

  着呼率。1 秒間に着信したコールの数（つまり、新しいコール セットアップが試行されたコールの数）として定義されます。着呼率は多くの場合 1 時間あたりのコール数で計算されますが、このメトリックでは 1 時間の最後の 5 秒間に 100 件のコールが着信した場合でも平均着呼率は 100 コール/時間となり（これは通信システムとしては非常に低い数値です）、厳密とは言えません。この例を 1 秒間あたりの着呼率に換算すると、20 コール/秒という高い率になります。20 コール/秒の着呼率が 1 時間持続すると、1 時間あたりのコール数は 72,000 件になります。したがって、コール数/時間は、着信バースト トラフィック パターンを処理するシステムの能力を把握するという目的では有効なメトリックではありません。

- Busy Hour Call Attempts（BHCA; 最繁時呼数）

  1 日の最も煩雑する時間（ピーク時間）に試行されたコールの数。これは 1 日の最も煩雑する時間のコール数/秒と同じですが、1 秒間ではなく 1 時間で表します。たとえば、10 cps は 36,000 コール/時間と同じです。Busy Hour Call Completions（BHCC; 最繁時呼完了数）というメトリックもありますが、これは一部のコールが成功しなかった場合（ブロック要因が存在する場合など）、BHCA（試行されたコールの数）より低くなる可能性があります。この章では、呼完了率が 100% である（つまり、BHCA = BHCC）と仮定しています。

- バースト トラフィック

  安定した着呼は、ある期間にわたってコール試行の間隔がほぼ均等であることを意味します。たとえば、着呼率が安定しているときには、60 コール/時間はほぼ 1 分間に 1 回コール試行があることを示します（約 0.02 cps）。着呼が集中すると、ある一定の期間（1 時間など）に到着するコールの間隔が均等でなくなり、短時間にコールが集中して 1 ～数回のスパイクが生じます。最悪のケースでは、着呼率が同じ 60 コール/時間であっても、1 時間のうちの 1 秒間にすべてのコールが集中します。この場合は、その 1 時間中のほぼすべての時間の着呼率は平均 0 cps になり、1 秒間だけが 60 cps と突出します。この種のトラフィックをバースト トラフィックといい、通信システムに非常に大きな負担をかけます。

- 保持時間

  音声コールの「通話時間」。つまり、コールのセットアップから終了までの間の、2 者間に通話路が開いている時間を示します。音声システムのトラフィック エンジニアリングで使用する保持時間の業界平均値は 3 分（180 秒）です。平均コールの保持時間が短くなるほど、コールのセットアップと終了に費やされるシステム CPU 時間の割合が、通話路の維持に費やされる CPU 時間に比べて高くなります。

公衆網トラフィック パターン

音声通信システムの文脈で使用される「トラフィック」は、送受信されるコールの量を指します。特に重要となるのは、公衆網などの外部回線によって伝送されるトラフィックです。トラフィックはアーランで測定され、1 アーランは「1 つのコールが 1 時間持続すること」と定義されています。この項では、アーランについては詳しく説明しません。単に、特定のトラフィック量に対して必要な回線の数を算出する際にアーラン B とアーラン C という数表を使用する、と述べるにとどめます。

必要な外部回線のサイズは、企業で受信および生成されるトラフィックの量によって決まります。ただし、お客様の多くは一般に、IP ベースの通信システムにおいても、それまで TDM ベースのシステムで使用していたのと同じ数の回線を使用し続けます。このサイジング方法は特に問題が発生しなければ有効ですが、その一方で継続的なシステム トラフィック分析プロセスを日常的なメンテナンス業務に組み込むことも重要です。トラフィック分析を行うと、現在のトラフィック レベルに対してシステムのプロビジョニングが過剰である（その結果、不要な回線にコストを費やしている）ことが判明したり、あるいは逆にプロビジョニングが不足していてコールのブロックや損失が起こる可能性のあることが指摘されたりします（この場合は回線数を増やすと状況が改善されます）。

一般業務のトラフィック プロファイル

ほとんどのお客様のトラフィック プロファイルは一般業務パターンです。これは、*煩雑時間*が通常 1 日 2 時間（午前 10:00 ～ 11:00 と午後 2:00 ～ 3:00）あることを意味します。これらの煩雑時間パターンは、多くの場合、1 日の業務の始まりや昼休み明けなどの要因に起因します。コールそのものは保持時間が長くなる傾向があり、安定的に着信、終了する傾向も見られます。トラフィック計算に使用する保持時間の一般的な業界平均値は、3 分です。

煩雑時間のトラフィックを考慮して通信システムを設計していれば、通常は問題は起こりません。それより低いレベルでシステムを設計していると、コールのブロックや損失が発生し、業務に悪影響をもたらすおそれがあります。

コンタクト センターのトラフィック プロファイル

コンタクト センターでは、通常ある一定数のオペレータまたは Interactive Voice Response（IVR; 自動音声応答）システムを利用して大量のコールを処理するという点で、少し異なるトラフィック パターンが見られます。コンタクト センターではリソースを最大限に活用する必要があるため、オペレータ、トランク、および IVR システムは業務時間中（通常は 1 日 24 時間）ずっと煩雑した状態が続きます。コール キューイングの使用が一般的で（着信コール トラフィックがオペレータの処理能力を超えると、次のオペレータが空くまでコールはキュー内で待機します）、オペレータは通常、自分の勤務時間の間、コンタクト センターに寄せられた電話の応対に専念します。

コンタクト センターでのコールの平均保持時間は、多くの場合、一般業務の電話よりも短くなります。コールの平均保持時間が短くなる理由は、IVR システムの段階で用件が済み、オペレータと通話しない場合が多いことによります（これを「セルフサービス コール」と呼ぶことがあります）。オペレータと通話した場合の平均保持時間は 3 分（一般業務トラフィックと同じ）であるのに対して、セルフサービス コールの典型的な保持時間は約 30 秒であることから、コンタクト センター全体での平均保持時間は一般業務トラフィックよりも短くなります。

リソース（IVR ポート、公衆網トランク、オペレータなど）の使用を最適化するというコンタクト センターの目標と、コンタクト センターが電話応対専門の組織であることを考え合せると、コンタクト センターのシステムでは通常の業務環境よりも着呼率は高くなります。これらの着呼率は、一般業務トラフィックとは異なる時間帯（通常の煩雑時間ではない時間帯）に異なる理由で最大になります。たとえば、特別な休日パックのテレビ CM を流して申し込み用のフリー ダイヤルを知らせた場合、その電話を受け付けるシステムの着呼率は、CM 放送後の約 15 分間にトラフィックのピークを迎えます。この着呼率は、コンタクト センターの平均着呼率を 1 桁上回ることもあります。

コンタクト センター トラフィックに対するゲートウェイのサイジング

短い通話時間とバースト性のある着呼率は、公衆網ゲートウェイのトラフィック処理能力に影響を与えます。このような状況では、通話時間の長いコールを一定期間にわたって均等に受けるような場合に比べて、すべてのコールをタイムリーに処理するためにゲートウェイでより多くのリソースが必要となります。ゲートウェイにはこのようなトラフィック パターンを処理するさまざまな機能が装備されているため、ゲートウェイを選定する際は使用する環境を考慮して入念に検討する必要があります。ゲートウェイの中には、サポートする T1/E1 ポートの数が多い機種や、同時に着信した複数コールの処理能力が高い機種などがあります。

複数のコールがほぼ同時に着信する（つまり、着呼率が高い、またはバースト性がある）トラフィック パターンでは、適切なコール数/秒（cps）性能を持つゲートウェイが最も適しています。このような状況で、コールの保持時間を 15 秒と仮定した場合、Cisco AS5400XM ユニバーサル ゲートウェイでは 16 cps（一度にアクティブにできるコール数は 250）、Cisco 3845 サービス統合型ルータでは 13 cps（一度にアクティブにできるコール数は 200）、Cisco 3945 サービス統合型ルータでは 28 cps（一度にアクティブにできるコール数は 420）を維持できます。Cisco AS5350XM ユニバーサル ゲートウェイのパフォーマンスは、コール数/秒の観点では AS5400XM と同等です。

着呼率が安定したトラフィック パターンでは、通常、ゲートウェイが処理可能なアクティブ コールの最大数がより重要になります。このような状況で、コールの保持時間を 180 秒と仮定した場合、Cisco AS5400XM ユニバーサル ゲートウェイでは 600 の同時アクティブ コール（着呼率は最大 3.3 cps）、Cisco 3845 サービス統合型ルータでは 450 の同時アクティブ コール（着呼率は最大 2.5 cps）、Cisco 3945 サービス統合型ルータでは 720 の同時アクティブ コール（着呼率は最大 4 cps）を維持できます。

これらの数値は、次の条件がすべて該当する場合を前提とします。

- CPU 使用率が 75% を超えない。
- 公衆網ゲートウェイ コールは、ISDN PRI トランクで H.323 を使用して行われる。
- Real Time Control Protocol（RTCP）タイマーがデフォルト値の 5 秒に設定されている。
- Voice Activity Detection（VAD; 音声アクティビティ検出）がオフになっている。
- G.711 のパケット化の周期は 20 ms である。
- Cisco IOS Release 15.0.1M が使用されている。
- 専用の音声ゲートウェイ設定を使用し、イーサネット（GE）出力を有効に、QoS 機能を無効にしている（QoS 対応の出力インターフェイスまたはイーサネット以外の出力インターフェイス、あるいはその両方を使用すると、CPU リソースの消費量が増えます）。
- 付加コール機能や付加サービス、たとえばセキュリティ全般（アクセス コントロール リストやファイアウォールなど）、音声固有のセキュリティ（TLS、IPSec、SRTP）、AAA ルックアップ、ゲートキーパーを介したコール セットアップ、VoiceXML または TCL 対応のコール フロー、コール アドミッション制御（RSVP）、SNMP ポーリング/ロギングなどを有効にしていない。このような追加のコール機能を有効にすると、CPU リソースの消費量が増えます。

音声アクティビティ検出（VAD）

VAD は、コールの特定の方向の通話路が無音と認識されている間、IP パケットがほとんど生成されないようにするデジタル信号処理機能です。通常は、ある時点で発話しているのは一方の通話者だけなので、パケットは一方向だけに流れればよく、逆方向（無音方向）では不定期のキープアライブを除き、パケットを送信する必要はありません。そのため、VAD を使用すると、VoIP コールで送信される IP パケットの数が大幅に減少し、それに伴ってゲートウェイ プラットフォームの CPU サイクルも大幅に低下します。VAD によってパケットが実際にどの程度減少するかは、コール フロー、アプリケーション、および会話の状況によって異なりますが、VAD 設定を無効にした場合と比べて、パケットが 10 ～ 30% 少なくなる傾向があります。

VAD は、エンドポイントや Unified CM ネットワークに配置された音声ゲートウェイではほとんどの場合無効にされており、その他の種類のネットワークに配置された音声ゲートウェイでは、ほとんどの場合、有効にされています。

コーデック

G.711 と G.729A のサンプリング時間はどちらもデフォルトで 20 ms に設定されているため、VoIP コールの一方向のパケット レートは 50 パケット/秒（pps）になります。G.711 の IP パケット（200 バイト）は G.729A のパケット（60 バイト）よりも大きいですが、この差が音声ゲートウェイの CPU パフォーマンスに大きな影響を与えるとは実証されていません。G.711 と G.729 のパケットはどちらもルータには「小さい」IP パケットと見なされます。そのため、パケット レートは CPU パフォーマンスに影響を与える重要なコーデック パラメータです。

パフォーマンスの過負荷

Cisco IOS は、割り込みレベルのイベントを処理するために、ピーク処理中にも CPU の使用率が 100% にならないように設計されています。この項に示すパフォーマンスの数値は、約 75% の平均的な負荷を実行しているプロセッサを基にしています。特定の Cisco IOS ゲートウェイの負荷がこのしきい値を継続的に超えると、次のようになります。

- Cisco Technical Assistance Center（TAC）でその配置がサポートされなくなります。
- Cisco IOS ゲートウェイで、Q.921 タイムアウト、ダイヤル後遅延の増大、インターフェイス フラップなどの異常な動作が起こります。

Cisco IOS ゲートウェイは短時間のコールのバーストであれば処理できるようになっていますが、推奨される着呼率（コール数/秒）が継続的に超過するような状況はサポートされていません。

（注） ゲートウェイに未使用のハードウェア ポートがある場合は、そのポートを他のタスクに割り当てたくなるものです（たとえば、CMM ゲートウェイで、トラフィック計算によって公衆網トラフィックに一部のポートしか使えないことがわかっている場合など）。しかし、残りのポートは*必ず*未使用のままにしておく必要があります。そうしないと、CPU がサポートされるレベルを超えて過負荷状態に陥ります。

パフォーマンスの調整

Cisco IOS 音声ゲートウェイの CPU 使用率は、シャーシで有効にされているすべてのプロセスの影響を受けます。最も低レベルのプロセスの一部（IP ルーティングやメモリのデフラグなど）は、シャーシにライブ トラフィックがないときにも実行されます。

CPU 使用率が下がると、リアルタイムの音声パケットやコール セットアップ命令の処理に十分な CPU リソースを使用できるようになり、Cisco IOS 音声ゲートウェイのパフォーマンスが向上します。CPU 使用率を削減する手法のいくつかを表 13-2 に示します。

表 13-2　CPU 使用率を削減する手法

手法	CPU 使用率の削減量	説明
VAD を有効にする	最大 20%	VAD を有効にすると、標準的な会話において音声パケットの量が最大 45% 減少します。問題は、音声認識を使用している場合や遅延が長い場合に音声品質が低下する可能性があることです。音声はトーク スパートの開始時に突然生じ、終了時に唐突に消失するように感じられます。
RTCP を無効にする	最大 5%	RTCP を無効にすると、発信側と着信側のゲートウェイ間で送信されるアウトオブバンド情報が減少します。その結果、相手側のゲートウェイに表示される統計情報の品質が低下します。また、コールがすでにアクティブでないかどうかを判断するために RTCP パケットが使用されている場合は、着信側ゲートウェイでコールの「未完結状態」が長くなる可能性があります。
その他の重要でない機能（Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、ロギングなど）を無効にする	最大 2%	これらのプロセスは、必要でない場合は無効にできます。これらのプロセスを無効にすると、CPU がその分解放されて CPU 使用率が低下し、リアルタイム トラフィックの処理が高速になります。
コール パターンを変更してコールの長さを長くする（これにより、1 秒あたりのコール数を削減する）	可変	これはさまざまな手法で実現できます。たとえば、コールの最初に長い導入プロンプトを再生する（または既存の導入プロンプトを長くする）、コール スクリプトをコール センターで調整する、といった手法があります。

追加情報

Cisco 音声ゲートウェイの機能とコール センター トラフィックの分析の詳細については、次の資料を参照してください。

- Cisco Voice Gateway ソリューション：
  http://www.cisco.com/en/US/products/sw/voicesw/index.html#~all-prod
- Cisco Unified Communications Manager（Unified CM）でサポートされるゲートウェイ プロトコル：
  http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/admin/8_0_1/ccmsys/a08gw.html
- 次の Cisco Voice Gateway でサポートされるインターフェイスおよびシグナリング タイプ：
  - Cisco 3900 シリーズ サービス統合型ルータ
    http://www.cisco.com/en/US/products/ps10536/products_relevant_interfaces_and_modules.html
  - Cisco 2900 シリーズ サービス統合型ルータ
    http://www.cisco.com/en/US/products/ps10537/products_relevant_interfaces_and_modules.html
  - Cisco 3800 シリーズ サービス統合型ルータ
    http://www.cisco.com/en/US/products/ps5855/products_relevant_interfaces_and_modules.html
  - Cisco 2800 シリーズ サービス統合型ルータ
    http://www.cisco.com/en/US/products/ps5854/products_relevant_interfaces_and_modules.html

- MGCP、SIP、および H.323 でサポートされるゲートウェイ機能：
  http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf
- SIP ゲートウェイ RFC 準拠：
  http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/gatecont/ps6831/product_data_sheet0900aecd804110a2.html
- FXS ゲートウェイでサポートされる Skinny Client Control Protocol（SCCP）機能：
  http://www.cisco.com/en/US/prod/collateral/voicesw/ps6790/gatecont/ps2250/ps5516/product_data_sheet09186a00801d87f6.html
- MGCP、SIP、および H.323 ゲートウェイ機能に必要な Cisco IOS および Unified CM の最小リリース：
  http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）ゲートウェイ機能に必要な Cisco IOS および Unified CM の最小リリース：
  http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf
- ゲートウェイ機能：
  http://www.cisco.com/en/US/prod/collateral/routers/ps259/product_data_sheet0900aecd8057f2e0.pdf
- 音声トラフィックに関する計算手法（アーラン計算など）：
  http://www.erlang.com/calculator/

ゲートウェイ冗長性に関する考慮事項

ゲートウェイ ソリューションを配置する際は、スケーラビリティと比較したときの冗長性を慎重に考慮してください。たとえば、Cisco VGD 1T3 Voice Gateway は、1 つの物理回路に 28 本の T1 回線を配信する機能を備えています。しかし、公衆網サービスに特有の冗長性に対するニーズを考慮すると、小規模な複数のゲートウェイで全体として物理的に同じ量のサービスを配信するほうが適しています。また、複数のゲートウェイを使用すると、異なる物理的ロケーションでの配置が可能になるため、1 レベル上の冗長性（この場合は空間的な冗長性）が実現されます。

さらに、緊急サービスとのアクセスにかかわるゲートウェイ配置についても考慮する必要があります。場合によっては、複数のソリューションが必要になることもあります。たとえば、リモートの本社にある SIP トランクを介して公衆網に接続されている小規模な支店ロケーションを考えてみます。WAN または SIP トランクに障害が発生した場合でも、支店ロケーションは緊急サービスにアクセスできる必要があります。この場合、最善のソリューションは、ローカルのアナログまたは PRI サービスです。つまり、スタンドアロンのアナログ サービスを使用するか、支店ルータ上で終端する PRI サービスを使用します。

TDM ゲートウェイと VoIP トランキング ゲートウェイ

2006 年ごろまでは、企業内部の VoIP ネットワークを外部の音声サービスに接続するには、従来の公衆網に接続された TDM ゲートウェイを経由する以外に方法はありませんでした。シスコの製品ライン ナップには、公衆網をはじめ、PBX やキー システムにもアナログおよびデジタル接続できる各種 TDM ゲートウェイが揃っています。TDM 接続では、低密度アナログ（FXS、FXO）、低密度デジタル（BRI）、高密度デジタル（T1、E1、T3）など、さまざまなインターフェイスを選択できます。

2006 年ごろから、一般に「SIP トランク サービス」と呼ばれる企業向けの新しい音声サービス オプションがサービス プロバイダーから提供されるようになりました。公衆網やその他の企業外部の宛先に SIP トランクを使用して接続するには、企業の VoIP ネットワークのエッジで IP-to-IP 接続が必要です。この相互接続ポイントでは、これまで TDM ゲートウェイによって実現されていたものと同じ機能（境界の設定、コール アドミッション制御、QoS の確保、トラブルシューティングの境界の確保、セキュリティのチェックなど）が引き続き必要となります。SIP トランキング接続では、企業とサービス プロバイダー ネットワーク間の相互接続ポイントにある Cisco Unified Border Element が Session Border Controller（SBC; セッション ボーダー コントローラ）としてこれらの機能を実行します。Cisco Unified Border Element には、プロトコル変換機能により、H.323 機器と SIP 機器、または異なる種類の SIP 実装を使用した SIP 機器どうしを相互接続する機能もあります。Cisco Unified Border Element ではトランスコーディングも実行可能です。これらのいずれかの機能を利用する場合は、企業ネットワーク内部におけるプロトコル変換 またはトランスコーディング サービスなしでは相互運用できない機器間の相互接続ポイントでも Cisco Unified Border Element を使用できます。

TDM ゲートウェイ プラットフォームについては、この章の残りの部分で詳しく説明します。Cisco Unified Border Element については、「Cisco Unified CM トランク」（P.14-1）の章に詳細が記載されています。両方の機能を同一の Cisco Integrated Services Router（ISR）プラットフォームで同時に有効にできます。

Cisco ゲートウェイの概要

Cisco アクセス ゲートウェイを使用すると、Cisco Unified Communications Manager（Unified CM）と IP 以外の通信デバイスとの間で情報を交換できます。Cisco アクセス ゲートウェイには、アナログとデジタルの 2 種類があります。

Cisco アクセス アナログ ゲートウェイ

Cisco アクセス アナログ ゲートウェイには、トランク ゲートウェイとステーション ゲートウェイの 2 つのカテゴリがあります。

- アクセス アナログ ステーション ゲートウェイ

  アナログ ステーション ゲートウェイは、Unified CM を Plain Old Telephone Service（POTS; 一般電話サービス）のアナログ電話機、IVR システム、FAX マシン、およびボイスメール システムに接続します。ステーション ゲートウェイは、Foreign Exchange Station（FXS）ポートを備えています。

- アクセス アナログ トランク ゲートウェイ

  アナログ トランク ゲートウェイは、Unified CM を公衆網 Central Office（CO; セントラル オフィス）または PBX トランクに接続します。トランク ゲートウェイは、公衆網、PBX、またはキー システムへのアクセス用の Foreign Exchange Office（FXO）ポート、および従来型の PBX とのアナログ トランク接続用の E&M（recEive and transMit、または ear and mouth）ポートを備えています。応答と接続解除の監視の問題を最小限に抑えるために、可能な限り、デジタル ゲートウェイを使用してください。アナログ Direct Inward Dialing（DID; ダイヤルイン方式）および Centralized Automatic Message Accounting（CAMA）も、公衆網接続に使用できます。

Cisco アクセス デジタル トランク ゲートウェイ

Cisco アクセス デジタル トランク ゲートウェイは、Primary Rate Interface（PRI; 一次群速度インターフェイス）、Basic Rate Interface（BRI; 基本速度インターフェイス）、または T1 Channel Associated Signaling（CAS; 個別線信号方式）などのデジタル トランクを経由して、Unified CM を公衆網または PBX に接続します。デジタル T1 PRI トランクは、所定の従来型ボイスメール システムとの接続にも使用できます。

ゲートウェイ ゲイン設定の調整

ゲートウェイを介して Cisco Unified Communications ネットワークを公衆網に接続するには、停電、インピーダンスの不整合、および遅延などによるエコーや信号の減衰から生じる、音声品質問題に適切に対処する必要があります。このため、予期されるすべての音声パスに信号損失の状況を詳細に提供する Network Transmission Loss Plan（NTLP）を確立する必要があります。このプランを使用して、最適な声の大きさと効果的なエコー キャンセレーションを得るために信号の強さを調整する必要があるロケーションを識別できます。すべての通信事業者が同じ損失プランを使用するわけではないこと、また、セルラー ネットワークの存在が NTLP の作成をさらに複雑にすることに注意してください。このような NTLP を作成する前に、ゲートウェイで入力ゲインや出力衰退を調整することは推奨できません。詳細については、次の Web サイトで入手可能な『*Echo Analysis for Voice Over IP*』を参照してください。

http://www.cisco.com/en/US/docs/ios/solutions_docs/voip_solutions/EA_ISD.pdf

ゲートウェイの選択

IP テレフォニー ゲートウェイを選択する場合は、次の点を考慮してください。

- 「コア機能要件」（P.13-9）
- 「ゲートウェイ プロトコル」（P.13-10）
- 「ゲートウェイ プロトコルとコア機能要件」（P.13-11）
- 「サイト固有のゲートウェイ要件」（P.13-18）

コア機能要件

IP テレフォニー アプリケーションで使用するゲートウェイは、次のコア機能要件を満たす必要があります。

- Dual Tone MultiFrequency（DTMF）リレー機能

  DTMF リレー機能、特にアウトバンド DTMF は、DTMF ディジットを音声ストリームから切り離し、音声ストリームまたはベアラ トラフィックの一部としてではなく、ゲートウェイ プロトコル（H.323、SCCP、MGCP、または SIP）シグナリング チャネルを通じて、シグナリング標識として送信します。音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失また歪みの可能性があるので、アウトバンド DTMF が必要です。

- 付加サービス サポート

  付加サービスは、一般に、保留、転送、および会議などの基本的なテレフォニー機能です。

- FAX/モデム サポート

  FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。詳細については、「FAX とモデムのサポート」（P.13-19）を参照してください。

- Unified CM 冗長性サポート

  Cisco Unified Communications は、分散モデルに基づき、高いアベイラビリティを確保しています。Unified CM クラスタには、Unified CM の冗長性が用意されています。ゲートウェイは、プライマリ Unified CM に障害が発生した場合に、セカンダリ Unified CM への「re-home」機能をサポートする必要があります。冗長性は、Unified CM またはネットワークの障害時のコール存続可能性とは異なります。

企業での配置用に選択する IP テレフォニー ゲートウェイがすべて、上記のコア要件を満たしていることを確認するには、ゲートウェイ製品の資料を参照してください。さらに、どの IP テレフォニーの実装についても、各サイト特有の機能要件（たとえば、アナログまたはデジタル アクセス、DID、およびキャパシティ要件）があります（「サイト固有のゲートウェイ要件」（P.13-18）を参照してください）。

ゲートウェイ プロトコル

Cisco Unified CM（Release 3.1 およびそれ以降）では、次のゲートウェイ プロトコルがサポートされています。

- H.323
- Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）

Cisco Unified CM Release 4.0 以降では、トランク側での Session Initiation Protocol（SIP）がサポートされています。Cisco Unified CM Release 5.0 ～ 7.*x* の SIP トランクの実装は、より多くの機能をサポートするよう拡張されました。

プロトコルの選択は、サイト特有の要件と機器の設置ベースによって決まります。ゲートウェイの設定では、MGCP は設定が単純なので H.323 または SIP よりも優先されます。一方、サポートされるインターフェイスの堅牢性により、H.323 または SIP が MGCP より優先される場合もあります。

Simplified Message Desk Interface（SMDI）は、ボイスメール システムを PBX または Centrex システムに統合するための標準です。SMDI を介してボイスメール システムに接続し、アナログ FXS またはデジタル T1 PRI を使用するには、SCCP または MGCP プロトコルが必要です。これは、H.323 または SIP デバイスは、ポートのグループから、使用される特定の回線を識別しないからです。この目的に H.323 または SIP ゲートウェイを使用すると、Cisco Message Interface は、着信コールに使用される実際のポートまたはチャネルと、SMDI 情報とを正常に相関させることができません。

また、使用される Unified CM の配置モデルも、ゲートウェイ プロトコルの選択に影響を与える場合があります（「Unified Communications の配置モデル」（P.5-1）の章を参照してください）。

（注）　配置する前に、Cisco IOS ソフトウェアのリリース ノートを調べて、機能またはインターフェイスのサポートを確認してください。

ゲートウェイ プロトコルとコア機能要件

ここでは、各プロトコル（SCCP、H.323、MGCP、および SIP）が次のゲートウェイ機能要件をどのようにサポートするかについて説明します。

- 「DTMF リレー」（P.13-11）
- 「付加サービス」（P.13-12）
- 「Unified CM の冗長性」（P.13-15）

DTMF リレー

DTMF は、信号に音声帯域内の特定の周波数ペアを使用するシグナリング方式です。64 kbps の Pulse Code Modulation（PCM; パルス符号変調）音声チャネルは、これらの信号を容易に伝送できます。しかし、音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失または歪みの可能性があります。Voice over IP（VoIP）インフラストラクチャを介して DTMF トーンを伝送するアウトバンド シグナリング方式は、コーデックにより誘発されるこれらの症状を簡単に解決します。

SCCP ゲートウェイ

Cisco VG248 は、Transmission Control Protocol（TCP; 伝送制御プロトコル）ポート 2002 を使用して、DTMF 信号をアウトバンドで伝送します。アウトバンド DTMF は、VG248 用のデフォルトのゲートウェイ コンフィギュレーション モードです。

H.323 ゲートウェイ

Cisco 3800 シリーズ製品などの H.323 ゲートウェイは、DTMF 信号をアウトバンドで交換するための拡張 H.245 機能を使用して、Unified CM と情報を交換できます。次の例は、Cisco IOS ゲートウェイ上のアウトバンド DTMF 設定例です。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
CODEC g729ar8
dtmf-relay h245-alphanumeric
preference 0
```

MGCP ゲートウェイ

Cisco IOS ベースのプラットフォームでは、Unified CM 通信に MGCP を使用します MGCP プロトコルには、*パッケージ*の概念があります。MGCP ゲートウェイは、始動後、DTMF パッケージをロードします。MGCP ゲートウェイは、制御チャネルを介して、受信した DTMF トーンを表す*シンボル*を送信します。次に、Unified CM は、これらの信号を解釈し、アウトバンドでシグナリング エンドポイントに DTMF 信号を渡します。DTMF リレーのグローバル コンフィギュレーション コマンドは、次のとおりです。

```
mgcp dtmf-relay CODEC all mode out-of-band
```

Unified CM MGCP ゲートウェイ設定インターフェイスで、追加の設定パラメータを入力する必要があります。

デフォルトで DTMF リレーは使用可能であり、追加の設定は必要ありません。

（注）　RFC 2833 を通じて DTMF を有効にするには、**fm-package** コマンドを使用します。このコマンドは、Cisco IOS Release 12.4(6)T 以降で使用できます。

SIP ゲートウェイ

Cisco IOS ベースのプラットフォームでは、Unified CM 通信に SIP を使用できます これらのプラットフォームはさまざまな方式の DTMF をサポートしていますが、Unified CM との通信に使用できるのは次の方式だけです。

- Named Telephony Events（NTE）、または RFC 2833
- Unsolicited SIP Notify（UN）
- Key Press Markup Language（KPML）

次の例は、NTE 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay rtp-nte
```

次の例は、UN 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay sip-notify
```

DTMF 方式の選択の詳細については、「メディア リソース」（P.17-1）の章を参照してください。

付加サービス

付加サービスは、保留、転送、および会議などのユーザ機能を提供します。これらのサービスは、音声通信の確立の基本的な要件であると見なされます。IP テレフォニー ネットワークでの使用について評価される各ゲートウェイは、ソフトウェアの Media Termination Point（MTP; メディア ターミネーション ポイント）を使用しなくても、独自に付加サービスをサポートする必要があります。

SCCP ゲートウェイ

Cisco SCCP ゲートウェイは、完全な付加サービス サポートを提供します。また、Cisco IOS Release 12.4.9T で FXS SCCP ポートもサポートしています。SCCP ゲートウェイは、ゲートウェイと Unified CM 間のシグナリング チャネル、および SCCP を使用して、呼制御パラメータを交換します。

H.323 ゲートウェイ

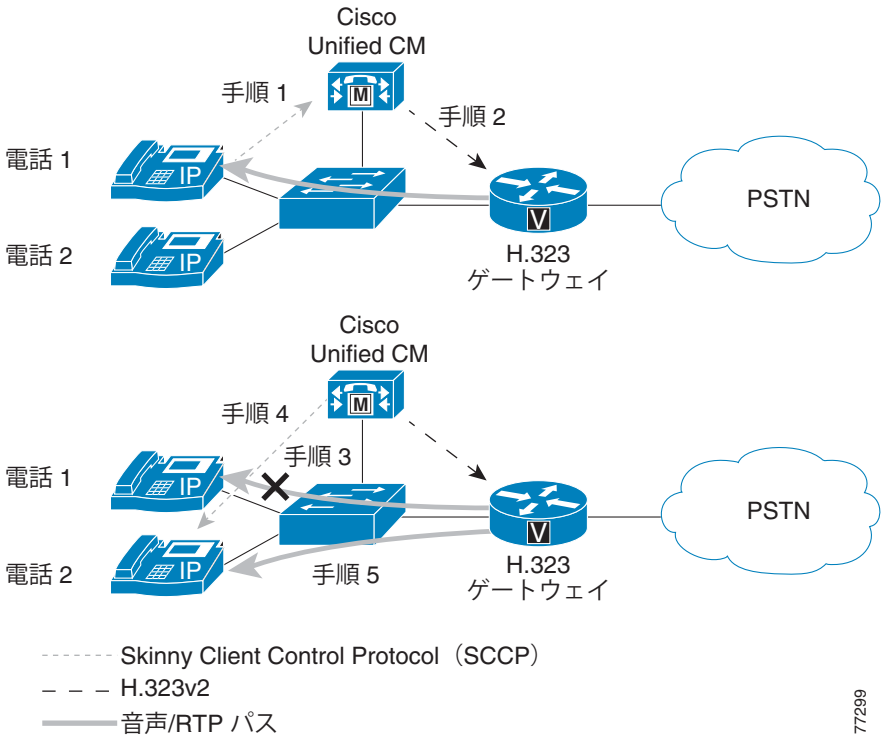
H.323v2 は、Open/Close LogicalChannel 機能と emptyCapabilitySet 機能を実行します。Cisco IOS Release 12.0(7)T および Cisco Unified CM Release 3.0 以降から始まった、H.323 ゲートウェイによる H.323v2 の使用により、MTP が付加サービスを提供する必要がなくなりました。Unified CM Release 3.1 以降では、トランスコーダが動的に割り当てられるのは、G.711 専用デバイスへのアクセスを提供すると同時に、WAN を介した G.729 ストリームを保持するために、コール中に必要な場合だけです。H.323v2 に対するフル サポートは、Cisco IOS Release 12.1.1T で利用可能です。

Unified CM を H.323 プロキシとして使用して、Cisco IOS ゲートウェイと IP Phone 間で H.323v2 コールがセットアップされた後は、その IP Phone は、ベアラ接続の変更を要求できます。Real-Time Transport Protocol（RTP）ストリームは、Cisco IOS ゲートウェイから IP Phone に直接接続されるので、サポートされる音声コーデックをネゴシエートできます。

図 13-1 と次の手順では、2 台の IP Phone 間のコール転送を示しています。

1. 電話機 1 が Cisco IOS ゲートウェイから電話機 2 にコールを転送しようとする場合、電話機 1 は、SCCP を使用して Unified CM に転送要求を出します。
2. Unified CM は、この要求を H.323v2 CloseLogicalChannel 要求に変換して、Cisco IOS ゲートウェイに送信して、適切な SessionID を求めます。
3. Cisco IOS ゲートウェイは、電話機 1 との RTP チャネルをクローズします。
4. Unified CM は、SCCP を使用して、Cisco IOS ゲートウェイとの RTP 接続をセットアップする要求を、電話機 2 に出します。同時に、Unified CM は、新しい宛先パラメータを指定して（ただし、同じ SessionID を使用）、Cisco IOS ゲートウェイに OpenLogicalChannel 要求を出します。
5. Cisco IOS ゲートウェイがこの要求を確認した後、RTP 音声ベアラ チャネルが、電話機 2 と Cisco IOS ゲートウェイとの間で確立されます。

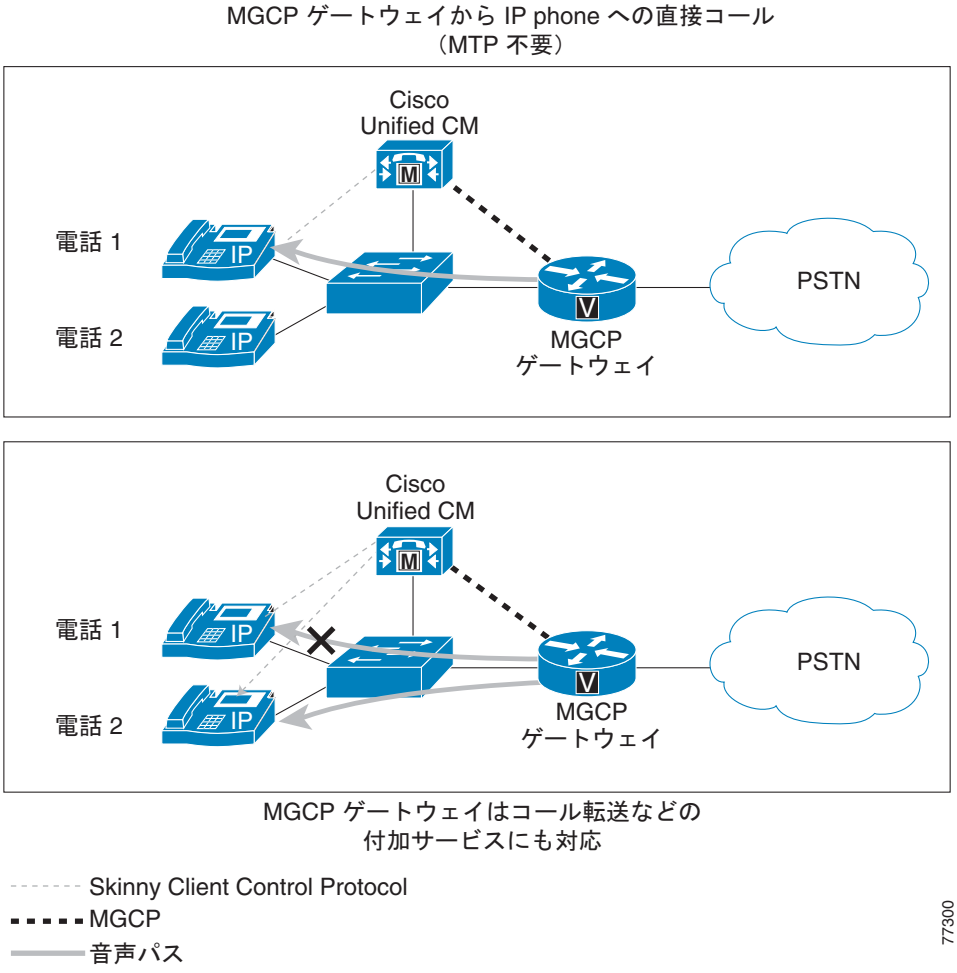
図 13-1　　H.323 ゲートウェイの付加サービス サポート



MGCP ゲートウェイ

MGCP ゲートウェイは、MGCP プロトコルを使用して、保留、転送、および会議機能を完全にサポートします。MGCP プロトコルは、すべてのセッション機能を制御する、Unified CM とのマスター / スレーブ プロトコルであるので、Unified CM は、MGCP ゲートウェイの音声接続を容易に操作できます。IP テレフォニー エンドポイント（たとえば、IP Phone）が、セッションの変更（たとえば、コールを別のエンドポイントに転送する）を必要とする場合、そのエンドポイントは、セッションの変更を SCCP を使用して Unified CM に通知します。次に、Unified CM は、Session ID に関連した現在の RTP ストリームを終了し、新しいエンドポイント情報を使用して新しいメディア セッションを開始することを、MGCP User Datagram Protocol（UDP; ユーザ データグラム プロトコル）制御接続を使用して、MGCP ゲートウェイに通知します。図 13-2 では、プロトコルが MGCP ゲートウェイ、エンドポイント、および Unified CM 間で交換される様子を示しています。

図 13-2　　MGCP ゲートウェイの付加サービス サポート



SIP ゲートウェイ

Cisco IOS SIP ゲートウェイへの Unified CM SIP トランク インターフェイスは、保留、ブラインド転送、在席転送などの付加サービスをサポートしています。付加サービスのサポートは、INVITE や REFER などの SIP 方式によって実現されます。詳細については、次のマニュアルを参照してください。

- 『*Cisco Unified Communications Manager System Guide*』。次のサイトにあります。
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html
- 『*Cisco IOS SIP Configuration Guide*』。次のサイトにあります。
  http://www.cisco.com/en/US/docs/ios/voice/sip/configuration/guide/12_4t/sip_12_4t_book.html

Unified CM の冗長性

IP テレフォニー アーキテクチャの必須部分は、高価な専有の従来型の PBX システムの代わりに、低コストの分散型 PC ベース システムを提供することです。この分散型設計は、クラスタ化された Unified CM の堅固なフォールト トレラント アーキテクチャに適しています。最も単純な形式（2 システムのクラスタ）であっても、セカンダリ Unified CM は、最初にプライマリ Unified CM によって管理されていたすべてのゲートウェイの制御権を引き受ける必要があります。

SCCP ゲートウェイ

ブート後、Cisco VG224、VG248、および ATA 188 ゲートウェイには、Unified CM サーバ情報が提供されます。これらのゲートウェイが初期設定されるときに、Unified CM のリストがゲートウェイにダウンロードされます。このリストでは、プライマリ Unified CM とセカンダリ Unified CM に優先順位が付けられています。プライマリ Unified CM が通信不能になった場合、ゲートウェイはセカンダリ Unified CM に登録されます。

WAN リンク障害用の H.323 VoIP コール プリザベーション

WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能を使用すると、他のエンドポイントとは異なるエンティティ（シグナリングをルーティングするゲートキーパーや、接続している 2 者間でシグナリングを仲介するコール エージェント（Cisco BTS 10200 Softswitch、Cisco PGW2200 Softswitch、Cisco Unified CM など）など）によってシグナリングが処理される H.323 トポロジにおいて、接続性が維持されます。コール プリザベーションが役立つのは、ゲートウェイと他のエンドポイント（通常は Cisco Unified IP Phone）は同じサイトにあるものの、コール エージェントがリモート サイトにあり、接続障害が起こりやすいような場合です。

H.323 コール プリザベーションは、次の種類の障害と接続に対応します。

障害の種類：

- WAN リンクのフラッピングや性能低下などの WAN 障害
- Cisco Unified CM ソフトウェアの障害（Unified CM サーバでの ccm.exe サービスのクラッシュなど）
- LAN 接続の障害（障害がローカル ブランチで発生した場合を除く）

接続の種類：

- Cisco Unified CM で制御された 2 つのエンドポイント間のコールで、次の条件に該当する場合
  - Unified CM がリロード中の場合
  - 一方または両方のエンドポイントと Unified CM との間で H.225.0 または H.245 メッセージのシグナリングに使用される TCP 接続が失われたか、フラッピングしている場合
  - エンドポイントがクラスタ内の異なる Unified CM に登録されていて、その 2 つの Unified CM 間の TCP 接続が失われた場合

  - IP Phone 間のコールで、公衆網が同じサイトにある場合
- ソフトスイッチによって制御されている Cisco IOS ゲートウェイとエンドポイント間のコールで、シグナリング（H.225.0、H.245、またはその両方）フローはゲートウェイとソフトスイッチ間で実行され、メディア フローはゲートウェイとエンドポイント間で実行される場合
  - ソフトスイッチがリロード中の場合
  - ゲートウェイとソフトスイッチ間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがエンドポイント上のコールをクリアしない場合
  - ソフトスイッチとエンドポイント間の H.225.0 または H.245 TCP 接続が失われ、ソフトスイッチがゲートウェイ上のコールをクリアしない場合
- メディア フローアラウンド モードで動作している Cisco Unified Border Element（旧称 Cisco Multiservice IP-to-IP Gateway）がコール フローに含まれていて、その Cisco Unified Border Element がリロードしているか、ネットワークの残りの部分との接続を失った場合

メディアが保持された後、一方の通話者が電話を切るか、メディアがアクティブでないことが検出されると、コールは終了します。コンピュータによって生成されたメディア ストリーム（メディア サーバからの音楽ストリーミングなど）が存在する場合は、メディア非アクティビティ検出は機能しませんが、コールは保留になる可能性があります。Cisco Unified CM はこの状況に対処するため、このようなコールは保持しないようにゲートウェイに指示しますが、サードパーティ製デバイスや Cisco Unified Border Element はそうしたことは行いません。

この機能において、フラッピングは「IP 接続の一時的な喪失が何度も繰り返されること」と定義されています。このような現象は、WAN または LAN の障害によって発生する可能性があります。Cisco IOS ゲートウェイと Cisco Unified CM 間の H.323 VoIP コールは、フラッピングが起こると終了する場合があります。Unified CM は、TCP 接続が失われたことを検出すると、コールをクリアし、TCP FIN を送信してコールで使用されていた TCP ソケットを閉じます。このとき、H.225.0 Release Complete メッセージまたは H.245 End Session メッセージは送信しません。これを *quiet clearing* と呼びます。ネットワークが短時間復帰した間に Unified CM から送信された TCP FIN がゲートウェイに到達すると、ゲートウェイはコールを終了します。TCP FIN がゲートウェイに到達しなくても、ネットワークが復帰すると、ゲートウェイから送信された TCP キープアライブが Unified CM に到達します。Unified CM はすでに TCP 接続を閉じているので、キープアライブに応答して TCP RST メッセージを送信します。ゲートウェイは RST メッセージを受け取ると、H.323 コールを終了します。

WAN リンク障害用の H.323 VoIP コール プリザベーション拡張機能の設定には、**call preserve** コマンドの設定を含める必要があります。Cisco Unified Communications Manager を使用している場合は、Service Parameters ウィンドウから Allow Peer to Preserve H.323 Calls パラメータを有効にする必要があります。

call preserve コマンドを発行すると、H.225.0 または H.245 接続でのアクティブ コールに関するソケットの終了またはソケット エラーがゲートウェイで無視されるため、これらの接続を使用しているコールを終了せずにソケットを閉じることができます。

すべてのコールに対して H.323 VoIP コール プリザベーションを有効にする例

次の設定例では、すべてのコールに対して H.323 VoIP コール プリザベーションを有効にします。

```
voice service voip
 h323
  call preserve
```

MGCP ゲートウェイ

MGCP ゲートウェイにも、プライマリ Unified CM との通信が失われた場合に、セカンダリ Unified CM にフェールオーバーする機能があります。フェールオーバーが起きても、アクティブ コールは保持されます。

MGCP ゲートウェイのコンフィギュレーション ファイル内で、プライマリ Unified CM は、**call-agent <hostname>** コマンドを使用して指定され、セカンダリ Unified CM のリストは、**ccm-manager redundant-host** コマンドを使用して追加されます。プライマリ Unified CM とのキープアライブは、MGCP アプリケーション レベルのキープアライブ メカニズムを介して行われます。このメカニズムでは、MGCP ゲートウェイは、空の MGCP notify（NTFY）メッセージを Unified CM に送信し、確認応答を待ちます。バックアップ Unified CM とのキープアライブは、TCP キープアライブ メカニズムを介して行われます。

プライマリ Unified CM が後で使用可能になると、MGCP ゲートウェイは、元の Unified CM に「re-home」（つまり復帰）できます。この復帰は、ただちに行われることもあれば、設定可能な時間が経過した後、または接続されているすべてのセッションが解除された後に行われることもあります。これは、次のグローバル コンフィギュレーション コマンドを使用して使用可能になります。

```
ccm-manager redundant-host <hostname1 | ipaddress1 > <hostname2 | ipaddress2>
[no] call-manager redundancy switchback [immediate|graceful|delay <delay_time>]
```

SIP ゲートウェイ

Cisco IOS SIP ゲートウェイでの冗長性は、H.323 と同様の方法で実現できます。SIP ゲートウェイがプライマリ Unified CM との接続を確立できない場合、高い優先順位を持ち、別の dial-peer ステートメントで指定されるセカンダリ Unified CM との接続を試行します。

デフォルトでは、Cisco IOS SIP ゲートウェイは dial-peer で設定された Unified CM の IP アドレスに SIP INVITE 要求を 6 回送信します。SIP ゲートウェイは、その Unified CM から応答を受信しなかった場合、他の dial-peer で設定された、優先順位の高い Unified CM との接続を試行します。

Cisco IOS SIP ゲートウェイは、INVITE に対する SIP 100 応答を 500 ms 待ちます。デフォルトでは、Cisco IOS SIP ゲートウェイがバックアップ Unified CM に到達するまでに最大 3 秒かかります。SIP INVITE の再試行回数は、**sip-ua** 設定で **retry invite** <*number*> コマンドを使用して変更できます。また、Cisco IOS SIP ゲートウェイが SIP INVITE 要求に対する SIP 100 応答を待つ期間は、**sip-ua** 設定で *timers trying* **<time>** コマンドを使用して変更できます。

バックアップ Unified CM へのフェールオーバーを高速化する別の方法としては、**dial-peer** 文での **monitor probe icmp-ping** コマンドの設定があります。Unified CM が Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー メッセージ（ping）に応答しなかった場合、そのダイヤル ピアはシャットダウンされます。このコマンドが役に立つのは、Unified CM が到達不能のときだけです。ICMP エコーメッセージは、10 秒ごとに送信されます。

次のコマンドを使用すると、Cisco IOS SIP ゲートウェイに対して Unified CM の冗長性を設定できます。

```
sip-ua
 retry invite <number>
 timers trying <time>

dial-peer voice 101 voip
 destination-pattern 2...
 session target ipv4:10.1.1.101
 preference 0
 monitor probe icmp-ping
 session protocol sipv2


dial-peer voice 102 voip
 destination-pattern 2...
```

```
session target ipv4:10.1.1.102
preference 1
monitor probe icmp-ping
session protocol sipv2
```

サイト固有のゲートウェイ要件

IP テレフォニーの実装にはそれぞれ、サイト固有の要件があります。次の質問は、IP テレフォニー ゲートウェイの選択に役立ちます。

- 公衆網（または PBX）アクセスは、アナログですか、デジタルですか。
- 公衆網または PBX には、どのタイプのアナログ（FXO、FXS、E&M、DID、CAMA）インターフェイス、またはデジタル（T1、E1、CAS、CCS）インターフェイスが必要ですか。
- 公衆網アクセスがデジタルである場合、どのタイプのシグナリングが必要ですか（T1 CAS、Q.931 PRI、E1 CAS、または R2）。
- PBX は、現在どのタイプのシグナリングを使用していますか。
  - FXO または FXS: ループ スタートまたはグラウンド スタート
  - E&M: ウィンク スタート、ディレイ スタート、またはイミディエート スタート
  - E&M: タイプ I、II、III、IV、または V
  - T1: CAS、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、または Proprietary D チャネル（CCS）シグナリング
  - E1: CAS、R2、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、Proprietary D チャネル（CCS）シグナリング
- PBX は、現在どのタイプのフレーム同期（SF、ESF、または G.704）と回線エンコーディング（B8ZS、AMI、CRC-4、または HDB3）を使用していますか。
- PBX に、専有シグナリングを渡す必要がありますか。必要な場合、そのシグナリングはどのタイムスロットで渡されますか。それは HDLC フレームですか。
- ゲートウェイにどれくらいのキャパシティが必要ですか。つまり、チャネルがいくつ必要ですか（一般に、音声チャネルが 12 本以上必要な場合は、デジタルの方が、アナログ ソリューションより費用対効果が高くなります）。
- ダイヤルイン方式（DID）が必要ですか。必要な場合は、アナログか、デジタルかを指定してください（日本ではアナログ DID 未対応）。
- 発呼回線 ID（CLID）が必要ですか。
- 発信者名が必要ですか。
- どのタイプの FAX およびモデム サポートが必要ですか。
- どのタイプの音声圧縮が必要ですか。
- どのタイプの付加サービスが必要ですか。
- PBX はクロッキングをサポートしますか。または PBX は、Cisco ゲートウェイがクロッキングをサポートすることを期待しますか。
- 必要なすべてのゲートウェイ、ルータ、およびスイッチを収容するラック スペースがありますか。

（注）　Direct Inward Dial（DID; ダイヤルイン方式）とは、オペレータが介在しなくても、外部コールを直接、端末回線に着信できるようにする Private Branch eXchange（PBX; 構内交換機）またはセントレック（Centrex）機能のことです。

（注）　発呼回線 ID（CLI、CLID、または ANI）とは、着呼側に対して発信番号を表示する、デジタル電話ネットワークで利用可能なサービスを指します。セントラル オフィス機器は、発信者の電話番号を識別し、発信者についての情報をコール自体と一緒に送信できるようにします。CLID は、Automatic Number Identification（ANI; 自動番号識別）と同義です。

Cisco Unified Communications ゲートウェイは、大部分の主要 PBX ベンダー製品と相互運用でき、EIA/TIA-464B に準拠しています。

可能な選択肢を絞り込むには、サイト固有およびコアのゲートウェイ要件から始めるのが適しています。必要な機能を指定した後、該当する設定ごとに、企業における規模と複雑さが異なる単一サイトの配置であるか、マルチサイトによる配置であるかに関係なく、ゲートウェイの選択を行うことができます。

次の表では、さまざまな Cisco ゲートウェイ モデルによってサポートされる機能とインターフェイス タイプをまとめています。

（注）　次の表では、Cisco IOS および Unified CM のリリース番号は、リストされている機能を特定のゲートウェイ プラットフォーム上でサポートできるようになったリリースを指しています。Cisco IOS 機能の詳細については、Cisco Feature Navigator（http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp）を参照してください。

FAX とモデムのサポート

ここでは、Unified CM と Cisco 音声ゲートウェイで使用可能な FAX とモデムのサポートについて説明します。まず、Cisco 音声ゲートウェイ上での FAX とモデムのサポートの概要を説明した後、サポートされるプラットフォームとコンフィギュレーション ファイル例をリストします。

ゲートウェイでの FAX パススルーと FAX リレーのサポート

FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタルで伝送されます。

元の形式では、FAX データはデジタルで、High-Level Data Link Control（HDLC; ハイレベル データリンク コントロール）フレームに含まれています。しかし、従来の公衆網を経由して送信するために、これらのデジタル HDLC フレームはアナログ搬送波に変調されます。このアナログ搬送波は、公衆網環境で効果的に FAX を送信するためには必要ですが、IP パケット ネットワークで使用されるデジタル転送方式にとっては最適ではありません。そのため、IP インフラストラクチャ上で FAX を送信できるように、専用の転送方法が考案されました。

IP 上で FAX を転送する主な方法には、パススルーとリレーの 2 つがあります。パススルーは最も単純な方法で、音声コーデックが人間の音声に対して行うのと同じように、アナログ FAX 信号をサンプリングしてデジタル化します。使用可能なコーデックは多数存在しますが、Cisco 音声ゲートウェイのパススルーでは、アナログ FAX 信号の歪みが最も少ないという理由で、常に G.711 コーデックを使用して FAX 情報が伝送されます。元の音声コールで高圧縮コーデックが使用されている場合は、アップス

ピード機能を使用してそのコーデックが G.711 に変更されます。パススルーは一般に Voice Band Data（VBD; 音声帯域データ）とも呼ばれています。シスコでは、モデム パススルーと FAX パススルーの 2 種類のパススルーを提供しています。この 2 つのパススルー バージョンの名前は、Cisco IOS Command Line Interface（CLI; コマンドライン インターフェイス）での設定から導出されます。これらのパススルー バージョン間のこの他の違いは、スイッチオーバーとトリガー トーンに集中しています。これらについては、以降の各パラグラフで詳しく説明します。

モデム パススルーは、通常、シスコ独自の Named Signaling Event（NSE）パケットを使用して、コールを音声モードからパススルー モードに切り替えます。一般に、これは NSE ベースのスイッチオーバーと呼ばれます。この音声モードからパススルーへの切り替えは、FAX パススルーだけでなくリレーにとっても重要な概念です。Cisco 音声ゲートウェイ上のコールはすべて音声コールとして開始され、そのコールが FAX コールであるとゲートウェイで認識された場合にだけ、モードが適切に切り替えられます。

モデム パススルー機能は、FAX またはモデム コールの開始時に、2100 Hz CED または ANSam トーンによってトリガーされます。CED トーンは G3 FAX および低速モデムと関連付けられていますが、ANSam トーンは SG3 FAX および高速モデムによって使用されます。従来的には、ANSam または CED トーンが検出されたとき、モデム パススルーはシスコ独自の NSE パケットを使用して、音声モードからモデム パススルーへのスイッチオーバーのリモート音声ゲートウェイをシグナリングしていました。しかし現在は、モデム パススルーでは、NSE ベースのスイッチオーバーだけでなく、H.323 または SIP 呼制御プロトコルを使用したプロトコルベースのスイッチオーバーもサポートしています。モデム パススルーは、H.323 または SIP を使用してスイッチオーバーを処理するように設定されている場合、標準ベースの NTE メッセージも使用します。これにより、オプションでリモート音声ゲートウェイをシグナリングして、エコー キャンセラを無効にします。このようなモデム パススルーの拡張機能によって、サードパーティ製のデバイスとの相互運用性が向上します。これらの拡張機能は、Cisco IOS Release 12.4(24)T 以降で導入されています。

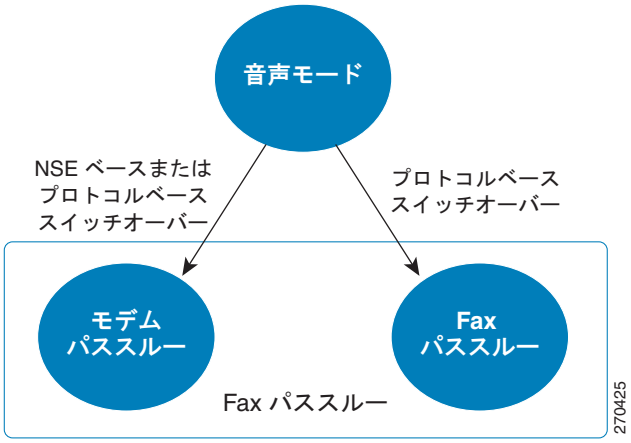
その名前にかかわらず、モデム パススルーは FAX コールにも広く使用されます。モデム パススルーをアクティブにするには、Cisco IOS Command Line Interface（CLI; コマンドライン インターフェイス）で、**modem passthrough** コマンド（H.323、SIP、および SCCP 音声ゲートウェイの場合）か、**mgcp modem passthrough** コマンド（MGCP 音声ゲートウェイの場合）を使用します。

FAX パススルーでは、モデム パススルーとは異なり、NSE ベースのスイッチオーバーをサポートしていません。FAX パススルーでは常に、基礎となる呼制御プロトコルに基づいて、コールを音声モードから FAX パススルーに切り替えます。FAX パススルーでは、H.323 および SIP の呼制御プロトコルを使用して、プロトコルベースのスイッチオーバーだけをサポートしています。FAX パススルーでは、スイッチオーバーに呼制御プロトコルを利用するため、通常はサードパーティ製のデバイスと相互運用できます。

FAX パススルーは、G3 FAX コールに関連付けられた V.21 フラグの検出によってトリガーされます。したがって、この転送方式はモデムや SG3 FAX コールに対しては使用できません。H.323 および SIP 音声ゲートウェイ上で FAX パススルーを有効にするコマンドは、**fax protocol pass-through** です。

図 13-3 は、Cisco 音声ゲートウェイで FAX コールに使用される 2 種類のパススルー実装を示しています。

図 13-3　シスコの FAX コール用のパススルー実装

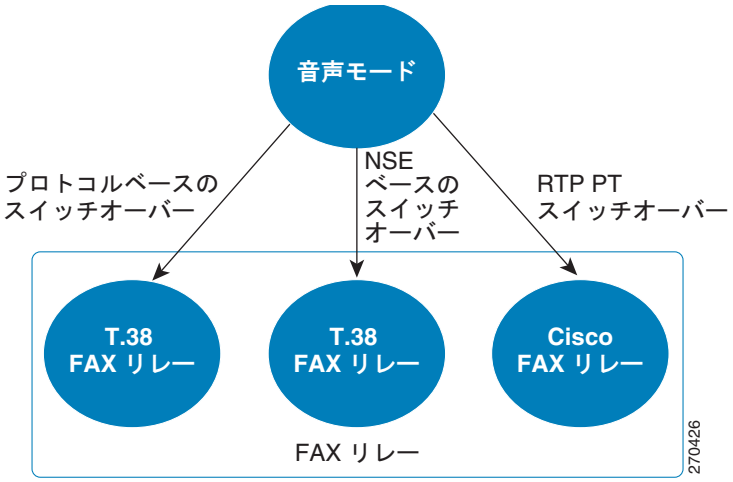


リレーは IP 上で FAX を送信するもう 1 つの主要な方法で、その実装はパススルーに比べて少し複雑です。リレーは、*復調*と呼ばれるプロセスによって FAX 信号からアナログ搬送波を取り除き、FAX HDLC データ フレームを復元します。続いて、これらの HDLC フレームから関連情報を取り出して FAX リレー プロトコルに効率的にパッケージ化し、相手側のゲートウェイに転送します。相手側で受信されると、FAX 情報がリレー プロトコルから取り出されて FAX HDLC フレームに再構築され、アナログ搬送波に変調されて FAX マシンに送信されます。

シスコは、T.38 と Cisco FAX リレーの 2 種類の FAX リレーをサポートしています。ITU 標準の T.38 を使用すると、T.38 仕様をサポートしているサードパーティ製デバイスと Cisco ゲートウェイを相互運用できます。ほとんどの場合、T.38 FAX リレーは呼制御プロトコルを使用して音声モードを T.38 FAX リレー モードに切り替えます（これをプロトコルベースまたは標準ベースの T.38 FAX リレーと呼びます）。ただし、シスコ独自の NSE を使用してモード切り替えを行うように T.38 FAX リレーを設定することもできます（これを NSE ベースの T.38 FAX リレーと呼びます）。サードパーティ製デバイスとの相互運用性を確保するには、プロトコルベースの T.38 を使用する必要があります。

Cisco FAX リレーは標準化前の実装で、Cisco 音声ゲートウェイに固有の機能です。これは、ほとんどすべての Cisco 音声ゲートウェイのデフォルトの FAX 転送設定でもあります。T.38 FAX リレーおよびパススルーで使用される NSE ベースまたはプロトコルベースの方法とは異なり、Cisco FAX リレーは、特定の RTP ダイナミック Payload Types（PT; ペイロード タイプ）を利用して音声モードからリレー モードに移行します。図 13-4 に、シスコの FAX リレー方式を示します。

図 13-4　シスコの FAX コール用のリレー実装



FAX トラフィックの転送に推奨される方法は、FAX リレー モード（もっと具体的に言うと T.38）です。ただし、T.38 FAX リレーがサポートされていない場合は、代わりに Cisco FAX リレーまたはパススルーを使用できます。

ベスト プラクティス

Cisco 音声ゲートウェイで FAX サポートを最大限に実装するには、次の推奨事項とガイドラインが役立ちます。

- QoS を使用する場合は、できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失
  - 遅延
  - 遅延変動（ジッタ）

  IP を経由するすべての FAX 転送は、パケット損失の影響を非常に受けやすくなっています。パケット損失はわずかであっても FAX 障害を引き起こす可能性があります。ネットワークでパケット損失が問題となっている場合は、T.38 FAX リレーの冗長性機能を使用する必要があります。また、ネットワーク上の恒常的なパケット遅延が 1 秒を超えないこと、および遅延変動（ジッタ）が T.38 および Cisco FAX リレーで 300 ミリ秒を超えないことを確認してください。パススルーを使用する場合、ジッタは VoIP 設計のベスト プラクティスに従い、30 ms 以下に抑える必要があります。Cisco Unified Communications ネットワークにおける QoS の実装についての詳細は、次の Web サイトにある『*Enterprise QoS Solution Reference Network Design Guide*』を参照してください。

  http://www.cisco.com/go/designzone

- FAX コールの完全性を確保するには、次のヒントが役立ちます。
  - Call Admission Control（CAC; コール アドミッション制御）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。次の表に、一般的な FAX 転送方式の FAX コール帯域幅使用量の概算値を示します。

FAX 転送方式	帯域幅[1]
モデム パススルーまたは FAX パススルー（G.711）	83 kbps
冗長性のあるモデム パススルー	170 kbps
T.38（冗長性なし）	25 kbps
T.38（高速冗長性レベルの設定値は 1）	41 kbps
T.38（高速冗長性レベルの設定値は 2）	57 kbps
Cisco FAX リレー	48 kbps

1. 帯域幅の値は、イーサネットまたはフレーム リレー L2 ヘッダーを使用した場合の概算値です。T.38 および Cisco FAX リレー帯域幅の値は、FAX ページを 14.4 kbps で送信している間だけ発生し、ピークに達します。

  - モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。
- T.38 FAX リレーは、ネットワークの考慮事項に基づいて最良の FAX パフォーマンスを実現するよう設計されており、FAX トラフィックの転送方法として最も推奨されます。

  他社の T.38 製品との相互運用性を確保する場合は、プロトコルベースの T.38 を使用します。

  特定の Cisco 音声ゲートウェイ（Cisco VG248 やいずれかの Cisco IOS SCCP ゲートウェイなど）と通信する場合は、NSE ベースの T.38 を使用する必要があります。旧バージョンの Unified CM では、プロトコルベースの T.38 のサポートがかぎられているため、代わりに NSE ベースの T.38 FAX リレーを使用することを推奨します。

  Unified CM のシナリオで、さまざまなコール シグナリング プロトコルを実行しているゲートウェイ間に T.38 を導入する場合は、プロトコルベースの T.38 が第一候補です。最新リリースの Cisco Unified CM では、H.323、SIP、および MGCP 呼制御プロトコルを使用するプロトコルベースの T.38 をサポートしています。インストールされている Cisco Unified CM のバージョンでプロトコルベースの T.38 がサポートされていない場合、または SCCP ゲートウェイが関係している場合は、NSE ベースの T.38 を使用します。ご使用のバージョンの Unified CM でプロトコルベースの T.38 がサポートされているかどうかを確認するには、次の Web サイトにある Cisco Unified Communications Manager のリリース ノートを参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html
- T.38 FAX リレーは、現行のほとんどの Cisco 音声ゲートウェイ（特に Cisco IOS を実行しているもの）でサポートされています。詳細については、該当するゲートウェイ モデルの製品データシートを参照してください。
- Error Correction Mode（エラー訂正モード; ECM）は、FAX コールにおいて取り決められた機能です。これによって、FAX ページは確実にエラーなく受信されます。しかし、ECM は、エラーがあれば再送信を試行するため、FAX の送信回数とコール失敗が増えることがあります。必要に応じて、複数の FAX マシンで ECM を無効にするのではなく、ゲートウェイ自体で ECM を無効にすることを検討してください。ただし、パケット ドロップやその他の IP または公衆網の障害が発生した場合、FAX のイメージ品質が低下することがあります。したがって、ECM を無効にするときには、コールの所要時間が長くなったりコールがドロップする代わりに、イメージ品質を損なってもよいかどうかを十分に検討してください。また、ネットワークをモニタおよび評価して、FAX ページのエラーの原因となっている障害を特定し、解決する必要があります。

スーパー G3 FAX のサポート

Super-Group 3（SG3; スーパー G3）分類は、一般には「高速」FAX または V.34 FAX と呼ばれ、V.34 変調を使用して、最大 FAX ページ送信速度を 33.6 kbps に高めます。SG3 FAX マシンは、最大ページ送信速度 14.4 kbps をサポートする標準の G3 FAX マシンとの後方互換性があります。

Cisco IOS Release 12.4.4T 以降を使用する Cisco IOS ゲートウェイは、T.38 または Cisco FAX リレーが設定されているとき、Super Group 3（SG3; スーパー G3）FAX 送信をサポートします。ただし、Group 3 の速度がネゴシエートされる場合だけです。この機能の詳細については、次の Web サイトにある『*Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide, Cisco IOS Release 15.1M&T*』を参照してください。

http://www.cisco.com/en/US/docs/ios/voice/fax/configuration/guide/15_1/vf_15_1_book.html

SG3 高速 FAX を本来の速度で送信する場合は、モデム パススルーを使用する必要があります。Cisco IOS バージョン 15.1.1T のリリースでは、新しい機能により、T.38 FAX リレーによる SG3 FAX のネイティブ サポートが提供されます。

ゲートウェイでのモデム パススルーとモデム リレーのサポート

一般に、音声ゲートウェイを使用して IP ネットワーク上のモデム セッションをサポートするには、次の 3 通りのメカニズムがあります。

- モデム パススルー
- Cisco モデム リレー
- セキュア モデム リレー（STE エンドポイント間の安全な通信）

これらの各メカニズムはいずれもモデム コールを転送できますが、リレー方式は特定のモデム変調方式だけがサポートされているという点で限定的です。これに対し、モデム パススルーは、通常、どのような変調方式でも処理できます。

IP ネットワーク経由でのモデム信号の転送を取り扱う際は、ゲートウェイで発生するモードの切り替えについて理解しておくことが重要です。Cisco ゲートウェイ上のコールはすべて、最初は音声コールとして開始されます。モデム間のコールであっても、まず音声コールとしてセットアップされます。続いて、そのコールが真にモデム コールであるとゲートウェイで認識されると、モードの切り替えが発生して、音声コール モードからモデム パススルー モードまたはモデム リレー モードに切り替わります。音声モードからモデム パススルーまたはモデム リレーへのコールの切り替え方法には、いくつかの種類があります。

「ゲートウェイでの FAX パススルーと FAX リレーのサポート」（P.13-19）の項ですでに説明したように、モデム パススルーでは、独自の NSE パケットまたは H.323/SIP プロトコル スタックを使用して、音声コールをパススルー モードに切り替えます。モデム信号が検出されると、ゲートウェイはこれらの NSE メッセージを使用して、これからモデム コールを送信することを互いに通知できます。また、H.323 または SIP 呼制御プロトコル内の特殊メッセージも使用できます。続いて、モデム信号の転送を適切に処理できるように調整を行います。たとえば、音声コーデックの G.711 へのアップスピード、Voice Activity Detection（VAD; 音声アクティビティ検出）の無効化、エコー キャンセラの無効化などの調整が必要に応じて行われます。モデム パススルーは G.711 コーデックを使用してアナログ モデム信号を単純にサンプリングするため、どのようなモデム変調方式でも処理できますが、常に最高の速度になるとは限りません。

Cisco モデム リレーはシスコ独自の実装で、V.34 モデム コールを IP ネットワーク経由で効率的に転送します。V.90 コールもサポートされますが、V.34 の速度に強制的に減速されます。モデム パススルーと同様に、NSE パケットを使用して、音声モードから Cisco モデム リレーへの切り替えが処理されます。

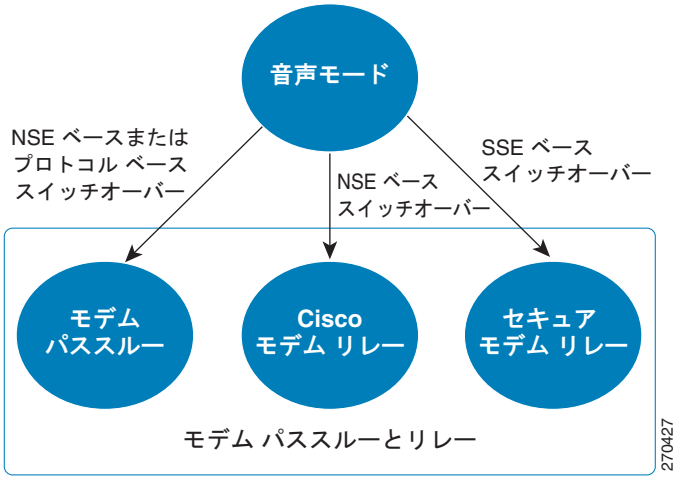
セキュア モデム リレー（「STE エンドポイント間の安全な通信」ともいいます）は、電話コールを IP インフラストラクチャ上で安全に転送できるよう設計されています。Secure Terminal Equipment（STE）と呼ばれる特殊なデバイスにより、V.32 変調を使用して暗号化された音声が伝送されます。セキュア モデム リレーは、SCCP および MGCP ゲートウェイが配置された Unified CM 環境において、STE 間の情報の転送を処理できるようになっています。セキュア モデム リレーは Cisco モデム リレーと互換性がありません。その主な理由の 1 つは、セキュア モデム リレーではモードの切り替えに NSE ではなく V.150.1 ベースの State Signaling Event（SSE）メッセージが使用されることです。

セキュア モデム リレーは STE 信号を転送するために特別に設計されたもので、政府機関または国防関連の配置以外ではほとんど使用されていません。ほとんどの場合、モデム コールの転送には Cisco モデム リレーまたはモデム パススルーを使用します。セキュア モデム リレーの詳細については、次の Web サイトにある「*Secure Communication Between IP-STE Endpoint and Line-Side STE Endpoint*」を参照してください。

http://www.cisco.com/en/US/docs/ios/12_4t/12_4t4/htv1501.html

図 13-5 に、シスコのモデム転送の実装をまとめた図を示します。モデム リレーはモデム パススルーに比べて帯域幅効率が高く、ネットワークの耐障害性にも優れているため、可能な場合は常にモデム リレーを使用してください。モデム リレーの欠点は、サポートされている変調方式がきわめて限定されていることです。それに対してモデム パススルーは、どのようなモデム変調方式でも処理できます。

図 13-5　　シスコのモデム コール用のパススルー実装とリレー実装



ベスト プラクティス

IP インフラストラクチャを介して転送されるモデム トラフィックの最適なパフォーマンスを確保するには、次の推奨ベスト プラクティスを守ってください。

- IP ネットワークで Quality of Service（QoS）が使用可能になっていること、および LAN、MAN、および WAN 環境で、QoS を提供するためのすべての推奨事項に従っていることを確認します。できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失：FAX とモデムのトラフィックには、本質的に損失のない転送が必要です。パケットが 1 つでも損失すると、再送信が行われることがあります。
  - 遅延
  - 遅延変動（ジッタ）

詳細については、次の Web サイトにある『*Enterprise QoS Solution Reference Network Design Guide*』を参照してください。

http://www.cisco.com/go/designzone

- Call Admission Control（CAC; コール アドミッション制御）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。計画の目的で、モデム変調が転送されるかどうかにかかわらず、モデム パススルー コールは常に約 83 kbps の帯域幅を消費するとします。冗長性が有効になっている場合は、170 kbps の帯域幅を消費するとします。モデム通信の性質上、モデム リレー帯域幅は断続的となりますが、V.34 接続の最大速度 33.6 kbps に対して約 45 kbps のピークを見込んで計画します。ここに挙げた帯域幅の値は概算値であり、イーサネットまたはフレーム リレーが L2 トランスポートであることを前提としています。
- 可能な場合は常に、モデム リレーを使用します。変調方式がモデム リレーでサポートされていない場合は、モデム パススルーを使用します。
- IP ネットワークにモデムを接続して、IP ネットワークの問題のトラブルシューティングや診断をしないでください。この場合、IP インフラストラクチャを構成するデバイスのトラブルシューティングに使用されるモデムは、一般電話サービス（POTS）に接続する必要があります。
- Cisco モデム リレーとモデム パススルーでは NSE に基づいてモードが切り替えられるため、異なる呼制御プロトコルを使用しているゲートウェイ同士でも簡単に通信できます。たとえば、Unified CM に接続されている MGCP ゲートウェイと H.323 ゲートウェイは、Cisco モデム リレーまたはモデム パススルーを正常にネゴシエートできます。これは、Unified CM によってすでに設定されている RTP 音声メディア ストリームの中で NSE 切り替えが行われるためです。
- モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。

V.90 サポート

現在、Cisco 機器は V.34 モデムのみをサポートします。V.90 モデムは既存のハードウェアで機能し、V.34 よりも高速ですが、V.90 の完全なサポートは保証できません。

サポートされるプラットフォームと機能

FAX とモデムの機能をサポートしている Cisco プラットフォームは、次のとおりです。

- Cisco IOS ゲートウェイは次のものをサポートします。
  - モデム パススルー。
  - H.323 および SIP プロトコルに基づく FAX パススルー。
  - T.38 FAX リレー。T.38 の NSE ベースの切り替えとプロトコルベースの切り替えがどちらもサポートされます。ただし、SCCP は例外で、NSE ベースの T.38 FAX リレーだけがサポートされます。
  - Cisco FAX リレー。Nextport DSP カードを使用する Cisco AS5350、AS5400、および AS5850 は、Cisco FAX リレーをサポートしていません。また、PVDM3 DSP モジュールも、Cisco FAX リレーをサポートしていません。
  - Cisco モデム リレー。
- IOS 以外の Cisco ゲートウェイは次のものをサポートします。
  - Cisco VG248 は、モデム パススルー、NSE ベースの T.38 FAX リレー、および Cisco FAX リレーをサポートします。
  - Cisco 6608 および 6624 は、モデム パススルーと Cisco FAX リレーだけをサポートします。

– Cisco ATA は、FAX コールについてだけモデム パススルーをサポートします。ATA でモデム コールに対してモデム パススルーを使用することは、正式にはサポートされていません。

（注）　ここに示した FAX とモデムのサポート情報は、Cisco IOS ゲートウェイについては Cisco IOS Release 12.4(9)T 以降、Cisco VG248 Analog Phone Gateway については Release 1.3.1 以降で有効です。

プラットフォーム プロトコルのサポート

企業ソリューションで現在使用されている一般的な呼制御プロトコルには、H.323、SIP、MGCP、および Skinny Client Control Protocol（SCCP）があります。すべての Cisco 音声プラットフォームが、これらのプロトコル、または FAX とモデム機能をすべてサポートしているわけではないので、相互運用性の問題が発生します。また、Cisco 2800 シリーズや Cisco 3800 シリーズなどの Cisco IOS ゲートウェイを、VG248 などの IOS 以外のゲートウェイと組み合せる場合は、さらに相互運用性の問題が発生します。ここでは、FAX、モデム、およびプロトコルの機能の相互運用性をサポートしているゲートウェイの組み合せをリストしています。

ネットワークにおける一般的なプロトコルの組み合せ例としては、MGCP と H.323、SCCP と H.323、SCCP と SIP、MGCP と SIP、H.323 と SIP、SCCP と MGCP などがあります。

表 13-3 では、FAX とモデムの相互運用性を現在サポートしている、プロトコルの組み合せをリストしています。

表 13-3　FAX とモデムの機能がサポートされる呼制御プロトコルの各種組み合せ

プロトコルの組み合せ	モデム リレー	モデム パススルー[1]	T.38 FAX リレー	Cisco FAX リレー	FAX パススルー
MGCP を使用する Unified CM と、H.323 または SIP を使用する Unified CM との組み合せ	あり	あり	あり[2]	あり	なし
MGCP を使用する Unified CM と、MGCP を使用する Unified CM との組み合せ	あり	あり	あり[2]	あり	なし
SCCP と、H.323 または SIP を使用する Unified CM との組み合せ	あり	あり	あり[3]	あり	なし
SCCP と、MGCP を使用する Unified CM との組み合せ	あり	あり	あり[3]	あり	なし
H.323 を使用する Unified CM と、H.323 または SIP との組み合せ	あり	あり	あり[2]	あり	あり
SIP を使用する Unified CM と、H.323 または SIP との組み合せ	あり	あり	あり[2]	あり	あり

1. モデム パススルーは、モデム パススルー コールと FAX パススルー コールの両方で機能します。
2. NSE ベースの T.38 FAX リレーは機能しますが、プロトコルベースの T.38 FAX リレーが機能するかどうかは Unified CM のバージョンによります。バージョン情報については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html にある Cisco Unified Communications Manager のリリース ノートを参照してください。
3. SCCP プロトコルは、NSE ベースの T.38 FAX リレーだけで機能します。

（注）　表 13-3 は一般的な情報を示したものです。製品によっては、この表に記載されていない制限がある場合がありますので、注意してください。たとえば、Cisco ATA は H.323、SIP、および SCCP の呼制御プロトコルをサポートしていますが、どの呼制御プロトコルが使用されているかにかかわらず、モデム パススルーだけがサポートされます。

ゲートウェイ設定例

ここでは、Cisco ゲートウェイでの FAX とモデムのサポートに関する設定の概要を示します。設定情報の詳細については、次の Web サイトで入手可能な『*Cisco IOS Fax, Modem, and Text Support over IP Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/docs/ios/voice/fax/configuration/guide/12_4t/vf_12_4t_book.html

Cisco FAX リレーは、それがサポートされているすべての音声ゲートウェイにおいて、デフォルトで有効になっています。これは明示的に無効にする必要があります。そうしなければ、音声ゲートウェイで検出されたすべての FAX コールについて転送が試行されます。モデム パススルーなどの機能を使用して FAX コールを転送しようとする場合は、ダイヤルピアあるいは **voice service voip** でグローバルに **fax protocol none** を設定することにより、Cisco IOS ゲートウェイ上の Cisco FAX リレーを無効化できます。

Cisco IOS ゲートウェイでのモデム パススルーの設定

モデム パススルーは、次の例に示すように、H.323 ゲートウェイと MGCP ゲートウェイで有効にできます。SIP ゲートウェイでは、H.323 の例と同じコマンドを使用します。また、H.323 および SIP 音声ゲートウェイでも、SCCP 音声ゲートウェイと同様に、**voice service voip** ですべてのダイヤル ピアに対してグローバルにモデム パススルーを有効にできます。

H.323

```
!
! Cisco fax relay is ON by default. It must be explicitly disabled for modem passthrough
! to handle fax calls in addition to high-speed modem calls.
!
dial-peer voice 1000 voip
 fax protocol none
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
!
```

MGCP

```
!
ccm-manager mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
!  no ccm-manager fax protocol cisco
mgcp modem passthrough voip mode nse
mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

Cisco VG248 でのモデム パススルーの設定

Cisco VG248 も Cisco FAX リレーとモデム パススルーをサポートしており、Cisco FAX リレーはデフォルトで有効になっています。Cisco FAX リレーは、VG248 の電話設定の Port specific parameters セクションから有効または無効にできます。

VG248 でモデム パススルーを設定するときは、2 つの重要なパラメータを設定する必要があります。1 つめは、Port specific parameters で **Passthrough mode** を **default: automatic** に設定します。2 つめは、Telephony Advanced settings で **Passthrough signalling** を **IOS mode** に設定します（次を参照）。

```
-----------------------------------------------------------
|                Cisco VG248 (VGC10d8002407)               |
----- -------------------------------------------------------
     | Advanced settings                                    |
     |------------------------------------------------------|
     | Allow last good configuration (enabled)              |
     | SRST policy                   (disabled)             |
     | SRST provider                 ()                     |
     | Call preservation             (enabled: no timeout)  |
     | Media receive timeout         (disabled)             |
     | Busy out off hook ports       (disabled)             |
     | DTMF tone dur ------------------------  100ms)       |
     | Echo cancelli| Passthrough signalling |e: use DSP)   |
     | Passthrough s|------------------------|)             |
     | Hook flash ti| legacy                 | default>)    |
     | Hook flash re| IOS mode               |              |
     | Fax relay max ------------------------  14400 bps)   |
     | Fax relay playout delay       (default: 300)         |
      ------------------------------------------------------
        ---------------------------------------------

-----------------------------------------------------------
|                Cisco VG248 (VGC10d8002407)               |
----- -------------------------------------------------------
     | Advanced settings                                    |
     |------------------------------------------------------|
     | Allow last good configuration (enabled)              |
     | SRST policy                   (disabled)             |
     | SRST provider                 ()                     |
     | Call preservation             (enabled: no timeout)  |
     | Media receive timeout         (disabled)             |
     | Busy out off hook ports       (disabled)             |
     | DTMF tone duration            (default: 100ms)       |
     | Echo cancelling policy        (alternate: use DSP)   |
     | Passthrough signalling        (IOS mode)             |
     | Hook flash timer              (<country default>)    |
     | Hook flash reject period      (none)                 |
     | Fax relay maximum speed       (default: 14400 bps)   |
     | Fax relay playout delay       (default: 300)         |
      ------------------------------------------------------
        ---------------------------------------------
```

FAX とモデム パススルー用のクロック ソーシング

FAX とモデム パススルーを正常に送信するには、クロック信号が重要な役割を果たします。ゲートウェイのクロックは、Stratum クロッキングが提供される公衆網クロックと同期させる必要があります。このクロック同期がないと、FAX およびモデム通信は機能しません。クロックを正しく同期させるには、Cisco IOS ゲートウェイの T1 コントローラに対して次の設定を入力します（この例では、T1 コントローラは、公衆網に接続している音声ゲートウェイです）。

```
!
```

```
controller T1 0
 framing esf
 linecode b8zs
 clock source line
 channel-group 1 timeslots 1-24 speed 64
 !
```

また、公衆網に接続している他のすべてのインターフェイスでも、この設定を入力してください。また、多くの Cisco 音声ゲートウェイには、さまざまなインターフェイスのクロックの基準となり、他のインターフェイスにクロックを伝播する TDM バックプレーンを搭載していることに注意して下さい。これにより、クロッキングの問題の解決がさらに困難になることがあります。

T.38 FAX リレー

T.38 FAX リレーは、Cisco ATA 6608 および 6624 ゲートウェイではサポートされていませんが、Cisco IOS 音声プラットフォームと VG248 ではサポートされています。

T.38 FAX リレーは、次の方法で設定できます。

- 「NSE ベースの T.38 FAX リレー」（P.13-30）
- 「プロトコルベースの T.38 FAX リレー」（P.13-31）

NSE ベースの T.38 FAX リレー

H.323 および SIP に対する NSE ベースの T.38 FAX リレーは、Cisco IOS ゲートウェイで dial-peer レベルで設定するか、**voice service voip** でグローバルに設定します。次の例は H.323 の dial-peer 設定例ですが、同じコマンド構文を SIP ダイヤル ピアにも適用できます。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
 fax protocol t38 nse
!
!
```

MGCP

Cisco IOS MGCP ゲートウェイでは通常、NSE ベースの T.38 FAX リレーのことを「*ゲートウェイによって制御される* T.38 モード」と呼びます。これは、ゲートウェイが NSE メッセージを通じて T.38 の切り替えを制御するためです。ゲートウェイによって制御される T.38 FAX リレーは、コマンド **no mgcp fax t38 inhibit** を使用して有効にします。

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

SCCP ゲートウェイ（Cisco IOS ゲートウェイまたは VG248）では、NSE ベースの T.38 FAX リレーを使用する必要があります。Cisco IOS SCCP ゲートウェイで NSE ベースの T.38 FAX リレーを有効にするには、**voice service voip** でコマンド **fax protocol t38 nse** を設定します。

ゲートウェイで使用されている呼制御プロトコルが異なる場合は、NSE 切り替えを「強制」する必要があります。同じ呼制御プロトコルを使用しているゲートウェイは、コール セットアップ中に、NSE ベースの T.38 FAX リレーがサポートされていることを互いに通知します。異なる呼制御プロトコルが使用されている場合（たとえば、一方のゲートウェイが H.323 を使用していて、他方が MGCP を使用している場合など）は、このような NSE ベースの T.38 FAX リレーの確認情報はゲートウェイ間で渡されません。そのため、NSE ベースの T.38 のサポート通知を受け取らなかった場合でも、NSE ネゴシエーションを強制的に行うようにゲートウェイをプログラムする必要があります。H.323、SIP、および SCCP 音声ゲートウェイでは、これは単に既存の t38 コンフィギュレーション コマンドに **force** オプションを付ける（**fax protocol t38 nse force**）だけで済みます。MGCP では、コマンド **mgcp fax t38 gateway force** を使用します。

プロトコルベースの T.38 FAX リレー

プロトコルベースの T.38 FAX リレーでは、音声モードから T.38 への切り替えは呼制御プロトコル内で行われます。プロトコルベースの T.38 FAX リレーでサポートされている呼制御プロトコルは、H.323、SIP、および MGCP です。H.323 および SIP では、プロトコルベースの T.38 はダイヤル ピア レベルまたは **voice service voip** でグローバルに設定できます。コマンド構文は、**nse** キーワードを省略する点以外は NSE ベースの T.38 FAX リレーと同じです。

NSE ベースの T.38 FAX リレーと、H.323 および SIP 呼制御プロトコルを使用したプロトコルベースの T.38 FAX リレーでは、追加のフォールバック オプションも指定できます。このオプションを使用すると、ゲートウェイ間で初回の FAX 転送方式のネゴシエーションが失敗した場合に、別の切り替え方法、または完全に異なる転送方式を試すことができます。次の例では、H.323 ダイヤル ピアに対してプロトコルベースの T.38 FAX リレーをフォールバック オプション付きで設定しています。コマンド構文は、SIP ダイヤル ピア、および **voice service voip** によるグローバル設定の場合でも同じです。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable protocol-based T.38 fax relay and fall back to Cisco fax relay when
! T.38 fax negotiation fails. This is the default case.
 fax protocol t38 fallback cisco
!
dial-peer voice 1001 voip
 destination-pattern 2T
 session target ipv4:10.10.10.2
 modem passthrough mode nse codec g711ulaw
!
! To enable protocol-based T.38 fax relay and fall back to fax passthrough when
! T.38 fax negotiation fails.
fax protocol t38 fallback pass-through
!
dial-peer voice 1002 voip
 destination-pattern 3T
 session target ipv4:10.10.10.3
 modem passthrough mode nse codec g711ulaw
!
! This CLI enables NSE-based T.38 and it is needed when talking to an MGCP endpoint
! where CA does not support T.38 fax relay, such as with early versions of Unified CM.
```

```
 fax protocol t38 nse force fallback none
!
!
```

MGCP

MGCP 音声ゲートウェイでは、プロトコルベースの T.38 FAX リレーのことを一般に「CA によって制御される T.38 モード」と呼びます。これは、Call Agent（CA; コール エージェント）が T.38 FAX リレーの切り替えを処理するためです。次の例に示すように、MGCP に対して T.38 FAX リレーが有効になっていて、2 つの **fxr-package** コマンドも一緒に設定されていることを確認する必要があります。

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
mgcp package-capability fxr-package
mgcp default-package fxr-package
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

プロトコルベースの T.38 FAX リレーには Unified CM が直接関与するため、ご使用の Unified CM のバージョンがゲートウェイの呼制御プロトコル内で T.38 FAX リレーをサポートしている必要があります。ご使用の Cisco Unified CM のバージョンが特定の呼制御プロトコルで T.38 FAX リレーをサポートしているかどうかを確認するには、次の Web サイトにある Cisco Unified Communications Manager のリリース ノートを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

T.37 Store-and-Forward FAX

Cisco IOS 音声プラットフォームでは T.37 Store-and-Forward FAX がサポートされていますが、これを使用せずに T.38 を使用してサーバを設計することを推奨します。詳細については、「T.38 FAX リレー」（P.13-30）を参照してください。

ビデオ テレフォニー用のゲートウェイ

ビデオゲートウェイは、IP テレフォニー ネットワークまたは公衆網へのビデオコールを終端します。ビデオ ゲートウェイは、ビデオをサポートし、そのコールを H.323 や SIP などのプロトコルを使用して IP ネットワーク上のビデオ コールに変換する ISDN トランクとデータをやり取りする必要がある点で音声ゲートウェイとは異なります。企業は、音声コールとビデオ コールでゲートウェイを分けることを検討することも、音声コールとビデオ コールの両方をルーティングする統合ゲートウェイを設置することもできます。

次の点を考慮することによって、音声とビデオで別々のゲートウェイが必要なのか、統合ゲートウェイが必要なのかを判断できます。

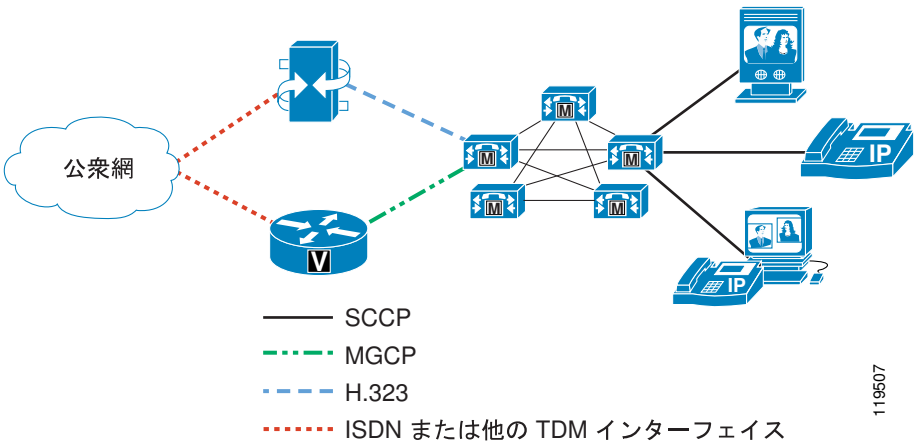
- ダイヤル プラン：ビデオ ユーザ用に別のダイヤル プランを用意できる場合は、既存のエンタープライズ ダイヤル プランを維持しながら、別のビデオ ゲートウェイを使用できます。
- ビデオ ユーザ：主にビデオよりも音声を使用するユーザの方が圧倒的に多い場合は、別のビデオ ゲートウェイを使用してビデオ コール ユーザにサービスを提供することを推奨します。
- ロケーション：多数のビデオ ユーザが地理的に分散している場合は、統合ゲートウェイを使用して総所有コスト（TCO）を削減することを推奨します。
- ビデオ IVR、自動応答、トランク上でのボンディングなどの付加的なビデオ機能：統合ゲートウェイでサポートされない高度な機能をサポートするには、専用ビデオ ゲートウェイが必要です。
- プロトコル：会社の方針や標準に合わせるために、ゲートウェイ プロトコルが重要な要素になる可能性があります。
- キャパシティ：専用ゲートウェイの場合、サポートされる同時コールの量はそれほど大きくない可能性がありますが、統合ゲートウェイでは音声コールに加えてビデオ コールもサポート可能なため、より大きなキャパシティを期待できます。
- デバイス管理：保守、管理、およびトラブルシューティングを容易にしておくことは重要な要素になる可能性があります。専用ゲートウェイはどちらかと言えば管理/設定用のユーザ インターフェイス（GUI）として利用するのに適しており、統合ゲートウェイはトラブルシューティングに使用するのに適しています。ただし、こうした要素は製品によって異なります。

専用ビデオ ゲートウェイ

音声ゲートウェイを含む大規模な音声インフラストラクチャを所有する企業は、ユーザがビデオ コールを PSTN に発信するためのビデオ ゲートウェイを追加できます。Cisco Unified Videoconferencing 3500 および 5200 シリーズ ビデオ ゲートウェイをこの目的に使用できます。

図 13-6 に、音声ゲートウェイ用に既存のプロトコルを使用しており、Unified CM ユーザが音声コールとビデオ コールを PSTN に発信できるようにビデオ ゲートウェイを追加できる、企業での展開の一例を示します。

図 13-6　音声と IP ビデオ テレフォニーに別々の公衆網回線を使用する Unified CM システム



Unified Videoconferencing ゲートウェイはビデオ コール用として優れていますが、シスコ音声ゲートウェイが提供するすべての機能をサポートしているわけではありません。Unified Videoconferencing ゲートウェイには、次の特性があります。

- H.323 と H.320 のみをサポートします。
- スタンドアロン デバイスです。Cisco IOS ルータまたは Cisco Catalyst スイッチに統合することはできません。
- T1/E1-PRI および ISDN BRI のみサポートします。
- H.261、H.263、および H.264 ビデオ コーデックをサポートします。
- G.711、G.722、G.722.1、G.723.1、および G.728 のみ をサポートし、G.729 オーディオはサポートしません。
- H.245 Empty Capabilities Set（ECS）をサポートします。
- T.120 および H.239 データ共有プロトコルをサポートします。
- H.235 暗号化をサポートします。
- Cisco 音声ゲートウェイに固有の、多数の管理機能とトラブルシューティング機能をサポートしません。

このように製品間の違いがあるため、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、Cisco 音声ゲートウェイの代わりとしては推奨できません。IP テレフォニーのユーザが通信環境にビデオを追加するには、両方のタイプのゲートウェイを配置して、すべての音声コールに Cisco 音声ゲートウェイを使用し、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイをビデオ コールのみに使用する必要があります。また、配置する Cisco IOS ゲートウェイのモデルによっては、公衆網サービス プロバイダーから音声とビデオに別個の回線を調達する必要がある場合もあります。

音声ゲートウェイとビデオ ゲートウェイを別々にする場合は（図 13-6 を参照）、着信コールと発信コールの両方に対するルート プランも別々にする必要があります。着信コールの場合、Direct Inward Dial（DID; ダイヤルイン）内線を 1 つしか持たないユーザが音声コールとビデオ コールの両方を受信することはできません。通常、各ユーザは、あらかじめ音声コール用の DID を持っています。そのシナリオにビデオを導入する場合は、何か別の方法でユーザにダイヤルする必要があります。たとえば、別の DID 番号を使用する方法や、ビデオ ゲートウェイのメイン番号にダイヤルし、音声自動応答装置（IVR）から促されてユーザのビデオ内線に入るなどの方法があります。発信コールの場合は、単一の公衆網アクセス コードを音声コールとビデオ コールの両方に使用することができません。通常、ユーザはすでに音声用の既知のアクセス コード（多くの米国企業における 9 など）を持っていますが、そのシナリオにビデオを導入した場合、ビデオ コールを発信するユーザは何か別のアクセス コードをダイヤルする必要があります。

2 つのタイプのゲートウェイを導入するための、もう 1 つの考慮事項は、それらのゲートウェイの配置です。通常、企業は多数の公衆網ゲートウェイ リソースを中央サイト（複数の場合もある）に集約し、それぞれの支社も、いくつかのローカル ゲートウェイ リソースを持っています。たとえば、Cisco Catalyst 6500 ゲートウェイを中央サイトに配置し、そのゲートウェイに複数の T1/E1 回線を接続する一方で、各支社に Cisco Integrated Services Router（ISR）と、ローカル CO へのアナログまたはデジタルのトランクが配備されている場合があります。このシナリオにビデオを導入するユーザは、ビデオに必要な公衆網回線の数と、ビデオ ゲートウェイの配置場所も決定する必要があります。たとえば、少数の Cisco Unified Videoconferencing ビデオ ゲートウェイのみを中央サイトに配置するのか、それとも各支社にもゲートウェイを配置するのか、といったことです。

最後に、トール バイパスを設けるためには IP ネットワーク内でコールをどのようにリモート ゲートウェイへルーティングするのか、および IP ネットワークが使用不能になったり、コールを完了できるだけの帯域幅がない場合に、公衆網上でコールをどのように再ルーティングするのかを考慮してください。具体的には、ビデオ コール用の自動代替ルーティング（AAR）を起動するのか、といったことです。

統合ビデオ ゲートウェイ

企業は、音声とビデオ両方のゲートウェイ機能を備えた統合デバイスを検討できます。このデバイスは、管理対象デバイスの数が少なくなり、ダイヤル プランが単純になるというメリットを企業にもたらします。このゲートウェイは、コールが音声の場合は音声コールとして処理し、コールがビデオの場合はビデオ コールとして処理します。

Cisco IOS Integrated Video Gateway には次のような特徴があります。

- Cisco ISO-13871 ボンディングをサポートします。
- H.320、H.323、および SIP サポートを提供します。
- 既存のビデオ コーデックと H.264 ビデオ コーデックをサポートします。
- さまざまな着信側および発信側変換機能を提供します。
- さまざまなロギングおよびトラブルシューティング機能を提供します。

次の留意点は、Cisco IOS Integrated Video Gateway の展開に適用されます。

- 追加のビデオ コール用の PSTN リンクに必要な容量を考慮してください。
- T.120 などのデータ アプリケーションを使用するためのデバイスが必要かどうかと、IP ネットワークで使用される追加の帯域幅を考慮してください。
- H.320 ゲートウェイでサポートする必要がある会議で使用される遠端カメラ制御や DTMF などの機能が必要かどうかを考慮してください。

公衆網からの着信コールのルーティング

公衆網からの着信コールをルーティングするには、次のいずれかの方法を使用します。

- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。この方法では、外部の（公衆網）発信者はビデオを有効にするために、正しい番号をダイヤルする必要があります。
- ビデオ コールの場合は、外部の発信者にビデオ ゲートウェイのメイン番号をダイヤルしてもらいます。Cisco Unified Videoconferencing ゲートウェイは統合 IVR を提供し、発信者に相手側の内線番号の入力を求めます。次に、Unified CM は、それがビデオ コールであることを認識し、宛先デバイスを呼び出します。この方法では、発信者はそれぞれの着信側ごとに 2 つの異なる DID 番号を覚える必要はありませんが、着信ビデオ コールをダイヤルするという余分な手順が増えます。

（注） 外部のビデオ エンドポイントは、IVR プロンプトに着信側の内線番号を入力するために、DTMF をサポートしている必要があります。

次の例は、2 番めの方法を示しています。

ユーザの Cisco Unified IP Phone 7960 は、Cisco Unified Video Advantage を実行している PC に接続されています。IP Phone の内線番号は 51212 で、完全修飾 DID 番号は 1-408-555-1212 です。DID 番号をダイヤルするだけで、音声専用コールの公衆網からそのユーザに到達できます。CO は、Cisco 音声ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その DID 番号にコールを送信します。ゲートウェイでコールが受信されると、Unified CM はゲートウェイが音声専用であることを認識し、そのコール用に 1 つの音声チャネルのみのネゴシエーションを行います。逆に、公衆網からビデオ コールのためにそのユーザに到達するには、ビデオ ゲートウェイのメイン番号をダイヤルした後、ユーザの内線番号を入力する必要があります。たとえば、1-408-555-1000 をダイヤルするとします。CO は、Cisco Unified Videoconferencing 3500 シリーズ ビデオ ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その番号にコールを送信します。ゲートウェイでコールが受

信されると、IVR プロンプトが発信元に、到達すべき相手の内線番号の入力を求めます。発信者が DTMF トーンで内線番号を入力すると、Unified CM はゲートウェイにビデオ機能があることを認識し、そのコール用に音声とビデオの両方のチャネルをネゴシエートします。

ゲートウェイの番号操作

Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、公衆網から受信したコールの番号を操作できません。Q.931 Called Party Number フィールドで渡されたものと正確に同じ数の番号を受け取り、それらすべてを Unified CM に送信します。したがって、Unified CM は番号を操作して、宛先デバイスの電話番号（DN）と照合する必要があります。たとえば、CO スイッチからゲートウェイへの回線が 10 桁を渡すように設定されていて、着信側の内線番号が 5 桁しかない場合、Unified CM は、一致する DN を検索する前に、先頭の 5 桁を削除する必要があります。この番号操作は、次のいずれかの方法で実装できます。

- Cisco Unified Videoconferencing ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランク上で Significant Digits フィールドを設定します。

  この方法では、Unified CM に、着信番号の下位 N 桁だけに注目するよう指示できます。たとえば、Significant Digits を 5 に設定すると、Unified CM は着信番号の最後の 5 桁以外を無視します。これは最も簡単な方法ですが、そのゲートウェイから受信したすべてのコールに影響を及ぼします。したがって、可変長の内線番号がある場合、この方法は推奨できません。

- トランスレーション パターンを設定し、それを Cisco Unified Videoconferencing ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランクのコーリング サーチ スペースに格納します。

  この方法では、Unified CM は受信した完全な桁数でコールを照合し、着信番号を修正してから、得られた変更後の番号に対して番号分析を続行できます。この方法は前の方法に比べてわずかながら複雑ですが、柔軟性があり、コールの照合と修正をきめ細かく行うことができます。

公衆網への発信コールのルーティング

発信コールを公衆網へルーティングするには、次のいずれかの方法を使用します。

- 音声コールとビデオ コールに異なるアクセス コード（異なるルート パターン）を割り当てます。たとえば、ユーザが 9 の後にコール先の公衆網電話番号をダイヤルすると、それがコールを音声ゲートウェイに送るルート パターンと一致します。同様に、数字の 8 を、ビデオ ゲートウェイにコールを渡すルート パターンとして使用することもできます。
- Unified CM クラスタ内にあるビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。その後、2 つの回線に異なるコーリング サーチ スペースを指定します。ユーザが第 1 の回線上でアクセス コード（たとえば 9）をダイヤルすると音声ゲートウェイにつながり、同じアクセス コードを第 2 の回線上でダイヤルするとビデオ ゲートウェイにつながります。この方法では、ユーザが 2 つの異なるアクセス コードを覚える必要がありませんが、コールの発信時に電話機で正しい回線を押す必要があります。

ゲートウェイ サービス プレフィックス

Cisco Unified Videoconferencing ゲートウェイは、発信コールの速度を定義するためにサービス プレフィックスを使用します。ゲートウェイでサービス プレフィックスを設定するときは、次のいずれかの速度を選択する必要があります。

- Voice-only
- 128 kbps
- 256 kbps
- 384 kbps

- 768 kbps
- Auto（動的に決定され、128 kbps ～ 768 kbps の範囲の任意のコール速度をサポート）

（注）　上記の各速度は、64 kbps の倍数を表します。56 kbps のダイヤリング用として、サービス プレフィックスの設定ページには、各チャネルを 56 kbps に制限するチェックボックスがあります。したがって、制限モードを有効にした 128 kbps サービスは 112 kbps サービスになり、制限モードを有効にした 384 kbps サービスは 336 kbps になり、その他も同様です。

IP エンドポイントから公衆網へ向かうコールは、ゲートウェイがそのコールにどのサービスを使用するかを決定できるように、着信番号の先頭にサービス プレフィックスを含んでいる必要があります。オプションとして、番号の先頭にサービス プレフィックスを含んでいないコールに使用する、デフォルト プレフィックスを設定できます。この方法は、非常に複雑になる可能性があります。ユーザは、求めるコール速度を得るためにダイヤルすべきプレフィックスを覚えておく必要があるからです。また、管理者は、Unified CM で複数の（速度ごとに 1 つずつ）ルート パターンを設定する必要があります。ただし、Auto 速度を使用するとその手間を最小にできます。コールの大多数が 1 チャネルあたり 64 kbps（たとえば、128 kbps、384 kbps、512 kbps、768 kbps など）を使用して行われる場合には、Auto サービスを使用できます。その場合、1 チャネルあたり 56 kbps（たとえば、112 kbps、336 kbps など）のコールを行うまれなケースに備えて、1 つだけ別のサービスを作成すれば済みます。

ゲートウェイは、# をダイヤル末尾の文字として認識するので、サービス プレフィックスの中に必ず # 文字を使用することを推奨します。この文字をサービス プレフィックスに入れておくと、ゲートウェイのメイン番号をダイヤルして IVR に接続してからオフネット番号にダイヤルするといった料金詐欺にゲートウェイが使用されることを防止できます。# は、サービス プレフィックスの先頭（推奨）と末尾どちらでもかまいません。たとえば、ビデオ コールで公衆網に到達するためのアクセス コードが 8 であれば、サービス プレフィックスを #8 または 8# として設定することを推奨します。あるいは、上記のように 2 つのサービス プレフィックスを使用する場合は、Auto の 64 kbps サービスに #80 を使用し、Auto の 56 kbps サービスに #81 を使用するという方法もあります。

サービス プレフィックスを使用する場合の欠点は、Cisco Unified Videoconferencing ゲートウェイにコールを送信するときに、Unified CM で着信番号の前にサービス プレフィックスを付加する必要があることです。ユーザに # をダイヤルさせるのはあまり使いやすくないので、ダイヤルされた番号の前に Unified CM が # を付加するように設定することを推奨します。たとえば、公衆網にビデオ コールをダイヤルするアクセス コードが 8 の場合、Unified CM でルート パターンを 8.@ として設定し、ルート パターン設定の中で、そのルート パターンがダイヤルされたときは必ず前に #8 を付加するように、着信番号変換ルールを設定します。あるいは、上記のようにサービス プレフィックスを 2 つ使用する場合は、80.@ を Auto 64 kbps サービス（着信番号の前に # を付ける）に使用し、81.@ を Auto 56 kbps サービス（着信番号の前に # を付ける）に使用するという方法もあります。

自動代替ルーティング（AAR）

IP ネットワークにコールを処理できるだけの帯域幅がない場合、Unified CM はコール アドミッション制御メカニズムを使用して、コールの処理方法を決定します。「IP ビデオ テレフォニー」（P.12-1）の説明のように、Unified CM は設定に従って、次のいずれかの処理を実行します。

- コールに失敗し、発信側に対してビジー トーンを再生し、発信側の画面に Bandwidth Unavailable メッセージを表示します。
- ビデオ コールを音声専用コールとして再試行します。
- Automated Alternate Routing（AAR; 自動代替ルーティング）を使用し、公衆網ゲートウェイなどの代替パス上でコールを再ルーティングします。

最初の 2 つのオプションについては、「IP ビデオ テレフォニー」（P.12-1）の章に説明があります。ここでは、AAR オプションについて説明します。

音声コールまたはビデオ コールに AAR を使用できるようにするには、発信側デバイスと着信側デバイスを AAR グループのメンバーとして設定し、着信側デバイスに外部電話番号マスクを設定する必要があります。外部電話番号マスクによって、ユーザの内線用の完全修飾 E.164 アドレスが指定されます。また、AAR グループによって、コールが公衆網上で正しくルーティングされるために、着信側デバイスの外部電話番号マスクの前に付加すべき数字が示されます。

たとえば、ユーザ A が San Jose AAR グループに属し、ユーザ B が San Francisco AAR グループに属しているとします。ユーザ B の内線番号は 51212 で、外部電話番号マスクは 6505551212 です。AAR グループは、San Jose と San Francisco の AAR グループ間のコールに対して、番号の前に 91 を付加するよう設定されています。この場合、ユーザ A が 51212 をダイヤルし、2 つのサイト間の IP WAN 上にそのコールを処理できるだけの帯域幅がない場合、Unified CM はユーザ B の外部電話番号マスクである 6505551212 を選択し、その前に 91 を付加して 916505551212 への新規コールを生成し、ユーザ A 用の AAR コーリング サーチ スペースを使用します。

ビデオ コールにも同じロジックが適用されますが、プロセスに 1 つだけ手順が追加されます。ビデオ対応デバイスに対して、Retry Video Call as Audio というフィールドが存在します。「IP ビデオ テレフォニー」（P.12-1）の章で説明するように、このオプションを有効（オン）にした場合、Unified CM は AAR を実行しないで、同じコール（つまり、51212 へのコール）を音声専用コールとして再試行します。このオプションを無効（オフ）にした場合、Unified CM は AAR を実行します。Unified CM のデフォルトでは、すべてのビデオ対応デバイスで Retry Video Call as Audio オプションが有効（オン）になります。したがって、ビデオ コールで AAR を使用できるようにするには、Retry Video Call as Audio オプションを無効（オフ）にする必要があります。また、ロケーション間で Resource Reservation Protocol（RSVP; リソース予約プロトコル）に基づいたコール アドミッション制御ポリシーが使用されている場合は、RSVP ポリシーを音声ストリームとビデオ ストリームの両方について Mandatory に設定する必要があります。

さらに、Unified CM は、着信側デバイスだけを見て Retry Video Call as Audio オプションが有効か無効かを判断します。したがって、上記のシナリオで AAR プロセスが実行されるためには、ユーザ B の電話機で Retry Video Call as Audio オプションが無効にされている必要があります。

最後に、デバイスは 1 つの AAR グループだけに所属できます。AAR グループによって、どの数字を前に付加するかが決定されるため、再ルーティングされたコールにどのゲートウェイが使用されるかにも影響があります。前項で述べたように、公衆網への発信コール ルーティングの設定に何を選択したかに応じて、AAR によって再ルーティングされるビデオ コールは、ビデオ ゲートウェイでなく音声ゲートウェイに送られる可能性もあります。したがって、AAR グループと AAR コーリング サーチ スペースの構築は入念に行い、必ず正しい数字が付加され、AAR に正しいコーリング サーチ スペースが使用されるようにしてください。

こうした考慮事項により、大規模な企業環境での AAR の設定がかなり複雑になる可能性がありますが、エンドポイントのタイプが 2 つのどちらかに限定されている場合（IP Phone が音声専用コール用で、Tandberg T-1000 などのシステムがビデオ コール専用など）には AAR の実装が容易です。エンドポイントが音声とビデオの両方のコールに対応している場合（Cisco Unified Video Advantage または Cisco IP Video Phone 7985G など）は、AAR の設定が非常に複雑になることがあります。したがって、音声とビデオのエンドポイントが混在する大企業では、ユーザごとに AAR の重要性をよく考え、専用のビデオ会議室や経営幹部用ビデオ システムなど、一部のビデオ デバイスだけに AAR を使用してください。表 13-4 に、さまざまなデバイス タイプで AAR を使用するのが適切なシナリオのリストを示します。

表 13-4　デバイス タイプ別の AAR 使用条件

デバイス タイプ	デバイスを使用したコールの宛先	AAR の必要性	備考
IP Phone	他の IP Phone およびビデオ対応デバイス	あり	ビデオ対応デバイスにコールするときでも、発信元デバイスが音声専用なので、コールを音声ゲートウェイにルーティングするように AAR を設定できます。
Cisco Unified Video Advantage の搭載された IP Phone、または Cisco IP Video Phone 7985G	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
Sony 社製または Tandberg 社製の SCCP エンドポイント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
H.323 または SIP クライアント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。

最低料金選択機能

Least-Cost Routing（LCR; 最低料金選択機能）と Tail-End Hop-Off（TEHO; テールエンド ホップオフ）は、VoIP ネットワークでは非常によく知られており、ビデオ コールにも利用できます。一般的にどちらの用語も、長距離電話番号へのコールが IP ネットワークを通じて宛先に最も近いゲートウェイにルーティングされ、通話料金が安くなるような、コール ルーティング ルールの設定方法を指しています。Cisco Unified CM Release 4.1 の場合、LCR は基本的に TEHO と同じ意味です。Unified CM は、次に示すような豊富な番号分析機能と番号操作機能を使用して、この機能をサポートします。

- パーティションとコーリング サーチ スペース
- トランスレーション パターン
- ルート パターンとルート フィルタ
- ルート リストとルート グループ

LCR をビデオ コール用に設定するのは、音声コールの場合よりも少し複雑で、その理由は次のとおりです。

- この章ですでに述べたように、ビデオ コールには独自の専用ゲートウェイが必要です。
- ビデオ コールには、音声コールをはるかに上回る帯域幅が必要です。

専用ゲートウェイに関しては、LCR をビデオ コールに使用するかどうかを決めるための基礎となるロジックは、「自動代替ルーティング（AAR）」（P.13-37）の項で説明したロジックとほとんど同じです。音声とビデオ用にさまざまなタイプのゲートウェイが必要になるため、LCR で音声コールを 1 つのゲートウェイに送り、ビデオ コールを別のゲートウェイに送るために必要なすべてのパーティション、コーリング サーチ スペース、トランスフォーメーション パターン、ルート パターン、ルート フィルタ、ルート リスト、およびルート グループを設定するのは、かなり複雑な作業になる可能性があります。

帯域幅の要件に関しては、LCR を使用するかどうかは、特定のロケーションとの間を結ぶビデオ コールの LCR をサポートできるだけの帯域幅が、使用している IP ネットワークにあるかどうかで決まります。現在の帯域幅が十分でない場合は、IP ネットワークをアップグレードしてビデオ コール用の空きを作ったり、ローカル ゲートウェイを導入して公衆網上でコールをルーティングしたりするためのコストと、ビデオ コールの利点を比較する必要があります。たとえば、ある中央サイトに 1.544 Mbps の T1 フレーム リレー回線を介して支店が接続されているとします。その支店内には、20 人のビデオ機能を持つユーザがいます。1.544 Mbps の T1 回線は、最大でほぼ 4 つの 384 kbps ビデオ コールを処理できます。この場合、中央サイトまでビデオ コールをルーティングして、通話料金を節約することに意味があるかどうかが問題です。サポートするコールの数に応じて、1.544 Mbps の T1 回線をもっと高速のものにアップグレードしなければならない場合もあります。ビデオには、そうしたアップグレードに要する毎月の追加料金に見合うだけの重要性があるのでしょうか。ない場合は、その支店に Cisco Unified Videoconferencing ゲートウェイを導入すると、LCR に煩わされずに済みます。ただし、支店ごとにローカル Cisco Unified Videoconferencing ゲートウェイを配置すれば費用がかかるため、最終的には、ビデオと PSTN 間のコールがビジネスにどれほど重要かを判断する必要があります。ビデオが重要でない場合は、帯域幅をアップグレードしたりビデオ ゲートウェイを購入したりするよりも、Retry Video Call as Audio 機能を使用し、使用可能な帯域幅を超過した場合にビデオ コールを音声専用コールとして再ルーティングした方がよいこともあります。コールが音声専用までダウングレードされると、LCR を実行するためのローカル ゲートウェイ リソースと帯域幅は、もっと手ごろな価格で設定しやすいものになります。

ISDN B チャネル バインディング、ロールオーバー、およびビジーアウト

Cisco IOS Release 12.4.20T 以降のリリースでは、Cisco IOS H.320 ゲートウェイで ISO-13871 ボンディング手法がサポートされており、これによって最大速度 1 Mbps のビデオ コールがサポートされます。この機能により、Cisco IOS ルータを音声コールとビデオ コールの両方に対応する統合ゲートウェイとして使用できます。

H.320 ビデオは、複数の ISDN チャネルをまとめて使用することで、フルモーション ビデオの受け渡しに必要な速度を実現します。このボンディング メカニズムの問題の 1 つは、着信 ISDN ビデオ コールを受信した時点でゲートウェイにはそのコールに必要なチャネル数がわからず、コールを受け入れて発信元デバイスから必要な追加チャネル数を指示されて、初めてそれがわかることです。その要求を満たせるだけの B チャネルがないと、コールは切断されます。したがって、そのような状況が発生する可能性を最小にするよう、慎重なトラフィック エンジニアリングが必要です。基本的に、次に着信する可能性があるコールを処理できる、十分な B チャネルを常に使用可能にしておく必要があります。

この B チャネルの問題は、次の 2 つのケースで発生します。

- 公衆網から IP ネットワークへの着信コール
- IP ネットワークから公衆網への発信コール

着信コール

着信コールについて、次のシナリオを考えてみます。

ある会社に Cisco Unified Videoconferencing 3527 ゲートウェイがあり、それが ISDN PRI 回線でセントラル オフィス（CO）のスイッチに接続されています。この場合、ISDN PRI 回線は 23 の B チャネルを提供します。ビデオ コールが公衆網から 384 kbps で受信されます。このコールは 6 つの B チャネルを使用するので、残りの空きは 17 になります。最初のコールがまだアクティブな間に、第 2 と第 3 の 384 kbps のコールがその回線上で受信されます。それぞれのコールが 6 チャネルを使用するので、残りの空きは 5 チャネルになります。第 4 の 384 kbps のコールが受信されると、ゲートウェイはそのコールに応答しますが、十分な B チャネルの空きがないこと（残りチャネルは 5 つだけだが、コールに必要なチャネルは 6 つ）を認識し、接続を解除します（「16: Normal Call Clearing」を理由とした Q.931 RELEASE COMPLETE を送信）。第 4 のコールを試みた発信側は、コールの失敗の原因がわからず、番号を繰り返しリダイヤルしてコールを発信しようとします。

Cisco Unified Videoconferencing ゲートウェイでは、こうした問題が起きる可能性を最小にするために、ゲートウェイが一定の使用率しきい値（総帯域幅に対するパーセンテージとして設定）に到達したときに、ゲートウェイから CO へ残りの B チャネル（この例では 5 チャネル）をビジーアウトする要求を送信するように設定できます。

さらに、トランク グループ内で CO から複数の ISDN 回線をプロビジョニングできます。最初の回線がビジーアウトしきい値に到達した時点で、コールはグループ内の次の PRI へロールオーバーされます。Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは 2 本の ISDN PRI 接続を提供し、両方のポートにまたがるボンディング チャネルをサポートします。たとえば、ポート 1 の空きが 5 チャネルしかなく、ポート 2 がアイドル状態であるため、23 チャネルが使用可能であるとします。この場合、ポート 1 から 5 チャネル、ポート 2 から 1 チャネルを使用してボンディングすることにより、第 4 の 384 kbps のコールに成功できます。これにより、コントローラ 2 上に残る空きは 22 チャネルとなり、ある時点で着信コールが再びビジーアウトしきい値に到達します。その時点で、ポート 2 上の残りのチャネルはビジーアウトされ、それ以後のすべての着信コールは原因コード「Network Congestion」で拒否されます。Cisco Unified Videoconferencing ゲートウェイでは、複数のゲートウェイにまたがってチャネルを結合したり、同じ Cisco 3545 シャーシ内の複数の Cisco 3500 シリーズ ゲートウェイ モデルにまたがってチャネルを結合したりすることができないため、ボンディングできる最大ポート数は 2 つです。CO スイッチは、トランク グループ内の第 3 または第 4 の PRI にコールをロールオーバーできます（ほとんどの CO が最大 6 回線のトランク グループをサポートしています）が、たとえば、PRI 番号 1 と PRI 番号 2 の間でチャネルをボンディングできても、PRI 番号 1 と PRI 番号 3 の間でボンディングすることはできません。

上記のビジーアウト ロジックは、すべてのコールが同じ速度で行われることを前提としています。たとえば、あるポート上で 384 kbps の 2 つのコールがアクティブなときに、128 kbps のコールが着信したとします。このコールは 2 チャネルしか使用しないため、3 つのコールに合計 14 チャネル（6+6+2 = 14）が使用され、回線上に 9 チャネルの空きが残ります。ところが、ビジーアウトしきい値が（すべてのコールが 384 kbps で行われると想定して）18 チャネルに設定されていると、このビジーアウトしきい値でまだ使用可能なチャネルは 4 つだけになります。この時点で別の 384 kbps のコールが着信すると、そのコールは、残りの 4 チャネルではコールのサポートに不十分なため、失敗します。また、18 チャネルというビジーアウトしきい値にまだ達していない（14 チャネルしか使用されていない）ので、回線はビジーアウトされず、コールは次の回線にロールオーバーされません。この状態は、既存のコールの 1 つが切断されるまで続きます。このような状況を避けるため、すべてのコールを単一のコール速度に標準化できるようにすることが重要です。

発信コール

発信コールでも着信コールと同じ状況が起きる可能性がありますが、ビジーアウトの発生の仕方は異なります。Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、Resource Availability Indicator および Resource Availability Confirm（RAI/RAC）というメッセージをサポートしています。RAI/RAC メッセージは H.225 RAS 仕様で定義されており、ゲートウェイが満杯でコールをそれ以上ゲートキーパーにルーティングできないことを、ゲートウェイからゲートキーパーに伝えるために使用されます。ゲートウェイはビジーアウトしきい値に達すると、ステータスが True の RAI メッセージをゲートキーパーに送信します。True は「これ以上のコールの送信不可」を意味し、False は「送信可」を意味します。ゲートウェイは、ビジーアウトしきい値を下回るとすぐに RAI=False を送信します。発信コールのビジーアウトしきい値は着信コールのビジーアウトしきい値とは別のもので、それぞれ別々に設定できるので、着信コールを次の空き回線にロールオーバーしても発信コールは引き続き受け入れられ、その逆も同様です。たとえば、RAI しきい値を 12 チャネルに設定し、ISDN ビジーアウトしきい値を 18 チャネルに設定できます。その場合、384 kbps の 2 つのコールがアクティブのとき、発信コールは次の空きゲートウェイにロールオーバーされますが、3 番めの 384 kbps の着信コールは引き続き受け入れられます。同じように効率的に発信コールのビジーアウト フェールオーバーを実現する方法として、RAI/RAC 方式ではなく、次項で述べるように Unified CM のルート グループとルート リストの構造を使用する方法があります。

Unified CM でのゲートウェイの設定

Unified CM では、次のいずれかの方法で Unified Videoconferencing ゲートウェイを設定できます。

- H.323 ゲートウェイとして設定し、Unified CM でコールをそのゲートウェイに直接ルーティングします。
- ゲートキーパーへの H.225 ゲートキーパー制御トランクを設定し、ゲートキーパーを通じてそのゲートウェイにコールをルーティングします。

ゲートウェイが 1 つだけであれば、多くの場合、トランクを介してゲートウェイに到達するよりも、Unified CM で直接設定した方が簡単です。ロード バランシングと冗長性を得るために複数のゲートウェイを使用している場合は、それらのゲートウェイをすべて Unified CM で設定し、ルート グループとルート リストの中に配置する方法があります。または、ゲートキーパーへの H.225 トランクを設定してゲートウェイ間の RAI/RAC を使用し、コールの送信先となるゲートウェイをゲートキーパーが Unified CM に指示するように設定する方法があります。

公衆網から Unified CM への着信コールの場合、各 Cisco Unified Videoconferencing ゲートウェイを 1 つのゲートキーパーに登録する方法と、それらのゲートウェイを、すべての着信コール要求の送り先とする最大 3 台の Unified CM サーバの IP アドレスを使用して設定する方法があります。この方法は、ピアツーピア モードと呼ばれます。どちらの方法でも最終的な目標は、各ゲートウェイが受信したすべての着信コールを Unified CM に送り、Unified CM がコールのルーティング方法を決定できるようにすることです。コールをゲートウェイから Unified CM にルーティングするようゲートキーパーを設定する方法の詳細については、「ゲートキーパー」（P.12-25）を参照してください。

コール シグナリング ポート番号

デフォルトでは、Cisco Unified Videoconferencing ゲートウェイは、ウェルノウン ポート 1720 の代わりに TCP ポート 2720 を監視します。ただし、同様にデフォルトで、Unified CM は H.323 コールをポート 1720 に送信します。ゲートウェイで監視するポートは変更できます。また、Unified CM からの送信先ポートを Unified CM の H.323 ゲートウェイ デバイス設定で変更することもできます。いずれの方法でも、ゲートウェイへの発信コールが成功するためには、両側で一致している必要があります。

着信方向では、Cisco Unified Videoconferencing ゲートウェイは、ピアツーピア モードで動作するように設定された場合、コールをポート 1720 で Unified CM に送信します。ゲートキーパーに登録するように設定された場合、Unified CM は、ランダムに生成されたポート番号をすべてのゲートキーパー制御トランクに使用します。この方法では、Unified CM が同じゲートキーパーに対して複数のトランクを持つことができます。このポート番号は、Unified CM からゲートキーパーへの Registration Request（RRQ）に含まれているため、ゲートウェイから Unified CM への着信 H.225 セットアップ メッセージは、このポート番号に送られます。ただし、ゲートウェイが Unified CM で H.323 ゲートウェイ デバイスとして直接設定されている場合、Unified CM はコールが H.225 トランクの TCP ポートに着信したことを無視し、発信元 IP アドレスをデータベースに設定されている H.323 ゲートウェイ デバイスと照合します。一致するデバイスが見つからない場合、Unified CM はそのコールがトランクに着信したかのように扱います。

発信方向に関しては、Unified CM がゲートキーパー制御 H.225 トランクを使用してゲートウェイに到達している場合は、ゲートキーパーが Unified CM に、どの TCP ポートを使用してゲートウェイに到達すべきかを知らせます。ゲートウェイが Unified CM で H.323 ゲートウェイ デバイスとして設定されている場合（ピアツーピア モード）、Unified CM は、ポート 2720（デフォルト）か 1720（ゲートウェイで監視ポートが変更された場合）にコールを送るように設定されている必要があります。

コール シグナリング タイマー

H.320 ボンディングに固有の遅延のため、ビデオ コールは音声コールよりも接続に時間がかかる場合があります。Unified CM のいくつかのタイマーは、デフォルトで音声コールをできるだけ高速に処理するように調整されているため、それが原因でビデオ コールが失敗する場合があります。したがって、H.320 ゲートウェイ コールをサポートするには、次のタイマーをデフォルト値から変更する必要があります。

- H.245TCSTimeout
- Media Exchange Interface Capability Timer
- Media Exchange Timer

これらの各タイマーを、Unified CM Administration の Service Parameters で 25 まで増やすことを推奨します。このパラメータは、クラスタ全体のサービス パラメータなので、既存の H.323 Cisco 音声ゲートウェイへの音声コールも含めて、あらゆるタイプの H.323 デバイスへのコールに影響を与えることに注意してください。

音声ゲートウェイのベアラ機能

H.323 コールは、どのタイプのコールを行うかを示すために、H.225/Q.931 Bearer Capabilities Information Element（bearer-caps）を使用します。音声専用コールでは、bearer-caps が「speech」または「3.1 KHz Audio」に設定され、ビデオ コールでは bearer-caps が「Unrestricted Digital Information」に設定されます。一部のデバイスでは、Unrestricted Digital Information の bearer-caps をサポートしていません。Unified CM が H.323 ビデオ コールとしてコールを試みると、これらのデバイスへのコールは失敗する場合があります。

Unified CM は、次の要因に基づいて、どの bearer-caps を設定するかを決定します。

- 発信側デバイスまたは着信側デバイス（あるいはその両方）がビデオ対応かどうか
- それらのデバイス間のコールにビデオを許可するように Unified CM のリージョンが設定されているかどうか

Unified CM では、ビデオ コールをオーディオとして再試行する機能をサポートしており、この機能は設定を介して有効にできます。Unified CM がビデオ コールの bearer-caps を「Unrestricted Digital」に設定し、コールが失敗すると、Unified CM は同じコールの bearer-caps を「speech」に設定したオーディオ コールとして再試行します。

H.323 を使用する場合、Cisco IOS ゲートウェイは、コールの設定で受信するベアラ機能に基づいて、コールを音声またはビデオとして処理できます。SIP を使用する場合、ゲートウェイはコールのネゴシエーションのため、ISDN 機能を SDP に変換します。

Cisco 音声ゲートウェイが Unified CM との通信に MGCP を使用している場合、この問題は発生しません。それは、Unified CM の MGCP プロトコル スタック上ではビデオがサポートされておらず、しかも、MGCP モードでは、Unified CM が公衆網への D チャネル シグナリングを完全に制御するためです。

CHAPTER 14

Cisco Unified CM トランク

トランクとは、Cisco Unified Communications Manager（Unified CM）における通信チャネルであり、Unified CM はトランクを使用することによって他のサーバと接続できます。1 つ以上のトランクを使用して、音声コール、ビデオ コール、および暗号化されたコールの送受信やリアルタイム イベント情報の交換など、Unified CM から呼制御サーバおよびその他の外部サーバとのさまざまな通信を行うことができます。

トランクは、Cisco Unified Communications 配置における重要かつ不可欠な部分であるため、利用可能なトランクの種類、それらの機能、および復元性、容量、ロード バランシングなどの設計と配置上の考慮事項について理解することが重要となります。

Unified CM で設定できる基本的なトランクには、次の 2 種類があります。

- SIP トランクと H.323 トランク。いずれも、外部通信に使用できます。
- Intercluster Trunk（ICT; クラスタ間トランク）。

この章では、これらのトランクの一般的な機能および特徴について説明します。Unified CM トランクの特定用途の詳細については、このマニュアルのその他の関連する章を参照してください。

この章では、次のトピックについて説明します。

Unified CM トランクの用途の詳細については、次に示す章の各項を参照してください。

- 「Unified Communications の配置モデル」（P.5-1）
- 「メディア リソース」（P.17-1）
- 「コール アドミッション制御」（P.11-1）
- 「IP ビデオ テレフォニー」（P.12-1）
- 「Cisco Unified Presence」（P.23-1）

この章の新規情報

表 14-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 14-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

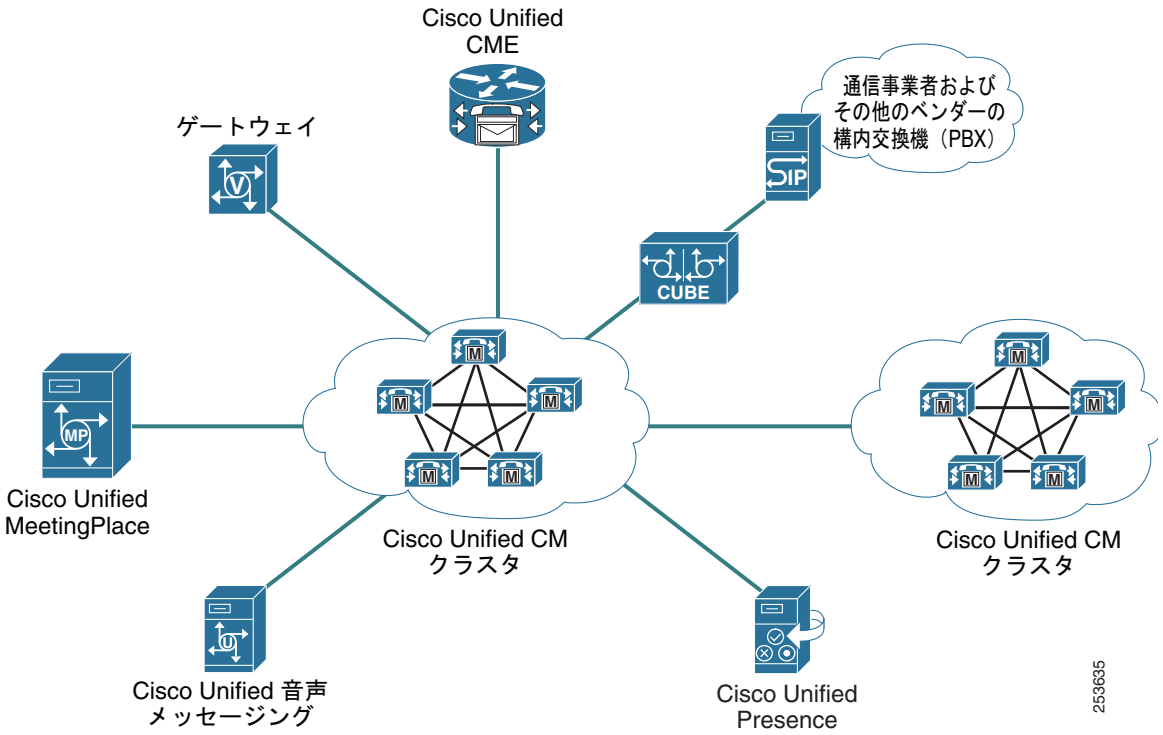
新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 6 月 2 日
SIP ディレイド オファーおよびアーリー オファーに関する推奨事項	「SIP ディレイド オファーおよびアーリー オファー」（P.14-20） 「SIP トランクの概要」（P.14-6）の各項で説明	2011 年 1 月 31 日
Cisco Unified CM Session Management Edition	「トランクの集約プラットフォーム」（P.14-61）	2010 年 11 月 15 日
H.323 トランク機能の強化と操作	「H.323 トランクの概要」（P.14-37）	2010 年 11 月 15 日
SIP トランク機能の強化と操作	「SIP トランクの概要」（P.14-6）	2010 年 11 月 15 日
Cisco Unified CM IP-PSTN 接続モデル	「トランク IP-PSTN 接続モデル」（P.14-64）	2010 年 4 月 2 日
リージョン間のコーデック選択	「Cisco Unified CM トランクおよび緊急サービス」（P.14-59）	2010 年 4 月 2 日
SIP トランク サービス タイプ	「SIP トランク サービス タイプ」（P.14-27）	2010 年 4 月 2 日

Unified CM トランク ソリューション アーキテクチャ

Unified CM では、IP トランクのメカニズムを使用して、Unified Communications ソリューションの他のコンポーネントとコール関連情報を交換します。この点においてトランクは重要であるため、プロトコル、期待される機能およびサービス、パフォーマンス要件などを適切に考慮して IP トランクのシステム アーキテクチャを開発することが重要です。

図 14-1 に、システムの接続性の観点から IP トランクの役割を示します。この図には、Unified CM クラスタからのすべての接続が示されているわけではありません。

図 14-1　IP トランクによって提供される Unified CM への接続



コールは、ダイヤル プランでの定義に従って、ルート パターン コンストラクトを使用してトランクに転送されます。ルート パターンでは、直接トランクを使用することも、ルート リストを通してトランクを使用することもできます。ルート リストが使用される場合、そのルート リストは、それぞれが 1 つ以上のトランクを含む 1 つ以上のルート グループから構成されます。ルート グループ内の個別のトランクは、トップダウン的に選択されるように設定することも、循環的に選択されるように設定することもできます。発信コールでは、ルート パターンを使用して、このように関連付けられたトランクの 1 つが Unified CM によって選択されます。Unified CM では、着信コールを受け付ける前に、コールの発信元のリモート アドレスにトランクが定義されているかどうかが確認されます。

SIP トランクおよび H.323 トランクの比較

Cisco Unified CM トランク接続は、SIP と H.323 の両方のトランクをサポートしています。多くの場合、SIP または H.323 のいずれを使用するかは、各プロトコルで提供される固有な機能により異なります。また、お客様の好みや、異なるベンダーの製品間で提供される相互運用性におけるプロトコルの成熟度および品質など、トランク プロトコルの選択に影響を与える外部的要素もたくさんあります。

シスコ デバイス間のトランク接続の場合、H.323 または SIP のいずれを使用するかは、比較的、簡単に決定できます。他のベンダーの製品およびサービス プロバイダー ネットワークとのトランク接続の場合、お客様がどの機能を必要としているか、および 2 つのベンダーの製品間での相互運用性の範囲を理解することが重要です。

表 14-2 に、Unified CM クラスタ間での SIP および H.323 トランクを介して提供される機能の一部についての比較を示します。

表 14-2　Cisco Unified CM トランクでの SIP および H.323 機能の比較

機能	SIP	QSIG over SIP	H.323	H.323 を介した QSIG
発呼回線（番号）ID 表示	あり	あり	あり	あり
発呼回線（番号）ID 表示禁止	あり	あり	あり	あり
発信者名 ID 表示	あり	あり	あり	あり
発信者名 ID 表示禁止	あり	あり	あり	あり
接続回線（番号）ID 表示	あり	あり	あり	あり
接続回線（番号）ID 表示禁止	あり	あり	あり	あり
接続者名 ID 表示	あり	あり	あり	あり
接続者名 ID 表示禁止	あり	あり	あり	あり
アラート名	あり	あり	なし	あり
転送（ブラインドまたは在席）	あり / あり	あり / あり	あり / あり	あり / あり
自動転送（すべて）	あり	あり	あり	あり
自動転送（通話中）	あり	あり	あり	あり
自動転送（無応答）	あり	あり	あり	あり
呼完了（ビジーサブスクライバ）	なし	あり	なし	あり
呼完了（無応答）	なし	あり	なし	あり
サブスクライブ / 通知、パブリッシュ - 表示	あり	あり	なし	なし
メッセージ待機インジケータ（MWI：ランプ点灯 / 消灯）	あり	あり	なし	あり
パス交換	なし	あり	なし	あり
コール保留 / 復帰	あり	あり	あり	あり
保留音（ユニキャストおよびマルチキャスト）	あり	あり	あり	あり
DTMF リレー	RFC 2833、KPML（OOB）、Unsolicited Notify（OOB）	RFC 2833、KPML（OOB）、Unsolicited Notify（OOB）	H.245 アウトオブバンド（OOB）[1]	H.245 アウトオブバンド（OOB）[1]
SIP アーリー オファー	あり：MTP が必要な場合があります	あり：MTP が必要な場合があります	該当なし	該当なし
SIP ディレイド オファー	あり	あり	該当なし	該当なし
H.323 Fast Start	該当なし	該当なし	あり：発信 Fast Start のために常に MTP が必要	あり：発信 Fast Start のために常に MTP が必要
H.323 Slow Start	該当なし	該当なし	あり	あり
音声コーデック	G.711、G.722、G.723、G.729、iLBC、AAC、iSAC	G.711、G.722、G.723、G.729、iLBC、AAC、iSAC	G.711、G.722、G.723、G.729	G.711、G.722、G.723、G.729

表 14-2　Cisco Unified CM トランクでの SIP および H.323 機能の比較（続き）

機能	SIP	QSIG over SIP	H.323	H.323 を介した QSIG
MTP でのコーデック	[Early Offer support for voice and video calls (insert MTP if needed)] がオンの場合、すべてのコーデックがサポートされます [MTP Required] がオンの場合、G.711、G.729	[Early Offer support for voice and video calls (insert MTP if needed)] がオンの場合、すべてのコーデックがサポートされます [MTP Required] がオンの場合、G.711、G.729	G.711、G.723、G.729	G.711、G.723、G.729
ビデオ	あり	あり	あり	あり
ビデオ コーデック	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC	H.261、H.263、H.263+、H.264 AVC
T.38 Fax	あり	あり	あり	あり
シグナリング認証	ダイジェスト、TLS	ダイジェスト、TLS	なし	なし
シグナリング暗号化	TLS	TLS	なし	なし
メディア暗号化（音声）	SRTP	SRTP	SRTP	SRTP
RSVP ベースの QoS およびコール アドミッション制御	あり	あり	なし	なし
+ 文字のサポート	あり	あり	なし	なし
着信コール：着信側：Significant Digit、Prefix-Digit	あり	あり	あり	あり
着信の発呼側設定：Strip Digit、番号タイプに基づく Prefix-Digit	SIP は番号タイプをサポートせず、すべてのコールに「Unknown」が使用されます	SIP は番号タイプをサポートせず、すべてのコールに「Unknown」が使用されます	Unified CM、Unknown、National、International、Subscriber	Unified CM、Unknown、National、International、Subscriber
着信の着呼側設定：Strip Digit、番号タイプに基づく Prefix-Digit	該当なし	該当なし	Unified CM、Unknown、National、International、Subscriber	Unified CM、Unknown、National、International、Subscriber
接続先変換	あり	あり	なし	なし
発信の発呼側変換	あり	あり	あり	あり
発信の着呼側変換	あり	あり	あり	あり

表 14-2　Cisco Unified CM トランクでの SIP および H.323 機能の比較（続き）

機能	SIP	QSIG over SIP	H.323	H.323 を介した QSIG
発信の発呼側/着呼側番号タイプの設定	SIP は番号タイプをサポートしません	SIP は番号タイプをサポートしません	Unified CM、Unknown、National、International、Subscriber	Unified CM、Unknown、National、International、Subscriber
発信の着呼側/発呼側番号計画の設定	SIP は番号計画をサポートしません	SIP は番号計画をサポートしません	Unified CM、ISDN、National Standard、Private、Unknown	Unified CM、ISDN、National Standard、Private、Unknown
トランクの宛先：状態検出メカニズム	OPTIONS Ping	OPTIONS Ping	コール別の試行	コール別の試行

1. H.323 トランクは、特定の接続の種類で、RFC 2833 に規定されたシグナリングをサポートします。

SIP トランクの概要

SIP トランクによって、ゲートウェイ、Cisco Unified CM Session Management Edition、SIP プロキシ、Unified Communications アプリケーション、その他の Unified CM クラスタなど、他の SIP デバイスに接続できます。現在、サービス プロバイダーや Unified Communications アプリケーションに接続するときに、最も一般的に選択されるプロトコルは、ほぼ間違いなく SIP です。Cisco Unified CM 8.5 以降のリリースでは、次の SIP トランクおよびコール ルーティングに関する強化がありました。

- すべての Unified CM ノードで実行可能
- 各トランクで最大 16 の宛先 IP アドレスをサポート
- SIP OPTIONS ping キープアライブ
- SIP アーリー オファーは音声コールとビデオ コールをサポート（必要に応じて MTP を挿入）
- QSIG over SIP
- SIP トランクの正規化および透過性
- すべての Unified CM ノードでルート リストの使用をサポート

最新リリースの Unified CM で使用できる SIP トランク機能によって、SIP は新規のトランク接続にも既存のトランク接続にも適した選択肢になりました。QSIG over SIP 機能は H.323 クラスタ間トランクにおけるものと同等を提供します。また、Cisco IOS ゲートウェイ（および QSIG ベースの TDM PBX）に対する QSIG over SIP トランク接続を提供するためにも使用されます。すべての Unified CM ノードで実行する機能、および最大 16 の宛先 IP アドレスを処理する機能によって、Unified CM クラスタからの発信の分配が改善され、クラスタおよびデバイス間に必要な SIP トランク数が減ります。SIP OPTIONS ping には、コール別の到達可能性の判断ではなく、SIP トランクの宛先に関するダイナミックな到達可能性を検出する機能があります。音声コールおよびビデオ コールに関する SIP アーリー オファーのサポート（必要に応じて MTP を挿入）によって、MTP を使用する必要性が軽減または排除され、SIP アーリー オファー トランク上で音声コール、ビデオ コール、および暗号化されたコールを処理できます。

SIP トランクの正規化および透過性によって、ネイティブの Unified CM とサードパーティのユニファイド コミュニケーション システム間、およびサードパーティ システム間の相互運用性が改善されます。正規化によって、着信および発信の SIP メッセージおよび SDP 情報を SIP トランクごとに変更できます。通過するメッセージの部分を Unified CM が理解またはサポートしていない場合でも、透過性によって、Unified CM は SIP ヘッダー、パラメータ、コンテンツ本文を SIP トランク コール レグから別の宛先に渡すことができます。

これらの機能については、この項で詳しく後述します。

SIP トランクの新規拡張機能の全リストについては、次の Web サイトで入手可能な Cisco Unified Communications Manager の製品リリース ノートを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

配置に関する一般的な考慮事項

Unified CM SIP トランクは、H.323 クラスタ間トランクと比較すると機能数が多いため、クラスタ間トランク接続のプロトコルとして SIP を選択できるようになります（ただし、以前のソフトウェア バージョンを使用する Unified CM に対するクラスタ間トランク接続の場合には、H.323 Annex M1 の方が推奨されます）。また、業界では SIP が幅広くサポートされているため、サードパーティのアプリケーションやサービス プロバイダーと接続するには、一般的に SIP トランクが推奨されます。

SIP トランクの機能と操作

ここでは、Unified CM SIP トランクの設計および配置時に考慮する必要がある Unified CM SIP トランクの操作と、いくつかの主要な SIP トランク機能について説明します。

SIP トランクで使用できる [Run on All Active Unified CM Nodes]

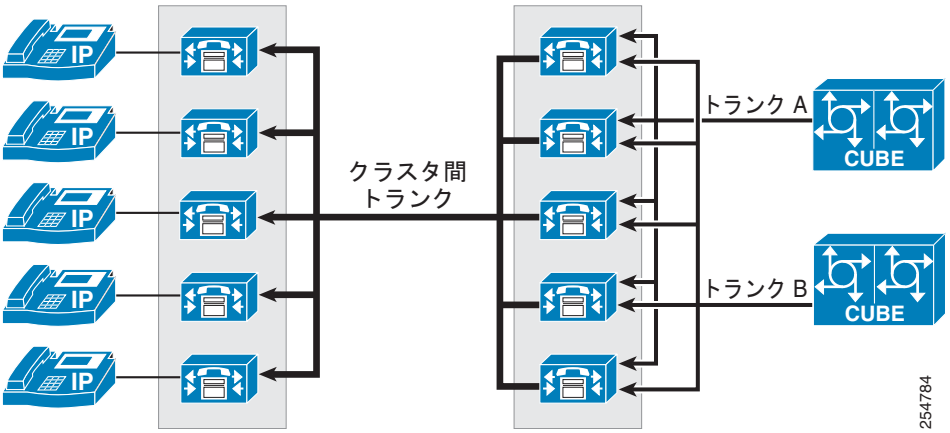
SIP トランクで [Run on all Active Unified CM Nodes] オプションをオンにすると、Unified CM は、クラスタ内のコール処理サブスクライバごとに SIP トランク デーモンのインスタンスを作成します。そのため、どのコール処理サブスクライバでも SIP トランク コールを発信または着信できます（この機能を使用できるようになる前は、Unified CM Group を使用してトランクごとに最大 3 つのノードを選択できました）。[Run on all Active Unified CM Nodes] をイネーブルにすると、発信 SIP トランク コールは、（たとえば電話またはトランクから）着信コールを受信したのと同じノードから発信します。すべての Unified CM SIP トランクと同様に、トランクに関連付けられている SIP デーモンは、トランクの宛先アドレス フィールドに定義された IP アドレスを持つエンド システムからの着信のみを受け入れます。大量のコールを処理するために SIP トランクが必要な場合、すべてのノードで SIP トランクを実行することが推奨されます。その結果、発信および着信の分配は、クラスタ内のすべてのコール処理サブスクライバに均等に分散できます。また、同じ宛先に対する複数の SIP トランクが同じサブスクライバを使用している場合、各トランクが一意に識別されるために、トランクごとに一意の着信および発信のポート番号を定義する必要があります。

最大 16 の SIP トランク宛先 IP アドレス

SIP トランクは、最大 16 の宛先 IP アドレス、16 の完全修飾ドメイン名、または単一の DNS SRV エントリを使用して設定できます。追加の宛先 IP アドレスをサポートしているため、2 つの Unified Communications システム間のコール分配のために、ルート リストおよびルート グループに関連付けられた複数のトランクを作成する必要性が軽減されます。結果として、Unified CM トランク設計が単純になります（図 14-2 を参照）。この機能を [Run on all Active Unified CM Nodes] 機能、または標準の Unified CM Group を使用する SIP トランクと併用して、クラスタ内の最大 3 ノードで SIP デーモン

を作成できます。ただし、Unified CM SIP トランクと関連付けられた SIP デーモンは、トランクの宛先アドレス フィールドに定義された IP アドレスを持つエンド システムからの着信のみを受け入れる点に注意してください。

図 14-2　すべてのアクティブ ノードで実行される複数の宛先 IP アドレスを持つ SIP トランク



SIP OPTIONS ping

SIP トランクに関連付けられた SIP プロファイルで SIP OPTIONS ping 機能をイネーブルにして、トランクの宛先の状態をダイナミックに追跡できます。この機能をイネーブルにすると、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断し、到達可能なノードにのみコールを送信します。宛先アドレスが OPTIONS 要求に応答しない場合、Service Unavailable（503）応答または Request Timeout（408）応答を送信する場合、または TCP 接続を確立できない場合、そのアドレスは「アウト オブ サービス」と見なされます。1 つ以上のノードが、1 つ以上の宛先アドレスから（408 または 503 以外の）応答を受信した場合、トランクの状態は「イン サービス」と見なされます。SIP トランク ノードは、トランクの設定済み宛先 IP アドレス、またはトランクの DNS SRV エントリの解決済み IP アドレスに対して OPTIONS 要求を送信できます。SIP OPTIONS ping のイネーブル化はすべての SIP トランクで推奨されます。イネーブルにすることで、Unified CM は、コールごとまたはタイムアウトごとにトランクの状態を判断するのではなく、ダイナミックにトランクの状態を追跡できるためです。

Unified CM SIP トランクでの SIP アーリー オファー

SIP は Session Description Protocol（SDP）によってメディア情報をネゴシエートします。これにより、一方が提示したメディア セットに他方が応答する形で、使用するメディアがある組み合わせに決定します。SIP では、発信側が初期 INVITE メッセージ（アーリー オファー）によって初期オファーを送信するか、発信側がそうしなかった場合は着信側が最初の信頼性のある応答（ディレイド オファー）で初期オファーを送信できます。

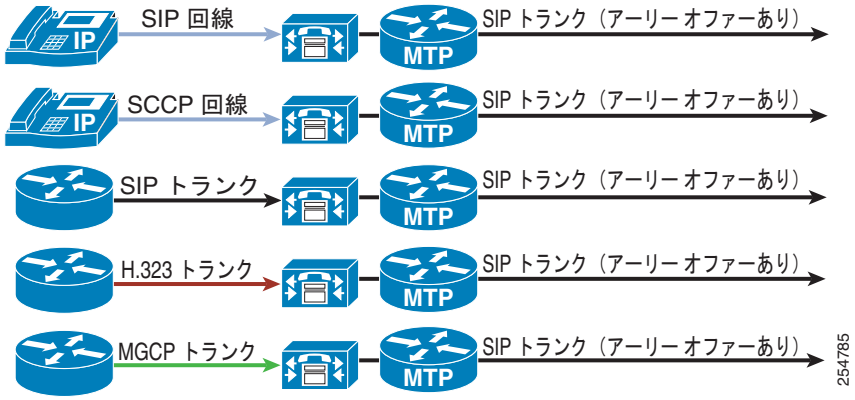
デフォルトで、Unified CM SIP トランクは、初期オファー（ディレイド オファー）を伴わない INVITE を送信します。通常、音声、ビデオ、または暗号化メディアに対するディレイド オファー コールを確立するのに MTP は不要なため、Unified CM SIP トランクには、SIP ディレイド オファーが適切です。SIP アーリー オファーが必要な場合は、Unified CM には、SIP トランクが INVITE でオファーを送信できるようにする 2 つの設定可能なオプションがあります。

- 「必要なメディア ターミネーション ポイント」（P.14-9）
- 「音声コールおよびビデオ コールをサポートするアーリー オファー（必要に応じて MTP を挿入）」（P.14-9）

必要なメディア ターミネーション ポイント

SIP トランクで [Media Termination Point Required] オプションをイネーブルにすると、トランクの Media Resources Group（MRG; メディア リソース グループ）からの MTP は各発信に割り当てられます（図 14-3 を参照）。この処理でスタティックに割り当てられた MTP は G.711 または G.729 コーデックのみをサポートするため、メディアは音声コールにのみ限定されます。

図 14-3　必要なメディア ターミネーション ポイントがある SIP アーリー オファー

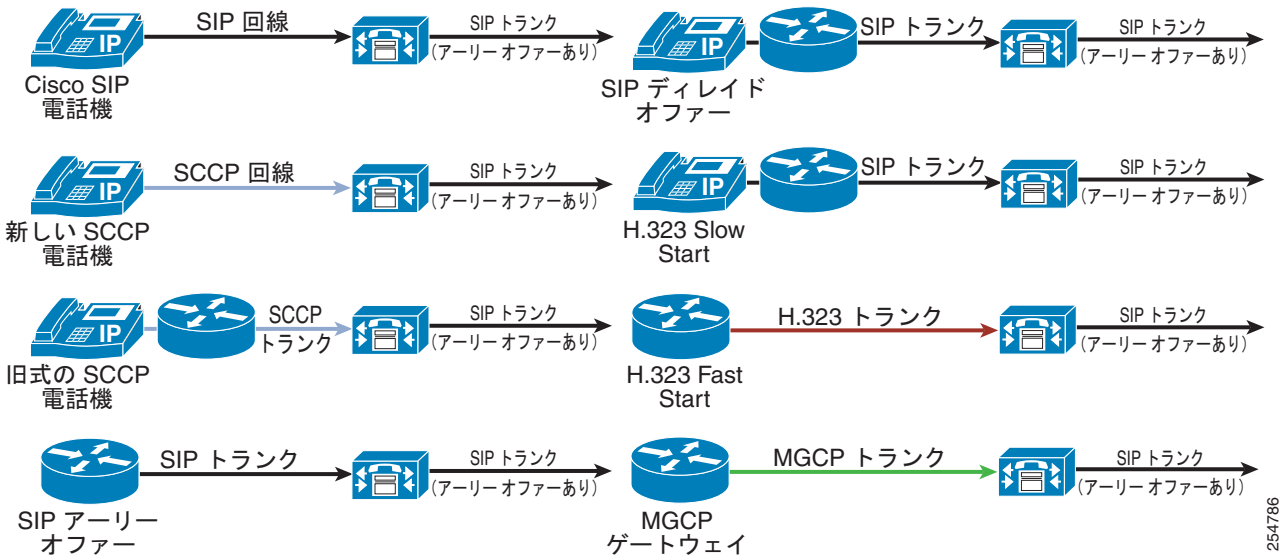


音声コールおよびビデオ コールをサポートするアーリー オファー（必要に応じて MTP を挿入）

SIP トランクに関連付けられた SIP プロファイルで [Early Offer support for voice and video calls (insert MTP if needed)] をイネーブルして MTP が挿入されるのは、発信デバイスがアーリー オファーの作成に必要な特性を Unified CM に提示できない場合のみです。一般的に、[Media Termination Point Required] よりも [Early Offer support for voice and video calls (insert MTP if needed)] が推奨されるのは、この設定オプションによって MTP の使用量が減るためです（図 14-4 を参照）。このオプションを使用して設定した SIP アーリー オファー トランク上の Unified CM に登録されている古い SCCP ベースの電話からのコールは、MTP を使用してオファー SDP を作成します。また、このようなコールは、音声メディア、ビデオ メディア、および暗号化されたメディアをサポートします（「エンドポイント機能の要約」（P.18-53）を参照）。SIP アーリー オファー トランクで拡張される SIP ディレイド オファー トランクまたは H.323 Slow Start トランクに対する着信は、MTP を使用してオファー SDP を作成します。ただし、このようなコールは最初のコール セットアップでのみ音声をサポートしますが、コール メディアを再ネゴシエートする場合（保留 / 再開後など）、ビデオおよび SRTP をサポートするためにコール中にエスカレーションできます。[Early Offer support for voice and video calls (insert MTP if needed)] を使用するタイミングのガイドラインについては、「SIP トランクの設計上の考慮事項」（P.14-27）を参照してください。

（注）　INVITE メッセージに初期オファー SDP が含まれているかどうかにかかわらず、着信 INVITE メッセージに MTP リソースは必須ではありません。

図 14-4　アーリー オファーによる音声コールおよびビデオ コールのサポート



Unified CM に対する着信を次のいずれかの手段で受信した場合、SIP トランク上で発信アーリー オファー コールを作成するために、Unified CM が MTP を挿入する必要はありません。

- アーリー オファーを使用する SIP トランク上
- Fast Start を使用する H.323 トランク上
- MGCP トランク上
- Unified CM に登録されている SIP ベースの IP 電話から
- Unified CM に登録されている新しい SCCP ベースの Cisco Unified IP 電話モデルから（詳細については、「エンドポイント機能の要約」（P.18-53）を参照）

上記のデバイスの場合、Unified CM はエンドポイントのメディア機能を使用して、発信デバイスと発信 SIP トランクのリージョンペアに基づいてコーデック フィルタリング ルールを適用し、発信 SIP トランク コールのオファー SDP を作成します。ほとんどの場合、オファー SDP には、発信したエンドポイントの IP アドレスとポート番号が含まれます。そのため、発信デバイスと SIP トランクの間に共通のコーデックがない場合でも、DTMF の不一致、TRP の要件、またはトランスコーダの要件など、他の理由で Unified CM が MTP を挿入する必要はありません。

トランクの SIP プロファイルで [Early Offer support for voice and video calls (insert MTP if needed)] を設定すると、他の理由でコールに MTP またはトランスコーダがまだ割り当てられていない場合、古い SCCP ベースの電話 (「エンドポイント機能の要約」（P.18-53）を参照) からのコール、SIP ディレイド オファー トランク、および H.323 Slow Start トランクによって、Unified CM は MTP を割り当てます。MTP は、有効なメディア ポートおよび IP アドレスを含むオファー SDP を生成するために使用されます。MTP は、発信 SIP トランクのメディア リソースではなく、発信デバイスに関連付けられたメディア リソースから割り当てられます（この処理で、メディア パスが発信 SIP トランクの MTP に固

定されるのを回避します)。発信デバイスの Media Resource Group List（MRGL; メディア リソース グループ リスト）から MTP を割り当てることができない場合、MTP の割り当ては SIP トランクの MRGL から試行されます。

Unified CM に登録されている古い電話（「エンドポイント機能の要約」（P.18-53）を参照）からのコールの場合、発信デバイスの一部のメディア機能（サポート対象の音声コーデック、ビデオ コーデック、暗号化キーなど、サポートされる場合）は、Session Description Protocol（SDP）を介したメディア交換に使用できます。Unified CM は、エンドポイントおよび MTP コーデック機能のスーパーセットを作成し、適用可能なリージョンペア設定に基づいてコーデックのフィルタリングを適用します。発信オファー SDP は、MTP の IP アドレスとポート番号を使用します。また、音声メディア、ビデオ メディア、および暗号化されたメディアをサポートできます。パススルー コーデックをサポートするには、MTP を設定する必要があります。

Unified CM が H.323 Slow Start または SIP ディレイド オファー トランクで着信を受信した場合、コールの開始時に発信デバイスのメディア機能を使用できません。この場合、Unified CM が MTP を挿入する必要があります。また、IP アドレスと UDP ポート番号を使用して、（リージョン ペアのフィルタリング後に）発信 SIP トランクで送信された最初の INVITE のオファー SDP で、サポート対象のすべての音声コーデックをアドバタイズします。アンサー SDP を SIP トランクで受信し、発信エンドポイントでサポートされるコーデックが含まれる場合、追加のオファー / アンサー トランザクションは不要です。コーデックが一致しない場合、Unified CM はトランスコーダを挿入して不一致に対処するか、reINVITE または UPDATE を送信してメディア ネゴシエーションをトリガーします。H.323 Slow Start または SIP ディレイド オファー トランクからのコールは、最初のコール セットアップでのみ音声をサポートしますが、コール メディアを再ネゴシエートする場合（保留 / 再開後など）、ビデオおよび SRTP をサポートするためにコール中にエスカレーションできます。

QSIG over SIP トランク

Unified CM は、SIP メッセージに QSIG コンテンツをカプセル化できるため、SIP QSIG クラスタ間トランク上および Cisco IOS ゲートウェイに対する SIP QSIG トランク上で、コール バック、MWI、パス交換などの機能を呼び出すことができます（図 14-5 を参照）。QSIG over SIP トランクは、H.323 Annex M1 クラスタ間トランクおよび MGCP QSIG トランクに設定されている QSIG 機能と同等を提供します（QSIG の ISO および ECMA のバリエーションは、トランク別にサポートされます）。

図 14-5　　QSIG over SIP トランク

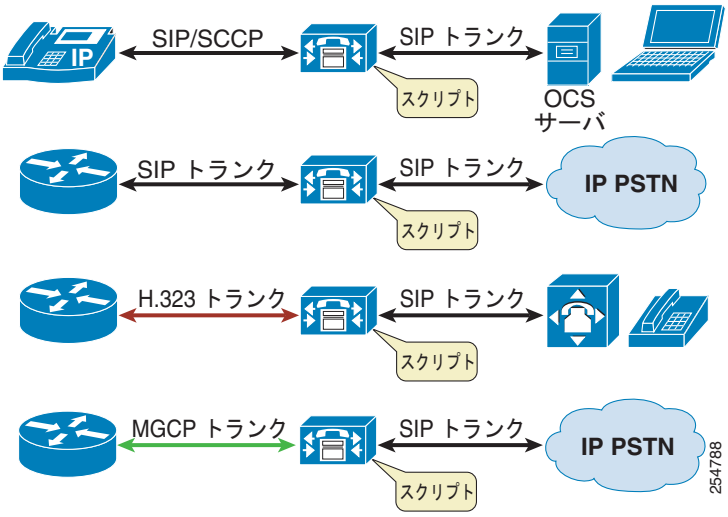
SIP トランク メッセージの正規化および透過性

正規化および透過性は、SIP トランクに強力なスクリプトベースの機能を提供します。この機能を使用すると、Unified CM を通過するときに SIP メッセージおよびメッセージ本文の内容を透過的に転送または変更できます。正規化および透過性のスクリプトは、SIP の相互運用性の問題に対処するように設計されているため、Unified CM は SIP ベースのサードパーティ PBX、アプリケーション、および IP PSTN サービスと相互運用できます。

SIP トランクの正規化

正規化によって、Unified CM を通過するときに着信および発信 SIP メッセージを変更できます。正規化は、コールに関係する他のエンドポイントで使用されるプロトコルに関係なく、スクリプトが関連付けられた SIP トランクを通過するすべてのコールに適用されます。たとえば、SIP トランクの正規化スクリプトは、SIP ライン デバイスから SIP トランクに対するコール、SCCP ベースのデバイスから SIP トランクに対するコール、MGCP から SIP トランクに対するコール、H.323 から SIP トランクに対するコールなどで実行できます（図 14-6 を参照）。正規化にはエンドツーエンドの SIP は必要ありません。

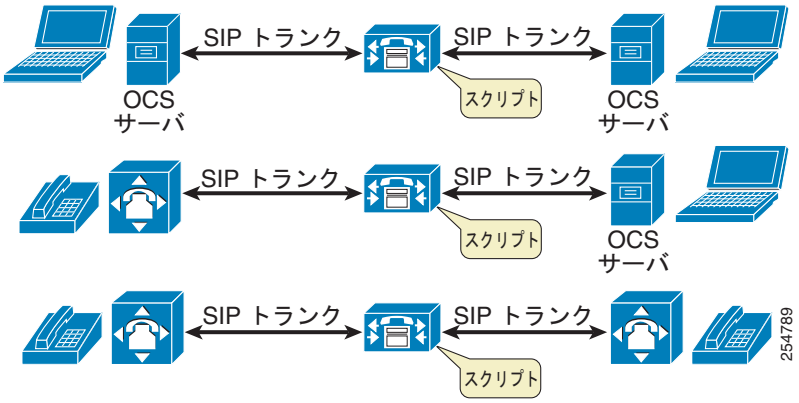
図 14-6　　SIP トランクの正規化



SIP トランクの透過性

通過するメッセージの部分を Unified CM が理解またはサポートしていない場合でも、透過性によって、Unified CM は SIP ヘッダー、パラメータ、コンテンツ本文を SIP トランク コール レグから別の宛先に渡すことができます。透過性（または透過的なパススルー）を適用できるのは、Unified CM を通過するコールが、図 14-7 のように SIP トランクから SIP トランクへの場合のみです。

図 14-7　SIP トランクの透過性



正規化と透過性のスクリプトは、強力、高速、軽量、そして埋め込み可能なスクリプティング言語である Lua を使用して、SIP トランク上の SIP メッセージと SDP 本文の内容を変更します（Lua の詳細については、http://lua-users.org/wiki/LuaOrgGuide で入手可能なマニュアルを参照してください）。

シスコでは、Lua ベースの SIP メッセージ API のライブラリを作成しました。このライブラリを使用して、SIP メッセージおよび SDP 本文に指定されている情報の取得、変更、置換、削除、パススルー、無視、追加、変換などを行うことができます。基礎となる Lua 言語では、取得した情報を変数として格納できます。また、If、elseif、while、do、<、>、= などの一連の演算を使用して処理できます。このスクリプティング方法では、スクリプトの決定のマーキングに複数の変数と状態固有のコンテキストをサポートします。シスコの SIP メッセージ ライブラリ API と Lua 言語の基礎となる機能を組み合わせると、ほとんどすべての SIP メッセージや SDP 本文の内容を変更できる強力なスクリプティング環境になります。

SIP トランクでの着信メッセージの場合、正規化および透過性スクリプトの処理は、ネットワークからメッセージを受信した直後に実行されます。発信メッセージの場合、スクリプト メッセージングは、ネットワークにメッセージを送信する直前に実行されます。

Lua スクリプト内では、コールバック機能（メッセージ ハンドラとも呼ばれます）は、関係するメッセージ タイプを要求するために使用されます。Cisco Lua 環境は、要求（inbound_INVITE など）のメッセージの方向およびメソッドに基づいて、また応答（outbound_180_INVITE など）の（CSeq ヘッダーの）メッセージの方向、応答コード、およびメソッドに基づいて、メッセージ ハンドラの名前を構築します。メッセージ オブジェクト（msg など）は、メッセージ ハンドラに渡されるため、スクリプトでメッセージ（inbound_INVITE(msg) など）を変更できます。

コールバック関数（メッセージ ハンドラ）の例：

inbound_INVITE()	outbound_INVITE()
inbound_UPDATE()	outbound_SUBSCRIBE()
inbound_3XX_INVITE()	outbound_180_INVITE()

次に、Lua スクリプトで、シスコの SIP メッセージ ライブラリを使用して、メッセージ パラメータのアクセスと操作を行います。次の例を参考にしてください。

- **getHeader**(*header-name*) はヘッダー値または "" を返します
- **getHeaderValues**(*header-name*) はヘッダー値のテーブルを返します
- **addHeaderValueParameter**(*header-name*, *parameter-name*, [*parameter-value*])
- **getUri**(*header-name*) は指定したヘッダーから URI を取得します

- **block()** は指定した SIP メッセージをブロックします
- **applyNumberMask**(*header-name, mask*) は指定したヘッダーを取得し、指定した番号マスクを URI に適用します
- **getSdp()** は SDP の内容を返します
- **sdp:getLine(start of line, line contains)** は、「start of line」で始まり、「line contains」という文字列も含む SDP の行を返します。
- **sdp:modifyLine(start of line, line contains,** *new-line***)** は、「start of line」で始まる SDP の行を検索し、「line contains」と一致する行は *new-line* パラメータで置換されます

次に、SIP メッセージ API スクリプトの使用例を示します。

例 14-1　SIP メッセージ API : getRequestLine

getRequestLine() はメソッド、Request-URI、およびバージョンを返します。

このメソッドは次の 3 つの値を返します。

- メソッド名
- Request-URI
- プロトコルのバージョン

スクリプト例：

1 行め	M = {}
2 行め	function M.outbound_INVITE(message)
3 行め	local method, ruri, ver = message:getRequestLine()
4 行め	end
5 行め	return M

1 行めで、コールバック関数セットを空の値に初期化します。この M というコールバック関数セットは、基本的に Lua テーブルです。

2 ～ 4 行めで、メッセージ ハンドラを定義します。このコールバック関数が実行されるのは、発信 INVITE が Unified CM から送信されるときです。次に、要求の行からメソッド、Request-URI、およびバージョンを取得し、その値を格納します。

スクリプトで複数のメッセージ ハンドラを定義できます。メッセージ ハンドラの名前は、特定の SIP メッセージに対して呼び出されるメッセージ ハンドラがあれば、そのハンドラを示します。

最後の行は、コールバック セットを返します。この行は必須です。

メッセージ：

```
INVITE sip:1234@10.10.10.1 SIP/2.0
```

出力と結果：

```
method == "INVITE"
ruri == "sip:1234@10.10.10.1"
version == "SIP/2.0"
```

例 14-2　発信 INVITE の「Cisco-Guid」ヘッダーを削除するのみのスクリプト

1 行め	M = {}
2 行め	function M.outbound_INVITE(message)
3 行め	message:removeHeader("Cisco-Guid")
4 行め	end
5 行め	return M

1 行めで、コールバック関数セットを空の値に初期化します。この M というコールバック関数セットは、基本的に Lua テーブルです。

2 ～ 4 行めで、メッセージ ハンドラを定義します。このコールバック関数が実行されるのは、発信 INVITE が Unified CM から送信されるときです。スクリプトで複数のメッセージ ハンドラを定義できます。メッセージ ハンドラの名前は、特定の SIP メッセージに対して呼び出されるメッセージ ハンドラがあれば、そのハンドラを示します。

最後の行は、コールバック セットを返します。この行は必須です。

メッセージ：

```
INVITE sip:1234@10.10.10.1 SIP/2.0
.
P-Asserted-Identity: "1234" <1234@10.10.10.1>
Cisco-Guid: 1234-4567-1234
Session-Expires: 1800
```

出力と結果：

```
INVITE sip:1234@10.10.10.1 SIP/2.0
.
P-Asserted-Identity: "1234"
```

SIP トランクの正規化および透過性のスクリプトについて詳しくは、次のサイトで入手可能な『*Developer Guide for SIP Transparency and Normalization*』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/sip_tn/8_5_1/sip_t_n.html

ルート リストの [Run on All Active Unified CM Nodes]

これは具体的には SIP トランク機能ではありませんが、すべてのノードでルート リストを実行すると、ルート リストおよびルート グループ内のトランクに利点があります。「ルート ローカル」ルールを使用してすべてのノードでルート リストを実行すると、発信の分配が改善され、不要なクラスタ内トラフィックを回避できます。

ルート リストの場合、ルート ローカル ルールは次のように動作します。

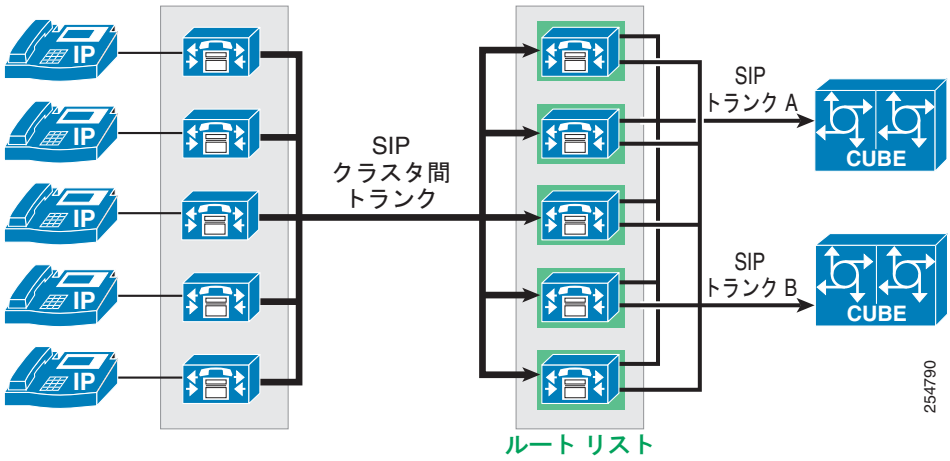
ルート リスト（および関連するルート グループとトランク）を使用する発信の場合、登録されている電話からのコールまたは着信トランクが、ルート リスト インスタンスがあるノードに到達したときに、選択した発信トランクのインスタンスがルート リストと同じノードに存在するかどうかが Unified CM によって確認されます。存在する場合、Unified CM はそのノードを使用して発信トランク コールを確立します。

ルート リストとトランクの両方で [Run on all Active Unified CM Nodes] がイネーブルの場合、発信の分配は、着信が到達したノードによって決定されます。すべてのノードでの実行ではなく、選択した発信トランクが Unified CM Group を使用すると、選択した発信トランクのインスタンスが、着信が到達した同じノードに存在する場合に、Unified CM はルート ローカル ルールを適用します。トランクのインスタンスがそのノードに存在しない場合、Unified CM は（クラスタ内の）コールをトランクがアクティブなノードに転送します。

ルート リストで [Run on all Active Unified CM Nodes] をイネーブルにしていない場合、ルート リストのインスタンスはクラスタ内の 1 つのノード（ルート リストの Unified CM Group のプライマリ ノード）でアクティブになり、ルート ローカル ルールはそのノードに適用されます。この設定では、ルート リストに関連付けられたいずれかのトランクの Unified CM Group に、ルート リストの Unified CM Group のプライマリ ノードを使用しないよう推奨します。これにより発信コールの分配が最適でなくなる場合があるためです。

一般的な推奨事項として、[Run on all Active Unified CM Nodes] はすべてのルート リストでイネーブルにしてください（図 14-8 を参照）。

図 14-8　すべてのアクティブな Unified CM ノードで実行されるルート リスト



DNS を使用する SIP トランク

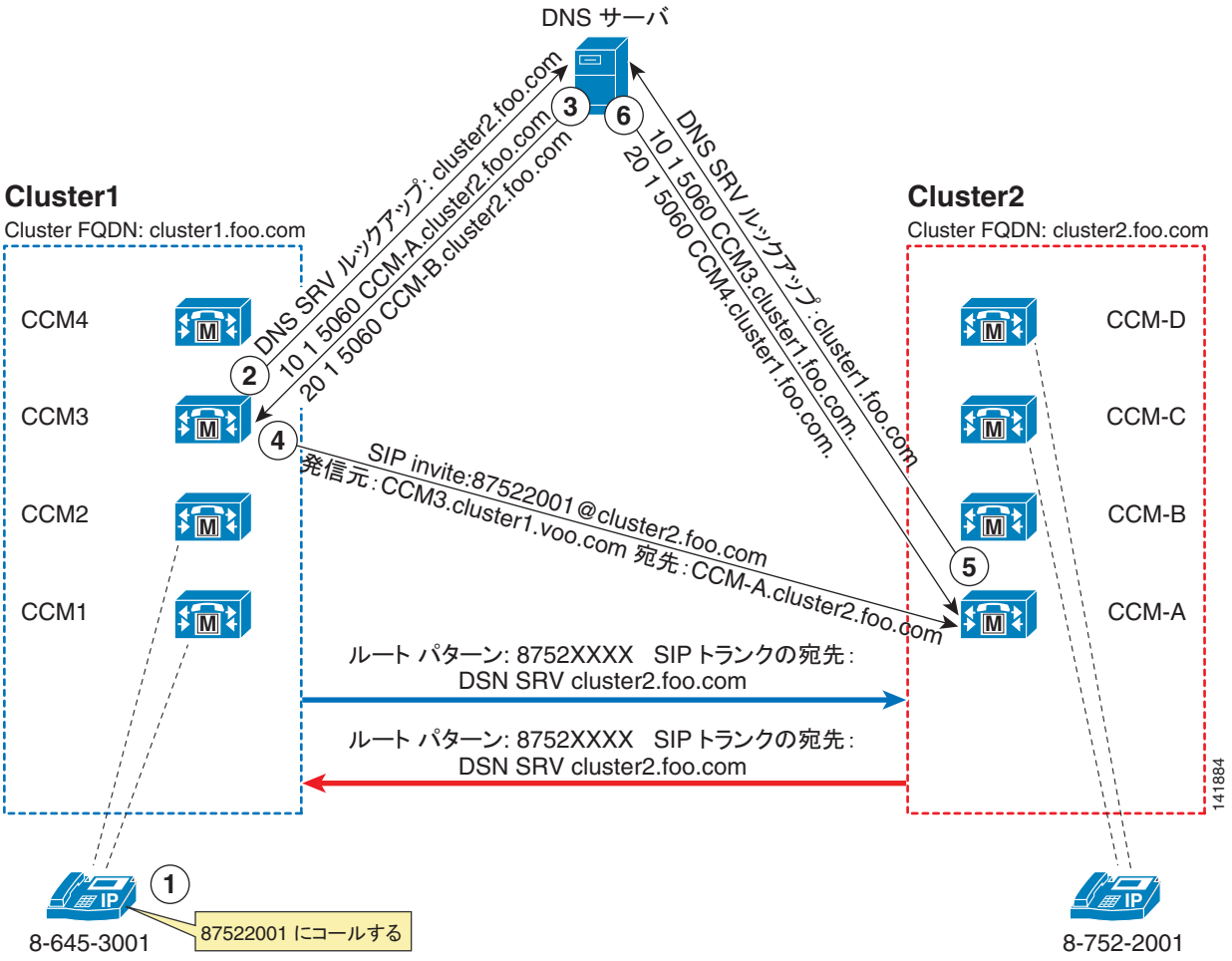
次のような特定の状況では、複数の宛先 IP アドレスを定義するよりも、SIP トランクの宛先として DNS SRV エントリを使用する方が推奨されます。

- SRV ホストの優先順位付けが必要な場合
- SRV ホストの重み付けが必要な場合
- 必要な宛先 IP アドレス数が 16 を超える場合
- DNS SRV の解決が、宛先 Unified Communications システムの要件の場合

（注）　設定オプション [Destination Address is an SRV] が選択されている場合、トランクの宛先として単一の SRV エントリのみを追加できます（たとえば、Destination Address = cluster1.cisco.com、Port = 0 です）。

図 14-9 に、DNS SRV を使用して、アドレスを宛先 Unified CM クラスタに解決する SIP トランクのコール フローを示します。ただし、この宛先は、サードパーティのユニファイド コミュニケーション システムの場合もあります。

図 14-9　DNS SRV を使用したクラスタ間 SIP トランクのコール フロー



注:DNS A ルックアップは、このコール フローから割愛しています。

図 14-9 は、このコール フローにおける次の手順を示しています。

1. Cluster1 内の IP Phone が 87522001 にコールします。
2. コールはルート パターン 8752XXXX と一致し、このパターンは cluster2.foo.com の DNS SRV を使用した SIP トランクを指しています。Cluster1 の CCM3 は、このコールを処理するノードです。その SIP トランクはこのノードに登録されているためです。CCM3 は、cluster2.foo.com の DNS SRV ルックアップを送信します。
3. DNS サーバは、CCM-A.cluster2.foo.com と CCM-B.cluster2.foo.com の 2 つのレコードで応答します。CCM-A.cluster2.foo.com のプライオリティの方が高いため、コールはその Unified CM に対して試みられます。SIP INVITE が送信される前に、CCM-A.cluster2.foo.com に関して別の DNS ルックアップが行われます。
4. CCM3 は、SIP INVITE を 87522001@cluster2.foo.com に送信します。宛先アドレスは CCM-A の IP アドレスに設定されます。
5. Unified CM は、このコールをローカル コールとして解釈します。Uniform Resource Identifier（URI; ユニフォーム リソース識別子）のホスト部分が Cluster FQDN エンタープライズ パラメータと一致しているためです。Cluster2 には、CCM3 の宛先が設定された SIP トランクがありませ

ん。したがって、DNS SRV を使用して SIP トランクに設定されたすべてのドメインに対して、DNS SRV ルックアップを行います。その場合、例では cluster1.foo.com の DNS SRV の宛先を持つ単一のトランクが示されています。

6. DNS サーバは 2 つのエントリを返し、そのうちの 1 つが INVITE の送信元 IP アドレスと一致します。クラスタはコールを受け入れ、内線 87522001 にコールをルーティングします。

SIP トランクのハイ アベイラビリティ

SIP トランクを使用したハイ アベイラビリティの設定には、多様な Unified CM オプションを使用できます。そのすべてを組み合わせて、SIP トランクの送信元サーバおよび宛先サーバの両方に冗長性と復元力を提供できます。これらのオプションは次のように分類できます。

- 「発信元 SIP トランク コールに対する複数の送信元 Unified CM サーバ」（P.14-18）
- 「SIP トランクごとの複数の宛先 IP アドレス」（P.14-19）
- 「ルート リストとおよびルート グループを使用する複数の SIP トランク」（P.14-19）
- 「SIP OPTIONS ping」（P.14-19）

発信元 SIP トランク コールに対する複数の送信元 Unified CM サーバ

標準の Unified CM Group の使用

個々のトランクに関連付けられている Unified CM Group 内に定義されたノードによって、トランク経由でコールを送受信できるサーバのセットが構成されます。1 つの Unified CM グループには 3 つまでノードを定義できるため、トランク自体のハイ アベイラビリティが確保されます。

[Run on All Active Unified CM Nodes] の使用

[Run on all Active Unified CM Nodes] 機能を使用すると、クラスタ内の各コール処理サブスクライバで SIP トランク インスタンスが作成され、イネーブルになるため、そのノードのトランク上で発信または着信できます。

発信 SIP トランク コールに関する Unified CM ルート ローカル機能とサブスクライバの選択の影響

Unified CM のルート ローカル機能は、クラスタ内トラフィックを減らすために設計されています。この機能は、次の示す例のように動作します。

> 電話機などのデバイスが SIP トランク 1 上で発信すると、SIP トランク 1 のインスタンスが、電話機の登録先と同じノードでアクティブな場合、クラスタ内の別のノード上にある別の SIP トランク 1 インスタンスに対してコールを内部的にルーティングするのではなく、常にこの同居する SIP トランク 1 インスタンスを使用します。

ノードの選択に関するルート ローカル機能の影響は、Unified CM Group と [Run on all Active Unified CM Nodes] のいずれがトランクに設定されているかによって変わります。[Run on all Active Unified CM Nodes] を設定したトランクの場合、発信デバイスの登録先ノードは、発信 SIP トランク コールの発信に使用されます。Unified CM Group がトランクに使用されているときに、発信デバイスが、トランクの Unified CM Group のノードの 1 つに登録されている場合、ルート ローカル ルールが適用されます。発信デバイスが、トランクの Unified CM Group のノードの 1 つに登録されていない場合、Unified CM は、トランクの Unified CM Group のノード上でコールをランダムに分配します。

SIP トランクの場合、[Run on all Active Unified CM Nodes] の使用が推奨される方法です。この方法を使用すると、ノード間のコールの分配を発信元デバイスが決定でき、クラスタ内のトラフィックが最小限に抑えられるためです。

SIP トランクごとの複数の宛先 IP アドレス

単一の SIP トランクには、最大 16 の宛先 IP アドレスを設定できます。Unified CM は、SIP トランク上で発信するときに、設定済みの宛先 IP アドレスに対してランダムな分配を使用します。SIP トランクで複数の IP アドレスを使用すると、ルート リストおよびルート グループを使用して複数のトランクを配置する必要性を軽減できます。

[Run on All Active Unified CM Nodes] を使用するときの設計の考慮事項

[Run on All Active Unified CM Nodes] と複数の宛先アドレスを併用する場合、着信を受け入れるには、SIP トランクで受信した着信の送信元 IP アドレスが、着信トランクに設定されている宛先 IP アドレスと一致する必要がある点に注意してください。たとえば、[Run on all Active Unified CM Nodes] が各クラスタ内の SIP クラスタ間トランクで設定されている場合、各トランクは、宛先クラスタ内の各アクティブ ノードの対応する宛先アドレスを使用して設定する必要があります。WAN 設計上にクラスタリングを配置し、地理的なコールの分配およびフェールオーバーが必要な場合、複数のクラスタ間トランク（それぞれ最大 3 つの宛先 IP アドレスを使用）上で標準の Unified CM Group を使用し、さらにルート リストとルート グループを併用します。

ルート リストとおよびルート グループを使用する複数の SIP トランク

複数の優先順位が付けられた SIP トランクが必要になるのは、多くの場合、Unified Communications 設計でのアドレス エラーのシナリオです。これらのトランクは、1 つのルート リスト内の複数のルート グループに設定し、ルート パターンに関連付ける必要があります。Unified CM は、リスト内の選択したトランク上で発信できない場合、リスト内の次のトランクを使用します。一般的な推奨事項として、[Run on all Active Unified CM Nodes] はすべてのルート リストでイネーブルにしてください

SIP OPTIONS ping

SIP トランクに関連付けられた SIP プロファイルで SIP OPTIONS ping をイネーブルにして、トランクの宛先の状態をダイナミックに追跡できます。このオプションをイネーブルにすると、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断します。SIP OPTIONS ping のイネーブル化は、ハイ アベイラビリティが必要なすべての SIP トランクで推奨されます。イネーブルにすることで、Unified CM は、コールごとまたはタイムアウトごとにトランクの状態を判断するのではなく、ダイナミックにトランクの状態を追跡できるためです。

SIP トランクのロード バランシング

SIP トランクのロード バランシングを設計する場合、コールの送信元となるノードとその宛先の両方について考慮します。Unified CM SIP トランクでは、発信に使用されるノードは、ルート ローカル ルール、発信トランクがアクティブなノード数、およびルート リストを複数の発信トランクと併用するかどうかによって決定されます。このような考慮事項について、次の項で説明します。

単一の SIP トランク上の発信

単一の SIP トランクは、Unified CM Group で最大 3 つの Unified CM ノードを実行できます。または、クラスタ内のすべてのアクティブな Unified CM ノードで実行できます。発信の送信元ノードを選択するために、Unified CM は次の決定プロセスを適用します。

- トランクのインスタンスがすべてのノードで実行される場合、ルート ローカル ルールが適用され、各発信に使用されるノードはコールが到達するノードによって決定されます（たとえば、発信元電話が登録されているノードや、着信トランク コールが到達したノード）。
- Unified CM Group を使用する場合、ルート ローカル ルールは、トランクの Unified CM Group と同じノードに登録されている発信元デバイスに適用されます。クラスタ内の他のサーバに登録されている発信元デバイスの場合、Unified CM は、トランクの Unified CM Group のノード間でコールを分配します。Unified CM は、トランクの設定済み宛先アドレス間でラウンドロビン式コールの分配を使用します。SIP トランクには、最大 16 の宛先 IP アドレスを設定できます。

複数の SIP トランク上の発信

SIP トランクはすべてのアクティブな Unified CM ノードで実行でき、最大 16 の宛先アドレスを設定できるので、一般的に、2 つの Unified Communications システム間でコールを均等に分配するために、複数の SIP トランクを使用する必要はありません。複数のトランクと、ルート リストおよびルート グループを併用する場合、すべてのアクティブな Unified CM ノードで実行するには、ルート リストをイネーブルにする必要があります。多くの場合、PSTN に対して、または WAN 上に配置されるクラスタの一部として異なるサイトにある Unified CM サーバのグループに対してフェールオーバー機能を提供するために、複数の SIP トランクとルート リストが併用されます。発信 SIP トランク コールの発信に使用される Unified CM ノードの選択、およびトランクの設定済み宛先 IP アドレス上のコールの分配は、単一のトランクの場合と同様の方法で決定されます。WAN 設計上にクラスタリングを配置し、地理的なコールの分配およびフェールオーバーが必要な場合、複数のクラスタ間トランク（それぞれ最大 3 つの宛先 IP アドレスを使用）と標準の Unified CM Group を、ルート リストおよびルート グループと併用します。

SIP OPTIONS ping

OPTIONS ping を使用して、ダイナミックに各 SIP トランク上の各宛先 IP アドレスの状態、およびトランク全体の総合的な状態を追跡します。宛先アドレスが到達不能の場合、Unified CM はそのデバイスにコールを転送しません。すべての宛先が到達不能の場合、SIP トランクはアウトオブサービスと見なされます。

SIP ディレイド オファーおよびアーリー オファー

Cisco Unified CM は、RFC 3264 で規定されているように、SIP セッションの確立に SIP オファー / アンサー モデルを使用します。この場合、オファーは、SIP メッセージ本文で送信される Session Description Protocol（SDP）フィールドに含まれます。このオファーは、通常、デバイスでサポートされるメディア特性（メディア ストリーム、コーデック、方向属性、IP アドレス、使用されるポート）を定義します。オファーを受信するデバイスは、対応する一致メディア ストリームおよびコーデック、これを受け入れるかどうか、メディア ストリーム受信に使用する IP アドレスおよびポートに関するアンサーを、その SIP 応答の SDP フィールドで送信します。Unified CM は、このオファー / アンサー モデルを使用して、主要な SIP 標準、RFC 3261 で規定されているように、SIP セッションを確立します。

RFC 3261 は、SDP メッセージをオファーおよびアンサーで送信できる 2 つの方式を規定しています。これらの方式は、一般的にディレイド オファーおよびアーリー オファーとして知られていて、この仕様では、ユーザ エージェント クライアント/サーバにより両方の方式がサポートされていなければなりません。簡単に言うと、メッセージ本文で SDP を使用して送信される初期 SIP Invite は、アーリー オファーを定義し、メッセージ本文で SDP を使用せずに送信される初期 SIP Invite は、ディレイド オファーを定義します。

アーリー オファーでは、セッションの開始側（発信側デバイス）は、初期 Invite に含まれる SDP でその機能（たとえば、サポートされるコーデック）を送信します（これにより、着信側デバイスは、セッションに適切なコーデックを選択できます）。ディレイド オファーでは、セッションの開始側は、その機能を初期 Invite で送信せず、着信側デバイスからその機能（たとえば、着信側デバイスでサポートされるコーデックのリスト）が送られるまで待機します（これにより、発信側デバイスは、セッションで使用されるコーデックを選択できます）。

ディレイド オファーおよびアーリー オファーは、メディア機能の交換にすべての標準ベースの SIP スイッチで使用できる 2 つのオプションです。ほとんどのベンダーは、ディレイド オファーまたはアーリー オファーのいずれかを選択しています。また、それぞれに独自の利点や制限事項があります。ディレイド オファー トランク上でコールを確立するのに、MTP は不要なため、Unified CM SIP トランクには、SIP アーリー オファーより SIP ディレイド オファーが適切です。

（注）　Unified CM は、一方でディレイド オファーをサポートし、SIP トランク上のもう一方でアーリー オファーをサポートできます。この機能は、通常、SIP トランクを介して Unified CM に接続する SIP スイッチで、発着信コールに提供および選択されるコーデックを制御する場合に便利です（つまり、Unified CM からのディレイド オファー発信および Unified CM へのアーリー オファー着信を使用する場合、サービス プロバイダーは、いかなる場合でもオファーを送信し、これにより、すべてのコールに提供されるコーデックを決定できます）。

アーリー メディア

場合によって、SIP セッションで、2 つの SIP エンドポイント間でのメディア機能交換を終了する前に、メディア パスをセットアップする必要があります。そのため、SIP プロトコルでは、初期オファーがエンドポイントで受信された後で、アーリー メディアを確立できます。アーリー メディアを使用する理由は、次のようにいくつかあります。

- 着信側デバイスでは、一定時間を超えるシグナリング遅延が発生したコールに対するオーディオ カットスルー遅延（クリッピング）の効果を軽減させるか、ネットワークベース音声メッセージを発信側に提供する場合に、アーリー メディア RTP パスを確立します。
- 発信側デバイスでは DTMF または音声での Interactive Voice Response（IVR; 音声自動応答）システムにアクセスする場合に、アーリー メディア RTP パスを確立します。

Unified CM は、アーリー オファーおよびディレイド オファーの両方のコールに対してアーリー メディアをサポートしています。

アーリー メディアのカットスルーをサポートする SIP トランクの場合、トランクに関連付けられている SIP プロファイルの [SIP Rel1XX Options] 機能で、PRACK をイネーブルにする必要があります。

（注）　「アーリー オファー」と「アーリー メディア」は混乱しやすい用語ですが、同じではないので注意してください。

メディア ターミネーション ポイント

MTP は次の用途で Unified CM に使用されます。

- SIP トランク上で SIP アーリー オファーを配信する場合
- DTMF トランスポートの不一致に対処する場合
- RSVP エージェントとして動作する場合
- Trusted Relay Point（TRP）として動作する場合
- 音声 RTP ストリームに対して IPv4 と IPv6 の変換を提供する場合

次のいずれかの方法を使用して、SIP トランク上でアーリー オファーをイネーブルにできます。

- SIP トランクで [MTP Required] チェックボックスをオンにする。

  この場合、各発信に MTP が使用されます。また、単一のコーデックを使用する音声コールのみがサポートされます。

- SIP トランクに関連付けられた SIP プロファイルで [Early Offer support for voice and video calls (insert MTP if needed)] チェックボックスをオンにする。

  この方法で MTP が挿入されるのは、発信デバイスまたはトランクから、最初の SIP INVITE（たとえば、SIP ディレイド オファーまたは H.323 Slow Start トランクから Unified CM に対する着信）でメディア機能に関するすべての情報を送信できない場合のみです。この場合に MTP を使用すると、MTP のパススルー コーデックを使用して、最初のコール セットアップで追加の音声コーデックをサポートできます。確立後は、コールのメディアを再ネゴシエートする場合（保留 / 再開後など）、ビデオおよび暗号化をサポートするように音声コールをエスカレーションできます。MTP が不要な場合、すべてのコールは音声メディア、ビデオ メディア、および暗号化されたメディアをサポートします。

Unified CM SIP ディレイド オファーおよびアーリー オファーに関する推奨事項

Cisco Unified CM SIP トランクは、デフォルトでディレイド オファー（SDP なしの INVITE）をサポートします。一般的に、Media Termination Point（MTP; メディア ターミネーション ポイント）は Unified CM SIP トランクからのディレイド オファー コールの場合は不要なので、音声コール、ビデオコール、および暗号化されたコールのすべてがサポートされます。Unified CM SIP トランク上の発信コールには、ディレイド オファーの使用を推奨します。

SIP アーリー オファーが Unified CM SIP トランクで必要な場合、[Early Offer support for voice and video calls (insert MTP if needed)] を推奨します。これは、[MTP Required] と比較すると、必要な MTP リソースが少ないためです。MTP が [Early Offer support for voice and video calls (insert MTP if needed)] で使用される場合、音声、ビデオ、および暗号化メディアに対するサポートを提供できます。

IP PSTN SIP トランク接続の場合、通常、SIP アーリー オファーはサービス プロバイダーによって要求されます。IP PSTN が大量の同時発生コールのサポートを必要とする設計では、Unified CM SIP トランクでアーリー オファーを使用する代わりに Cisco Unified Border Element（アーリー オファーに対する SIP ディレイド オファー機能）を使用できるため、MTP の使用をなくすことができます。

Unified CM からのコール発着信では、エンドポイントは、RFC 2833 またはアウトオブバンド DTMF 方式（たとえば、KPML）エンドツーエンドのいずれを使用するかネゴシエートできます。エンドポイント間で共通の DTMF メソッドをネゴシエートできない場合、Unified CM は MTP をダイナミックに挿入します。

MTP は、次の 3 種類の形式で利用できます。

- Cisco IOS ゲートウェイのソフトウェア MTP。任意の Cisco IOS T-train ソフトウェア リリースで使用できます。また、Route Processor RP2 を搭載した Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、5,000 セッション（コール）まで拡張できます。
- Cisco IOS ゲートウェイでのハードウェア MTP。任意の Cisco IOS T-train ソフトウェア リリースで使用できます。ハードウェア MTP は、オンボード DSP リソースを使用し、Cisco ルータ プラットフォームでサポートされる DSP 数に従ってコールを拡張します。
- Cisco Media Convergence Server（MCS）で Cisco IP Voice Media Streaming Application を使用する Cisco Unified CM ソフトウェア MTP。

一般的に、Unified CM MTP 上では Cisco IOS MTP が推奨されます。これは、Cisco IOS MTP が、追加のコーデック タイプやパススルー コーデックのサポートなど、追加機能を提供するためです（詳細については、「メディア ターミネーション ポイント（MTP）」（P.17-16）を参照してください）。

次の設定例は、Cisco IOS ソフトウェアベース MTP の場合の例です。

```
!
sccp local Vlan5
sccp ccm 10.10.5.1 identifier 5 version 5.0.1
! Communications Manager IP address (10.10.5.1)
sccp
!
sccp ccm group 5
 bind interface Vlan5
 associate ccm 5 priority 1
 associate profile 5 register MTP000E83783C50
! MTP name (MTP000E83783C50) ... must match the Unified CM MTP name.
!
dspfarm profile 5 mtp
 description software MTP
 codec g711ulaw
 codec pass-through
 maximum sessions software 500
 associate application SCCP
```

DTMF Transport

DTMF 情報を SIP エンドポイント間で転送する方法はいくつかあります。一般的に、これらの方法は、アウトオブバンド（OOB）およびインバンド シグナリングに分類できます。インバンド DTMF 転送方式では、RTP ストリーム内でそのままの、またはシグナリングされた DTMF トーンのいずれかが送信されます。これらは、発信側または着信側、あるいはその両方のエンドポイントで処理および解釈される必要があります。アウトオブバンド シグナリング方式では、DTMF トーンは RTP パス外で、エンドポイントに対して直接転送されるか、必要に応じてこれらのトーンの解釈または転送、あるいはその両方を行う Cisco Unified CM などのコール エージェントを介して転送されます。

アウトオブバンド（OOB）SIP DTMF シグナリング方式には、Unsolicited Notify（UN）、Information（INFO）および Key Press Markup Language（KPML）が含まれます。KPML（RFC 4730）は、シスコが推奨する OOB シグナリング方式ですが、現時点では、市場で広く利用されていません。現在、KPML をサポートするとされる製品は、Cisco Unified CM、Cisco IOS ゲートウェイ（Release 12.4 以降）、および Cisco IP Phone の一部のモデルだけです。INFO は、Unified CM ではサポートされていません。

インバンド DTMF 転送方式は、RTP メディア ストリームのそのままのトーン、または RFC 2833 を使用した RTP ペイロードのシグナリングされたトーンのいずれかで DTMF トーンを送信します。
RFC 2833 は、SIP 製品ベンダーにおいて、主流の DTMF トーン送受信方式となっていて、シスコ音声製品の大部分でサポートされています。

インバンド シグナリング方式では、RTP メディア ストリームの DTMF トーンが送信されるため、セッションの SIP エンドポイントは、使用される転送方式（たとえば、RFC 2833）をサポートするか、このインバンド シグナリングを解釈し変換する方式を提供しなければなりません。2 つのエンポイントで、呼制御に Back-To-Back User Agent（B2BUA; バックツーバック ユーザ エージェント）サーバ（たとえば、Cisco Unified CM）が使用されていて、これらのエンドポイントで、各デバイスと呼制御ボックス間で異なる DTMF 方式がネゴシエートされる場合、DTMF の違いをどのように扱うか、つまり、MTP 挿入または OOB 方式のいずれを介するかが、コール エージェントにより決定されます。Unified CM では、DTMF 転送方式の不一致（たとえば、インバンドとアウトオブバンド DTMF）は、Media Termination Point（MTP; メディア ターミネーション ポイント）を挿入することで解決されます。MTP は、インバンド DTMF シグナリング（RFC 2833）で RTP ストリームを終端させ、RTP ストリームから DTMF トーンを抽出して、これらのトーンをアウトオブバンドで Unified CM に転送します。ここで、これらのトーンは、アウトオブバンド シグナリングをサポートするエンドポイントに転送されます。この場合、DTMF 変換ではどの MTP コーデックも使用できるため、MTP は、2 つのエンドポイント間のメディア パスに常に存在します。

インバンド DTMF トーンは、RTP メディア ストリームでそのままの（可聴）トーンとして転送することもできます。ただし、この転送方式は、シスコ製品では広くサポートされていないため、通常、エンドツーエンド DTMF 転送メカニズムとしては推奨できません。インバンド オーディオ DTMF トーンは、通常、G.711 a-law または mu-law コーデックを使用した場合だけ、その再生成が信頼できるため、低帯域幅コーデックでの使用には適していません。インバンド オーディオだけが、唯一使用できる DTMF 転送メカニズムである場合、Cisco Unified Border Element を使用して、インバンド オーディオ DTMF シグナリングを RFC 2833 シグナリングに変換できます。

Unified CM SIP トランクでは、DTMF Signaling Method を **No Preference** に設定することを推奨します。このように設定することで、Unified CM は、最適な DTMF 転送方式を選択し、MTP 割り当てを最小に抑えることができます。

SIP Trunk Transport Protocol

SIP トランクは、メッセージ トランスポート プロトコルとして TCP または UDP のいずれかを使用できます。信頼性が高く、接続の状態を保持する接続指向のプロトコルとして、TCP が適切です。UDP は接続指向ではなく、遠端デバイスの障害を検出し、それに応答するために SIP INVITE の再試行回数と SIP Trying タイマーに依存しています。SIP OPTIONS ping を使用して、ダイナミックに各 SIP トランク上の各宛先 IP アドレスの状態、およびトランク全体の総合的な状態を追跡します。

SIP トランク タイマーの調整の詳細については、次に示す設定例およびテクニカル ノートを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a008082d76a.shtml

安全な SIP トランク

安全な SIP トランクには次の 2 つのプロセスが必要です。

- メディアを暗号化するようにトランクを設定する（「メディア暗号化」（P.14-25）を参照）
- シグナリングを暗号化するようにトランクを設定する（「シグナリング暗号化」（P.14-25）を参照）

メディア暗号化

メディア暗号化を SIP トランクで設定するには、トランクの [SRTP allowed] チェックボックスをオンにします。[SRTP allowed] をオンにすると、コールのメディアは暗号化されますが、トランクのシグナリングは暗号化されない点に注意してください。結果として、安全なメディア ストリームの確立に使用されるセッション キーは暗号化されていない状態で送信されます。そのため、Unified CM と宛先 SIP トランク デバイス間のシグナリングも暗号化し、キーや他のセキュリティ関連の情報がコールのネゴシエーション中に漏洩しないようにすることが重要です。

シグナリング暗号化

SIP トランクはシグナリング暗号化に TLS を使用します。TLS は SIP トランクに関連付けられた SIP セキュリティ プロファイルで設定します。また、TLS は X.509 証明書の交換を使用してトランク デバイスを認証し、シグナリング暗号化を可能にしています。

証明書は、次のいずれかの処理が実行されます。

- 各 Unified CM ノードの SIP トランク デーモンに対して TLS 接続を確立したい各デバイスから、そのノードに対してインポートします。
- Certificate Authority（CA; 認証局）から署名されます。この場合、リモート デバイスの証明書をインポートする必要はありません。インポートする必要があるのは CA 証明書のみです。

Unified CM には、証明書の一括インポートおよびエクスポート機能があります。ただし、[Run on all Active Unified CM Nodes] および最大 16 の宛先アドレスを使用する SIP トランクの場合、認証局を使用するほうが、管理上の負荷の少ない集中管理的な方法で SIP トランクにシグナリング暗号化を設定できます。

SIP トランクの TLS の詳細については、次のサイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Security Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

認証局については、次のサイトで入手可能な最新バージョンの『*Cisco Unified Communications Operating System Administration Guide*』で Certificate Authority（CA; 認証局）の情報を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

システムが安全なメディアまたはシグナリング パスを確立でき、さらにエンド デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。システムが安全なメディアまたはシグナリング パスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送の場合、または会議、トランスコーディング、保留音などの場合に発生する可能性があります。

SRTP が設定されたデバイスでは、デバイスの [SRTP Allowed] チェックボックスがオンで、そのコールでデバイスの SRTP 機能が正常にネゴシエートされた場合、Unified CM はコールを暗号化済みと分類します。これらの条件を満たさない場合、Unified CM はコールを安全ではないと分類します。デバイスが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

（注）　[MTP Required] チェックボックスを使用して、スタティックに SIP トランクに割り当てられている MTP は、パススルー コーデックをサポートしないため、SRTP をサポートしません。

すべてのコールで SRTP をサポートするには、ディレイド オファーについて SIP トランクを設定します。

[Early Offer support for voice and video calls (insert MTP if needed)] が設定されている場合、暗号化をサポートするデバイスについて、MTP を使用する必要のないすべてのコールが SRTP をサポートできます。MTP をコール パスに挿入する場合、このダイナミックに挿入された MTP はパススルー コーデックをサポートするため、次の場合に暗号化されたコールがサポートされます。

- 発信元デバイスが古い SCCP ベースの電話の場合（「エンドポイント機能の要約」（P.18-53）を参照）、最初のコール セットアップ時に SRTP をネゴシエートできます。
- ディレイド オファー SIP トランクまたは H.323 Slow Start トランクで Unified CM に対してコールを着信した場合、最初のコール セットアップ時に SRTP はネゴシエートされません。これは、使用できるセキュリティ キーがないためです。ただし、コール メディアを再ネゴシエートする場合（保留 / 再開後など）、SRTP をサポートするようにコール中にコールをエスカレーションできます。

アーリー オファー以外の理由（Trusted Relay Point のためや、RSVP エージェントとしてなど）で、Unified CM がダイナミックに MTP を挿入する場合、パススルー コーデックをサポートする MTP で SRTP がサポートされます。

MTP を使用する **dtmf-relay** は（MTP が、インバンドおよびアウトオブバンド DTMF 信号を変換する必要がある場合）、メディア ストリームの DTMF パケットを復号化できないため、SRTP では機能しないので注意してください。

（注）　SRTP は SAF 対応 SIP トランクではサポートされません。

発番号の変換および SIP トランク

Unified CM には、ゲートウェイおよびトランクを介して着信するコールの発番号を正規化形式に変換する機能があります。通常、この形式は、E.164 仕様に従ってグローバルにルーティングできる国際的な番号表現にします。

正規化のプロセスは、着信コールの番号および関連する番号タイプに依存します。番号タイプ パラメータは、発番号のプレフィックスとして付加する適切な番号を選択するときに使用できます。番号タイプは、Unknown、Subscriber、National、または International のいずれかです。これらの番号タイプがどのように使用されるかについての詳細および例については、「ダイヤル プラン」（P.9-1）の章を参照してください。

Unified CM の H.323 トランクおよび H.323 ゲートウェイの設定ページで 4 つの番号タイプのそれぞれに対してプレフィックス番号を指定できます。H.323 では、これらの番号タイプをシグナリング時に転送できます。対照的に、SIP では、番号タイプ情報をそのシグナリング時に転送できません。そのため、SIP トランク上の SIP ゲートウェイを介して Unified CM に着信するコールでは、発番号が local、regional、national のいずれかであるかが示されません。番号タイプ情報がない場合、Unified CM は、発番号に正しいプレフィックスを適用できません。

SIP トランクでは番号タイプを転送できないため、発番号の正規化は、コールが Unified CM に送られる前に実行する必要があります。この変換は、たとえば、着信 SIP ゲートウェイで実行できます。次の設定例は、このような変換を実行するために Cisco IOS ゲートウェイで定義できる変換ルールを示しています。

```
voice translation-rule 1
 rule 1 // /+4940/ type subscriber subscriber
 rule 2 // /+49/ type national national
 rule 3 // /+/ type international international
...
voice translation-profile 1
 translate calling 1
...
dial-peer voice 300 voip
 translation-profile outgoing 1
```

```
 destination-pattern .T
 session protocol sipv2
 session target ipv4:9.6.3.12
...
```

上記の例のように設定されている場合、Unified CM との通信に SIP を使用する Cisco IOS ゲートウェイは、+ 記号を含む、E.164 形式に正規化された発信側情報番号を送信します。この Unified CM 設定では、番号タイプが「unknown」のすべてのコールが、このゲートウェイから受信されます。プレフィックスを追加する必要はありません。

変換ルールの設定の詳細については、次のサイトから利用できる『*Voice Translation Rules*』マニュアルを参照してください。

http://www.cisco.com/en/US/tech/tk652/tk90/technologies_tech_note09186a0080325e8e.shtml

Unified CM は、発信コールの発番号を、正規化されたグローバル形式に設定できます。SIP トランクから発信されるコールの番号タイプは「unknown」になります。Cisco IOS ゲートウェイは、除去が行われない場合はこの番号タイプを International に変更し、接続サービス プロバイダーにより要求された場合は除去と番号タイプ変更の両方を実行しなければなりません。

SIP トランク サービス タイプ

ほとんどの SIP トランクは、他の Cisco Unified CM、Cisco Unified Border Element、Cisco Unified Gateway などのさまざまな SIP サーバに接続できる、汎用目的トランクです。これらの汎用目的トランク以外に、Unified CM には、特定のサービス専用の SIP トランクも用意されています。これらの特殊目的トランクによって、次のようなテクノロジーを使用できるようになります。

- Cisco Intercompany Media Engine（IME）

  「Cisco Intercompany Media Engine」（P.5-35）を参照してください。

- Cisco IOS Service Advertisement Framework（SAF）による Cisco Unified Communications Call Control Discovery（CCD; コール制御ディスカバリ）

  「Service Advertisement Framework（SAF）」（P.3-64）を参照してください。

- Cisco Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）

  「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10）を参照してください。

SIP トランクの設計上の考慮事項

SIP クラスタ間トランクの考慮事項

クラスタ間トランク接続の場合、各クラスタに設定されている SIP トランクは標準の Unified CM Group または [Run on all Active Unified CM Nodes] 機能を使用している可能性があります。各機能を使用する理由は、一般的にクラスタで使用されている Unified CM バージョンによって決定されます。または、WAN 上にクラスタリングが配置され、地理的な位置に基づくコールの分配が必要な場合に決定されます。

SIP クラスタ間トランクによる標準の Unified CM Group の使用

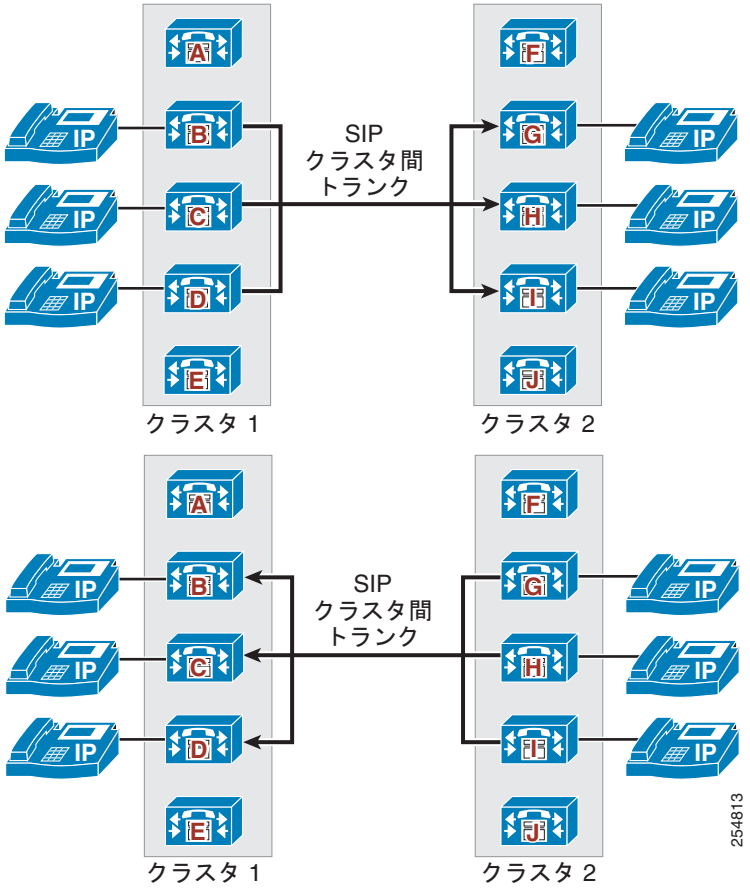
この種類の配置では、標準の Unified CM Group は各クラスタ内の SIP クラスタ間トランクによって使用されます。標準の Unified CM Group を使用してこの種類のトランクを定義する場合、リモート クラスタの宛先 IP アドレスとして、最大 3 つのリモート Unified CM サーバを定義する必要があります。

トランクによって、定義されているすべてのリモート Unified CM サーバで自動的にロード バランシングされます。リモート クラスタでは、Unified CM Group 内で、最初のクラスタ内のリモート宛先 Unified CM サーバとして定義されているものと同じ Unified CM ノードを持つ、対応する SIP クラスタ間トランクを設定することが重要です。

たとえば、クラスタ 1 にクラスタ 2 への SIP トランクがあり、クラスタ 2 にクラスタ 1 への SIP トランクがある場合は、次の設定が必要になります（図 14-10 を参照）。

- クラスタ 1
  - サーバ B、C、および D を、クラスタ 2 への SIP トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - SIP トランクには、宛先としてクラスタ 2 のリモート サーバ G、H、および I が設定されています。
- クラスタ 2
  - サーバ G、H、および I を、クラスタ 1 への SIP トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - SIP トランクには、宛先としてクラスタ 1 のリモート サーバ B、C、および D が設定されています。

図 14-10　Unified CM Group による SIP クラスタ間トランク



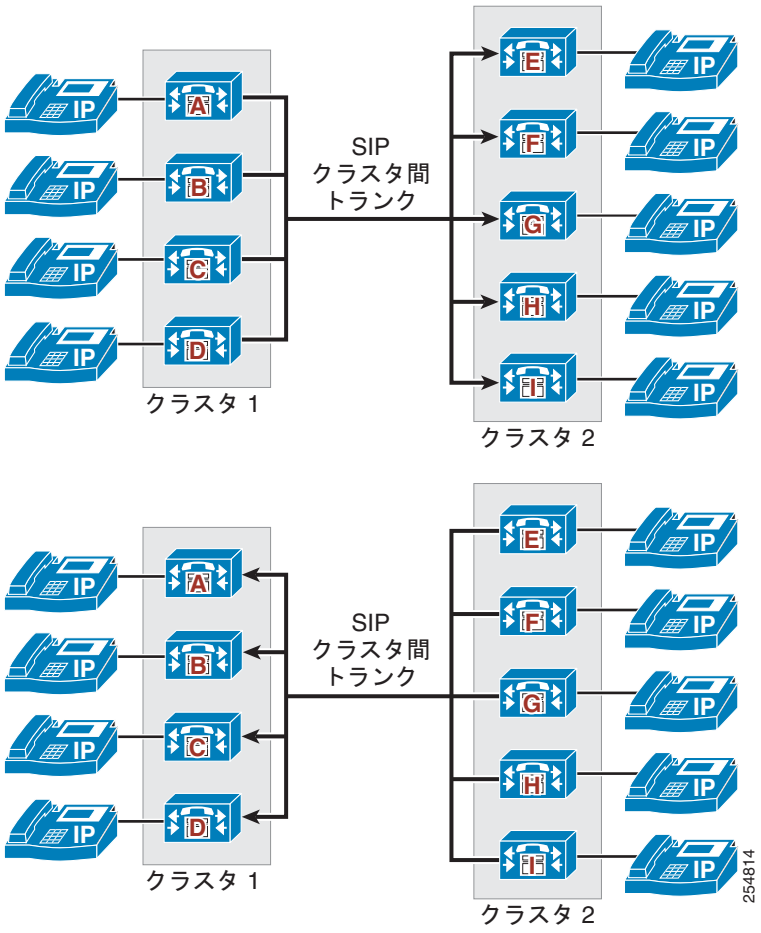
SIP クラスタ間トランクによる [Run on All Active Unified CM Nodes] の使用

この種類の配置では、各クラスタ内の SIP クラスタ間トランクによって [Run on all Active Unified CM Nodes] が使用されます。この種類のトランクを定義する場合、同一の宛先クラスタに最大 16 個のリモート Unified CM サーバを定義できます（定義する必要があるリモート サーバの数は、宛先クラスタ内のアクティブな Unified CM ノード数によって変わります）。トランクによって、定義済みリモート宛先サーバ全体のコールが自動的にロード バランシングされます。リモート クラスタの場合、[Run on all Active Unified CM Nodes] が設定された対応する SIP クラスタ間トランクを設定することが重要です。この場合、これらのノードは、最初のクラスタのリモート宛先 Unified CM サーバとして定義されます。

たとえば、クラスタ 1（4 つのアクティブなノードあり）にクラスタ 2 に対する SIP トランクがあり、クラスタ 2（5 つのアクティブなノードあり）にクラスタ 1 に対する SIP トランクがある場合、次の設定が必要です（図 14-11 を参照）。

- クラスタ 1 には、4 つのアクティブな Unified CM ノードがあります（A、B、C、および D）。
  - [Run on all Active Unified CM Nodes] をイネーブルにすると、サーバ A、B、C、および D では、アクティブな SIP トランク デーモンがクラスタ 2 に対する SIP トランクと関連付けられます。
  - SIP トランクには、宛先としてクラスタ 2 のリモート サーバ E、F、G、H、および I が設定されています。
- クラスタ 2 には、5 つのアクティブな Unified CM ノードがあります（E、F、G、H、および I）。
  - [Run on all Active Unified CM Nodes] をイネーブルにすると、サーバ E、F、G、H、および I では、アクティブな SIP トランク デーモンがクラスタ 1 に対する SIP トランクと関連付けられます。
  - SIP トランクには、クラスタ 1 のリモート サーバ A、B、C、および D が設定されています。

図 14-11　すべてのアクティブな Unified CM ノードで実行される SIP クラスタ間トランク



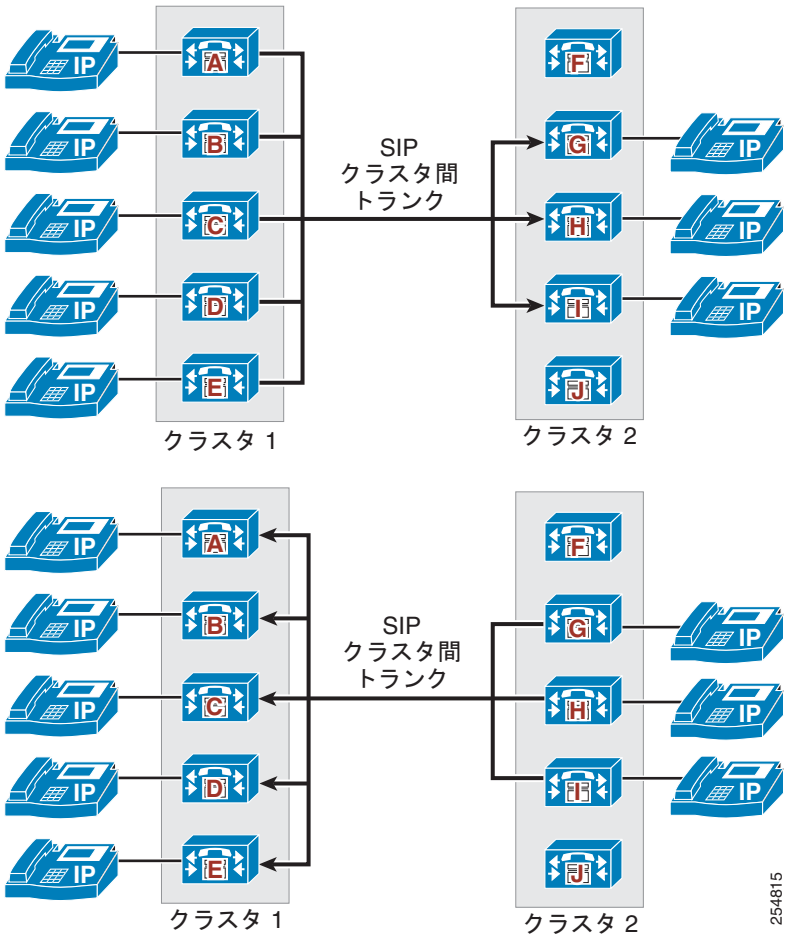
SIP クラスタ間トランクによる標準の Unified CM Group および [Run on All Active Unified CM Nodes] の使用

この種類の配置では、1 つのクラスタ内の SIP クラスタ間トランクで [Run on all Active Unified CM Nodes] が使用され、他のクラスタ内の SIP クラスタ間トランクでは標準の Unified CM Group が使用されます。このようなトランクを設定する場合、定義するリモート Unified CM サーバの宛先の数は、宛先クラスタの対応するトランクに関連付けられたアクティブな Unified CM ノードの数と一致する必要があります。トランクによって、定義されているすべてのリモート宛先 Unified CM サーバでコールが自動的にロード バランシングされます。リモート クラスタの場合、アクティブな SIP デーモンを持つ Unified CM ノードがある、対応する SIP クラスタ間トランクを設定することが重要です。この場合、これらのノードは、最初のクラスタのリモート宛先 Unified CM サーバとして定義されます。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります（図 14-12 を参照）。

- クラスタ 1 には、5 つのアクティブな Unified CM ノードがあります（A、B、C、D、および E）。
  - [Run on all Active Unified CM Nodes] をイネーブルにすると、サーバ A、B、C、D、および E では、アクティブな SIP トランク デーモンがクラスタ 2 に対する SIP トランクと関連付けられます。
  - SIP トランクには、宛先としてクラスタ 2 のリモート サーバ G、H、および I が設定されています。
- クラスタ 2 には 5 つのアクティブな Unified CM ノードがあり、ノード G、H、および I を含む Unified CM Group と共にクラスタ間トランクを使用しています。
  - サーバ G、H、および I を、クラスタ 1 への SIP トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - SIP トランクには、宛先としてクラスタ 1 のリモート サーバ A、B、C、D、および E が設定されています。

図 14-12　Unified CM Groups および [Run on All Active Unified CM Nodes] を使用する SIP クラスタ間トランク



マルチクラスタ配置のトランクの種類と機能に関する推奨事項

すべて Unified CM 8.5 以降のリリースを実行する複数のクラスタ

すべてのクラスタが Unified CM 8.5 以降のリリースを実行している場合、適用可能な場合は次の SIP トランク機能を使用する必要があります（図 14-13 を参照）。

- SIP OPTIONS ping
- SIP ディレイド オファー
- 音声およびビデオをサポートするアーリー オファー（必要に応じて MTP を挿入）
- [Run on All Active Unified CM Nodes]
- 複数の宛先 IP アドレス
- QSIG over SIP
- SIP の正規化および透過性

これらの機能を展開すると、MTP の使用が軽減され、ハイ アベイラビリティを実現し、コールを均等に分配し、SIP トランク障害をダイナミックに検出できます。通常、ディレイド オファー コールを確立するのに MTP は不要なため、Unified CM SIP トランクからの発信コールでは、ディレイド オファーが適切です。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。

SIP クラスタ間トランクは、Unified CM クラスタ間で音声メディア、ビデオ メディア、および暗号化されたメディアをサポートします。また、上記のすべての機能を使用できます。ディレイド オファー コールを確立するのに MTP は不要なため、クラスタ間トランクでは、SIP ディレイド オファーが適切です。ルート リストで複数のトランクを使用する場合、ルート リストで [Run on All Active Unified CM Nodes] 機能をイネーブルにします。

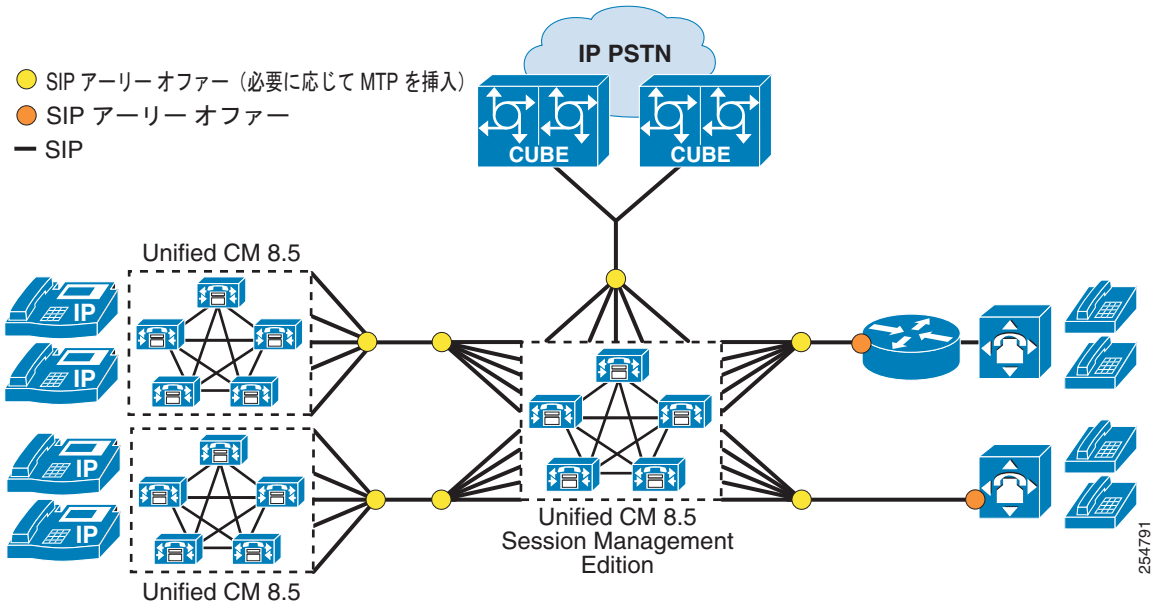
IP PSTN に対する SIP トランクの場合、一般的に、SIP アーリー オファーはサービス プロバイダーによって要求され、ほとんどのプロバイダーは音声コールのみをサポートします。ただし、必要に応じて、ビデオ コールおよび暗号化されたメディアもサポートされます。SIP アーリー オファーがサービス プロバイダーによって要求される場合、Unified CM SIP トランクでアーリー オファーを設定する代わりに Cisco Unified Border Element（アーリー オファーに対する SIP ディレイド オファー機能）を使用できます。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。サービス プロバイダーの IP PSTN ネットワークに接続する場合、エンタープライズ エッジ Session Border Controller として Cisco Unified Border Element を使用し、企業ネットワークとサービス プロバイダーのネットワーク間に制御された境界およびセキュリティ ポイントを用意することが強く推奨されます。

サードパーティのユニファイド コミュニケーション システムに対する SIP トランクは、音声メディア、ビデオ メディア、および暗号化されたメディアをサポートする可能性があります。エンド システムの機能を確認して、サポートする SIP トランク機能およびメディア機能を判断してください。ディレイド オファー コールを確立するのに MTP は不要なため、Unified CM SIP トランクからの発信コールでは、ディレイド オファーが適切です。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。

（注）　Cisco IOS ゲートウェイ上の SIP トランクは、常にアーリー オファーを送信します。

IP PSTN およびサードパーティのユニファイド コミュニケーション システムに対する SIP トランク接続の場合、正規化と透過性のスクリプトを使用して、SIP の相互運用性に関する問題に対処できます。

図 14-13　Unified CM 8.5 以降による マルチクラスタ配置



Unified CM 8.5 以前のリリースを実行するマルチクラスタ

リーフ クラスタが、Unified CM 8.5 と、旧リリースの Unified CM を組み合わせて実行している場合、次のトランクの種類と機能を使用する必要があります（図 14-14 を参照）。

リーフ クラスタが旧バージョン（8.5 よりも前）の Unified CM を実行し、音声、ビデオ、および暗号化が必要な場合、必要に応じて、H.323 Slow Start クラスタ間トランクおよび Annex M1（QSIG）を使用します。標準の Unified CM Group および最大 3 つの宛先 IP アドレスを使用して、1 つまたは複数の H.323 Slow Start クラスタ間トランクを配置します。ルート リストで複数のトランクを使用する場合、ルート リストの Unified CM Group に含まれるプライマリ サーバが、関連する発信 H.323 トランクと同じノードに存在しないように、ルート ローカル ルール（前述を参照）を設定します。

Unified CM 8.5 を実行するリーフ クラスタの場合、SIP ディレイド オファー クラスタ間トランクを使用し、[Run on All Active Unified CM Nodes] をイネーブルにし、複数の宛先 IP アドレスおよび SIP OPTIONS ping を使用して、ハイ アベイラビリティと均等なコールの分配を実現します。ルート リストで複数のトランクを使用する場合、ルート リストで [Run on All Active Unified CM Nodes] 機能をイネーブルにします。

Unified CM 8.5 リーフ クラスタで SIP ディレイド オファー クラスタ間トランクを使用し、旧バージョンの Unified CM を使用するリーフ クラスタで H.323 Slow Start クラスタ間トランクを使用すると、クラスタ間で音声コール、ビデオ コール、および暗号化コールを実行でき、必要な MTP 数が軽減されます（MTP が挿入されるのは、DTMF の変換、トランスコーディングなどに必要な場合のみです）。

IP PSTN に対する SIP トランクの場合、一般的に、SIP アーリー オファーはサービス プロバイダーによって要求され、ほとんどのプロバイダーは音声コールのみをサポートします。ただし、必要に応じて、ビデオ コールおよび暗号化されたメディアもサポートされます。SIP アーリー オファーがサービス プロバイダーによって要求される場合、Unified CM SIP トランクでアーリー オファーを設定する代わりに Cisco Unified Border Element（アーリー オファーに対する SIP ディレイド オファー機能）を使用できます。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。サービス プ

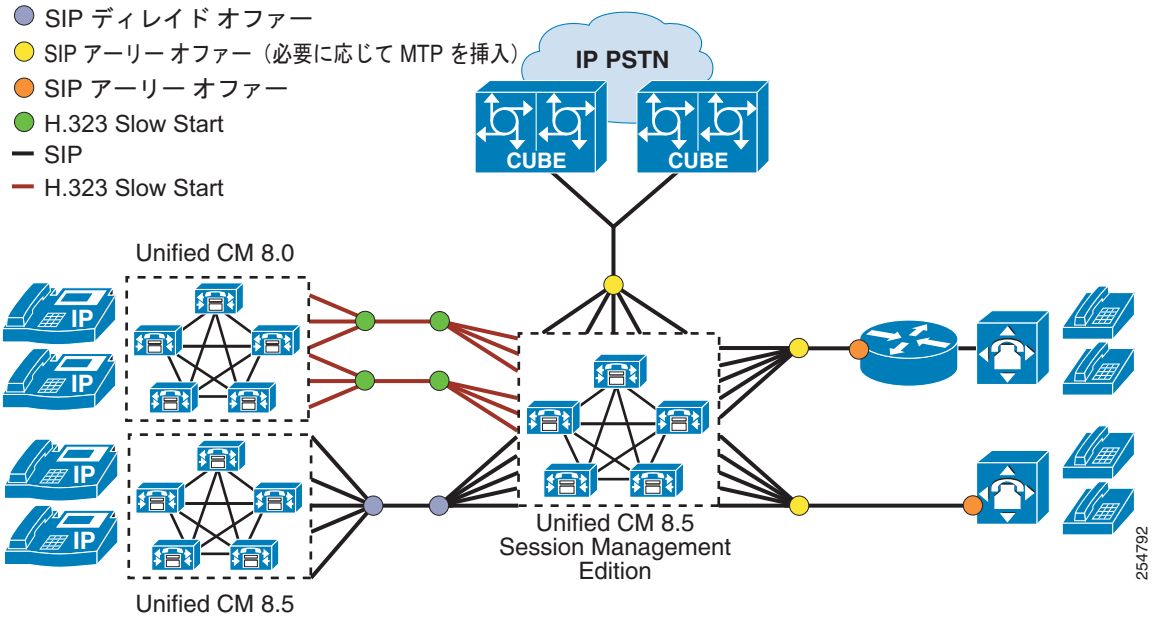
ロバイダーの IP PSTN ネットワークに接続する場合、エンタープライズ エッジ Session Border Controller として Cisco Unified Border Element を使用し、企業ネットワークとサービス プロバイダーのネットワーク間に制御された境界およびセキュリティ ポイントを用意することが強く推奨されます。

サードパーティのユニファイド コミュニケーション システムに対する SIP トランクは、音声メディア、ビデオ メディア、および暗号化されたメディアをサポートする可能性があります。エンド システムの機能を確認して、サポートする SIP トランク機能およびメディア機能を判断してください。ディレイド オファー コールを確立するのに MTP は不要なため、Unified CM SIP トランクからの発信コールでは、ディレイド オファーが適切です。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。

（注）　Cisco IOS ゲートウェイ上の SIP トランクは、常にアーリー オファーを送信します。

IP PSTN およびサードパーティのユニファイド コミュニケーション システムに対する Unified CM SIP トランク接続の場合、正規化と透過性のスクリプトを使用して、SIP の相互運用性に関する問題に対処できます。

図 14-14　Unified CM 8.5 以前のリリースによる マルチクラスタ配置



WAN 上のクラスタリングに関するトランク設計の考慮事項

空間的な復元力と冗長性のために WAN 上でクラスタリングを配置する場合、OPTIONS ping、音声およびビデオのためのアーリー オファーのサポート（必要に応じて MTP を挿入）、QSIG などの SIP トランク機能を必要に応じて適切に使用できます。[Run on all Unified CM Nodes] や複数の宛先アドレスなどの SIP および H.323 トランク機能は、主にトランクが着信コールの識別と受け入れに使用するメカニズムのため、慎重に使用する必要があります（着信の送信元 IP アドレスが、宛先 IP アドレスとして定義されているアドレスの 1 つに一致する場合、トランクはコールを受け入れます）。

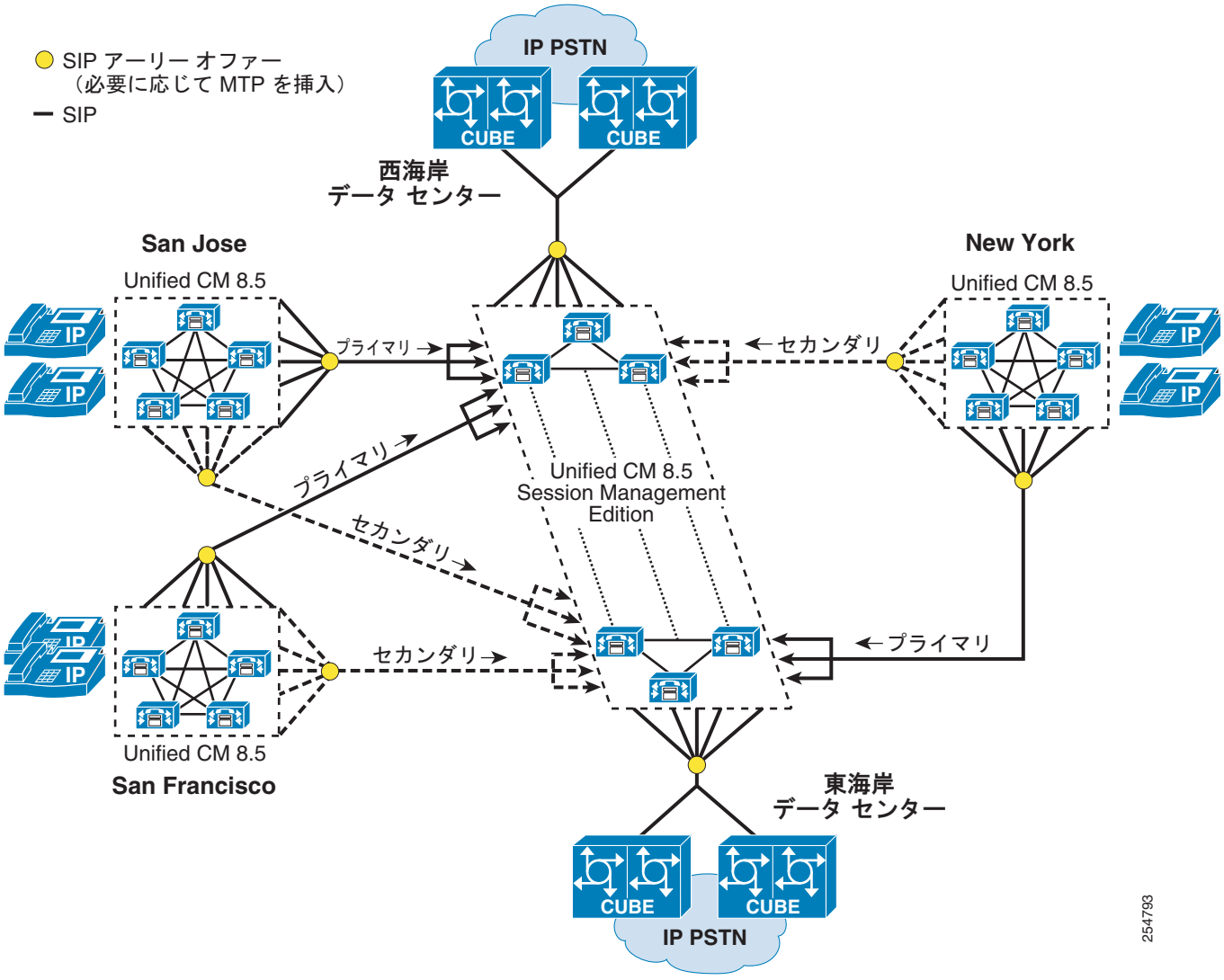
地理的な位置に基づいて、異なるグループの Unified CM ノードにコールをルーティングする必要がある、WAN 配置上のクラスタリングの場合、着信と発信の両方についてトランク設定を慎重に検討する必要があります。この点については、WAN 上でクラスリングされる Unified CM Session Management Edition クラスタを例に使用して、次の項で説明します。

リーフ クラスタ トランクがある WAN 上のクラスタリングに関する設計ガイドライン

各リーフ クラスタでルート リストに複数の SIP トランクを作成し、優先順位を付けて、各データ センター内の Unified CM Session Management Edition ノードの各グループにコールを分配し、すべてのノードでルート リストを実行します（図 14-15 を参照）。

各リーフ クラスタの SIP トランクで [Run on all Nodes] をイネーブルにします（各 SIP トランクは一意の着信ポート番号を使用する必要があります）。地理的なコール分配のために、トランクごとに宛先 IP アドレスを定義します。

図 14-15　リーフ クラスタから Unified CM Session Management Edition へのコール



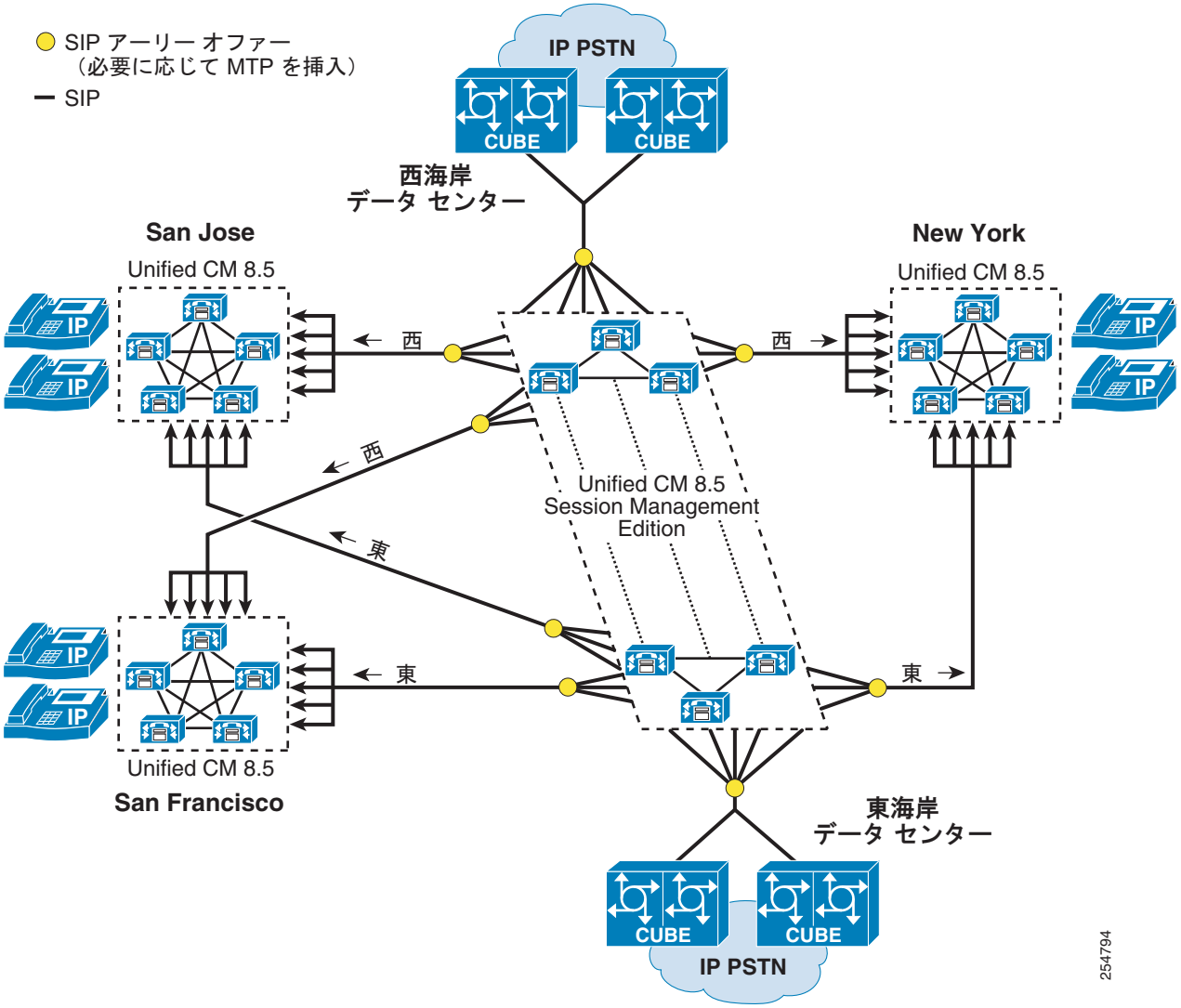
Unified CM Session Management Edition クラスタ トランクがある WAN 上のクラスタリングに関する設計ガイドライン

Unified CM Session Management Edition クラスタのルート リストに複数の SIP トランクを作成し、優先順位を付けて、各データ センター内の Unified CM Session Management Edition ノードの各グループからリーフ クラスタに対してコールを開始します。すべてのノードでルート リストを実行します（図 14-16 を参照）。

各 SIP トランクで標準の Unified CM Group を使用し、リーフ クラスタの各コール処理ノードについて宛先 IP アドレスとポート番号を定義します。

着信トランク コールの場合、ローカル ルート グループを使用して、同じデータ センターのトランク上で発信をルーティングします。

図 14-16　Unified CM Session Management Edition からリーフ クラスタに対するコール



その他の SIP トランク配置に関する考慮事項

SIP ベースの PBX またはサービス プロバイダーの IP PSTN 接続などのサードパーティのデバイスに対する接続がある Unified CM SIP トランクからの発信コールの場合、ディレイド オファー コールを確立するのに MTP は不要なため、ディレイド オファーが適切です（ただし、DTMF トランスポート タイプの不一致が、着信および発信のエンドポイント間に存在する場合を除きます。この場合、Unified CM は MTP をダイナミックに挿入します）。Unified CM SIP トランクへの着信コールでは、アーリー オファーまたはディレイド オファー（あるいはアーリー オファーとディレイド オファー両方の混在）を使用できます。

監視されている場合、音声クリッピングは、トランクで PRACK を有効にすることで、最小化または削減できます。このパラメータは、Cisco CallManager サービスのサービス パラメータで有効にできます（SIP Rel1XX Enabled）。

セキュリティ設定や SIP トランクを介して受け入れられるメッセージのタイプなどの他の操作パラメータは、SIP Trunk Security Profile で有効にできます。ここでは、TLS およびダイジェスト認証のパラメータだけでなく、トランクが Presence Subscription、Out-Of-Dialog REFER メッセージ、Replaces ヘッダー、または Unsolicited Notification メッセージを受け入れるかどうかを指定するパラメータも設定できます。

SIP トランクは、SIP プレコンディションを使用するトポロジ対応の RSVP コール アドミッション制御と、基礎となる WAN トポロジを意識しないロケーションベースのコール アドミッション制御をサポートします。

サービス プロバイダー ネットワークに接続する場合、Cisco Unified Border Element を使用することを推奨します。企業とサービス プロバイダーのネットワーク間への境界ポイント提供のほか、Cisco Unified Border Element は、2 つのネットワーク間でのアドレスの隠蔽と SIP シグナリング相互運用性の拡張にも使用できます。

Cisco Unified Border Element の詳細については、次のサイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps5640/index.html

H.323 トランクの概要

H.323 トランクは、ゲートウェイ、Unified CM Session Management Edition、ゲートキーパー、Unified Communications アプリケーション、その他の Unified CM クラスタなど、他の H.323 デバイスに接続を提供します。Cisco Unified CM 8.5 以降のリリースでは、すべての H.323 トランク タイプについて、次のコール ルーティングの強化がありました。

- すべての Unified CM ノードでルート リストを実行

この機能に加え、H.323 非ゲートキーパー制御のクラスタ間トランクも、次の機能をサポートします。

- すべての Unified CM ノードで実行
- 各トランクで最大 16 の宛先 IP アドレスをサポート

これら 2 つの機能によって、Unified CM クラスタからの発信の分配が改善され、クラスタ間に必要な H.323 非ゲートキーパー制御のクラスタ間トランク数が軽減されます。

これらの機能とその動作について詳しくは、この項で後述します。

H.323 トランクの新規拡張機能の全リストについては、次の Web サイトで入手可能な最新の Cisco Unified Communications Manager の製品リリース ノートを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html

一般的な H.323 クラスタ間トランク配置に関する考慮事項

Unified CM 8.5 よりも前のリリースでは、H.323 Annex M1 トランクは Unified CM クラスタ間の接続によく使用される選択肢でした。Unified CM SIP トランクは、H.323 クラスタ間トランクと比較してより多くの機能を提供しているため、クラスタ間トランクの接続に使用するプロトコルとして SIP が選択されるようになりました。ただし、旧ソフトウェア バージョンを使用する Unified CM クラスタの多数は、H.323 Annex M1 クラスタ間トランクで配置される可能性が高いため、このようなクラスタに使用するクラスタ間トランク タイプが決まる可能性があります。

H.323 トランクの基本的な操作

H.323 トランクは、他の Unified CM クラスタや、ゲートウェイなどの他の H.323 デバイスに対する接続性を提供します。H.323 トランクは、Unified CM がクラスタ内通信用にサポートするオーディオおよびビデオ コーデックのほとんどをサポートします。ただし、ワイドバンド オーディオおよびワイドバンド ビデオについてはサポートしません。

H.323 トランクは、Empty Capabilities Set（ECS）を使用して、保留 / 保留解除や転送などの付加コール サービスを提供します。この方式は、メディア ストリーム（またはチャネル）を停止または終了し、同一または別のエンドポイント アドレスに対してメディア ストリームを開始または起動するための標準の H.245 メカニズムです。この方式を使用すると、Unified CM は、コールをアクティブにしたままでも、メディア ストリームの送信元および宛先を迅速に制御できます。

たとえば、H.323 トランクを使用した 2 つのクラスタ（A と B）間のコールについて考えます。クラスタ A のユーザがクラスタ B のユーザを保留にした場合、2 人のユーザ間のメディア ストリームは終了し、クラスタ B のユーザはクラスタ A の Music On Hold（MoH; 保留音）サーバに接続されます。MoH サーバは、ユーザにメディア（音楽ファイル）を送信するよう指示されます。クラスタ A のユーザがコールを保留解除すると、MoH ストリームが終了し、2 人のユーザ間で双方向メディア ストリームが再開されます（Unified CM は、付加コール サービス用に H.450 をサポートしていません）。このケースでは、MoH は ECS 動作の一例です。H.323 トランクはマルチキャスト MoH をサポートするため、H.323 トランクの Media Resource Group List（MRGL; メディア リソース グループ リスト）は、ユニキャストおよびマルチキャスト両方の MoH 送信元を含む可能性があります（詳細については、「保留音」（P.17-26）を参照してください）。

H.323 トランク上のコールに使用される帯域幅を制御するには、Unified CM で設定される、各トランクに割り当てられるリージョンを使用します。音声についてはリージョン間の最大音声ビット レートを指定し、ビデオ（音声込み）についてはリージョン間の最大ビデオ コール ビット レート設定を指定することで、コールに割り当てられる帯域幅の量が制限されます。1 つのリージョンと別のリージョン間のコールは、指定された帯域幅の制限内にする必要があります。H.323 トランク上でコールを発信するデバイスが、より限定的なリージョン内にある場合や、ビデオなどの特定のコーデックをサポートしない場合、そのデバイスはそのコールに使用可能なコーデックのサブセットになっています。

H.323 トランク タイプ

Unified CM では、次の主要なタイプの H.323 トランクを設定できます。

- 「クラスタ間トランク（非ゲートキーパー制御）」（P.14-39）
- 「クラスタ間トランク（ゲートキーパー制御）」（P.14-46）
- 「H.225 トランク（ゲートキーパー制御）」（P.14-47）

これらの各 H.323 トランク タイプとその具体的な設計の考慮事項については、次の項で説明します。

クラスタ間トランク（非ゲートキーパー制御）

このトランクは、最も単純な H.323 トランク タイプで、単一のマルチクラスタ キャンパスまたは分散型コール処理配置で他の Unified CM クラスタに接続するために使用されます。このトランクは、コール アドミッション制御にゲートキーパーを使用しません。ただし、帯域幅制御が必要な場合は、Unified CM で設定されたロケーションを使用できます。

Cisco Unified CM 8.5 以降のリリースでは、次のトランク機能と、H.323 非ゲートキーパー制御のクラスタ間トランクに関するコール ルーティングの強化をサポートしています。

- すべてのアクティブな Unified CM ノードで実行
- 各トランクで最大 16 の宛先 IP アドレスをサポート
- すべての Unified CM ノードでルート リストを実行

これらの機能については、次の項で説明します。

すべてのアクティブな Unified CM ノードで実行される H.323 非ゲートキーパー クラスタ間トランク

H.323 非ゲートキーパー クラスタ間トランクで [Run on all Active Unified CM Nodes] オプションがオンの場合、Unified CM は各コール処理 Unified CM Group で H.323 トランク デーモンのインスタンスを作成します。これによって、H.323 非ゲートキーパー クラスタ間トランク コールは、どのコール処理サブスクライバでも発着信できます。[Run on all Active Unified CM Nodes] をイネーブルにすると、発信 H.323 非ゲートキーパー クラスタ間トランク コールは、（電話やトランクなどからの）着信を受信したのと同じサーバから発信されます。すべての Unified CM H.323 非ゲートキーパー クラスタ間トランクと同様に、トランクに関連付けられている H.323 デーモンは、トランクの宛先アドレス フィールドに定義されている IP アドレスを持つエンド システムからの着信のみを受け入れます。大量のコールを処理するために、H.323 非ゲートキーパー クラスタ間トランクが必要な場合、すべてのノードで H.323 非ゲートキーパー クラスタ間トランクを実行することが推奨されます。これによって、発信および着信の分配を、クラスタ内のすべてのコール処理サブスクライバに均等に分散できます。ただし、（SIP トランクとは異なり）H.323 非ゲートキーパー クラスタ間トランクでは固定の宛先ポートと一時的な送信元を使用するため、H.323 非ゲートキーパー クラスタ間トランクはポート番号を使用して区別できません。H.323 非ゲートキーパー クラスタ間トランクを設定し、[Run on all Active Unified CM Nodes] をイネーブルにする場合、各トランクが異なる宛先 IP アドレスを使用するようにしてください。

1 つの H.323 非ゲートキーパー クラスタ間トランクあたり最大 16 の宛先 IP アドレス

H.323 非ゲートキーパー クラスタ間トランクには、最大 16 の宛先 IP アドレスを設定できます。追加の宛先 IP アドレスをサポートしているため、2 つの Unified Communications システム間のコール分配のために、ルート リストおよびルート グループに関連付けられた複数のトランクを作成する必要性が軽減されます。結果として、Unified CM トランク設計が単純になります この機能は、[Run on all Active Unified CM Nodes] 機能と併用できます。ただし、Unified CM H.323 非ゲートキーパー クラスタ間トランクに関連付けられた H.323 デーモンの場合、トランクの宛先アドレス フィールドに定義された IP アドレスを持つエンド システムからの着信のみを受け入れる点に注意してください。

すべてのアクティブな Unified CM ノードで実行されるルート リスト

これは具体的には H.323 非ゲートキーパー クラスタ間トランク機能ではありませんが、すべてのノードでルート リストを実行すると、ルート リストおよびルート グループ内のトランクに利点があります。ルート ローカル ルールを使用してすべてのノードでルート リストを実行すると、発信の分配が改善され、不要なクラスタ内トラフィックを回避できます。

ルート リストの場合、ルート ローカル ルールは次のように動作します。

ルート リストおよび関連するルート グループとトランクを使用する発信の場合、登録されている電話または着信トランクからのコールが、発信に選択されたトランクに関連付けられたルート リスト インスタンスがあるノードに到達したときに、選択した発信トランクのインスタンスがルート リストと同じノードに存在するかどうかが Unified CM によって確認されます。存在する場合、Unified CM はそのノードを使用して発信トランク コールを確立します。

ルート リストと選択した発信トランクの両方で [Run on all Active Unified CM Nodes] がイネーブルの場合、発信の分配は、着信が到達したノードによって決定されます。すべてのノードでの実行ではなく、選択した発信トランクが Unified Group を使用すると、選択した発信トランクのインスタンスが、着信が到達した同じノードに存在する場合に、Unified CM はルート ローカル ルールを適用します。トランクのインスタンスがそのノードに存在しない場合、Unified CM は（クラスタ内の）コールをトランクがアクティブなノードに転送します。

ルート リストで [Run on all Active Unified CM Nodes] をイネーブルにしていない場合､ルート リストはクラスタ内の 1 つのノード（ルート リストの Unified Group のプライマリ ノード）でアクティブになり、ルート ローカル ルールはそのノードに適用されます。

一般的な推奨事項として、[Run on all Active Unified CM Nodes] はすべてのルート リストでイネーブルにしてください

H.323 非ゲートキーパー クラスタ間トランクに関する設計ガイドライン

クラスタ間トランクの接続の場合、各クラスタに設定されている H.323 非ゲートキーパー クラスタ間トランクは標準の Unified CM Group または [Run on all Active Unified CM Nodes] 機能を使用している可能性があります。各機能を使用する理由は、一般的にクラスタで使用されている Unified CM バージョンによって決定されます。または、WAN 上にクラスタリングが配置され、地理的な位置に基づくコールの分配が必要な場合に決定されます。

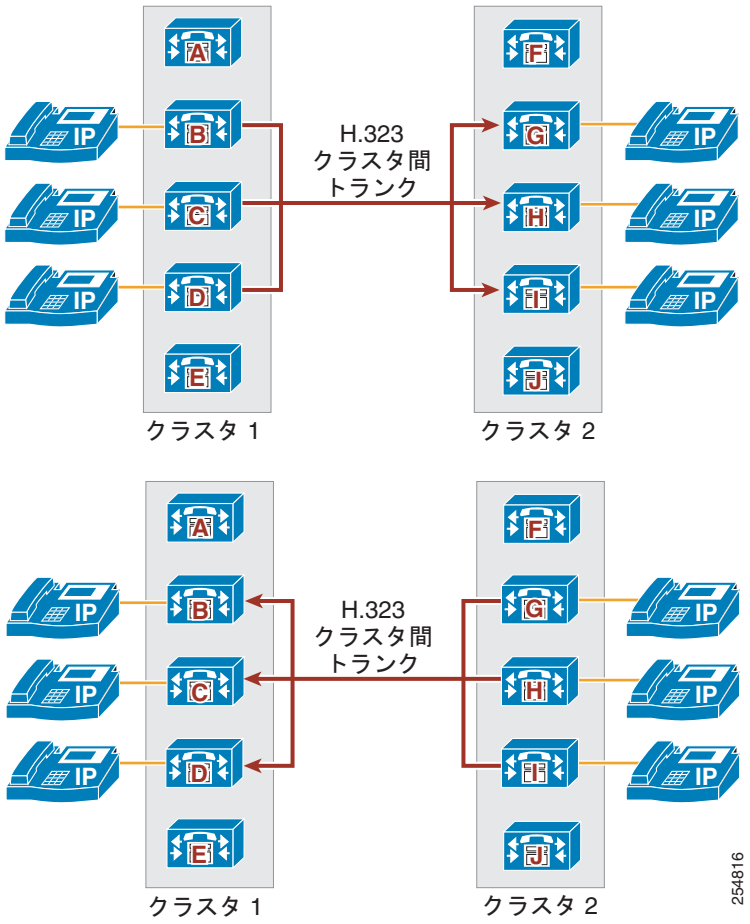
H.323 非ゲートキーパー クラスタ間トランクによる標準の Unified CM Group の使用

この種類の配置では、標準の Unified CM Group は各クラスタ内の H.323 非ゲートキーパー クラスタ間トランクによって使用されます。標準の Unified CM Group を使用してこの種類のトランクを定義する場合、宛先クラスタで最大 3 つのリモート Unified CM サーバを定義する必要があります。トランクによって、リモート宛先アドレスとして定義されているすべてのサーバでコールが自動的にロード バランシングされます。リモート クラスタでは、Unified CM Group 内で、最初のクラスタ内のリモート宛先 Unified CM サーバとして定義されているものと同じ Unified CM ノードを持つ、対応するクラスタ間トランク（非ゲートキーパー制御）を設定することが重要です。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります（図 14-17 を参照）。

- クラスタ 1
  - サーバ B、C、および D を、クラスタ 2 への非ゲートキーパー制御トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - 非ゲートキーパー制御トランクには、宛先としてクラスタ 2 のリモート サーバ G、H、および I が設定されています。
- クラスタ 2
  - サーバ G、H、および I を、クラスタ 1 への非ゲートキーパー制御トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、宛先としてクラスタ 1 のリモート サーバ B、C、および D を設定します。

図 14-17　標準の Unified CM Group を使用する H.323 非ゲートキーパー クラスタ間トランク



H.323 非ゲートキーパー クラスタ間トランクによる [Run on All Active Unified Nodes] の使用

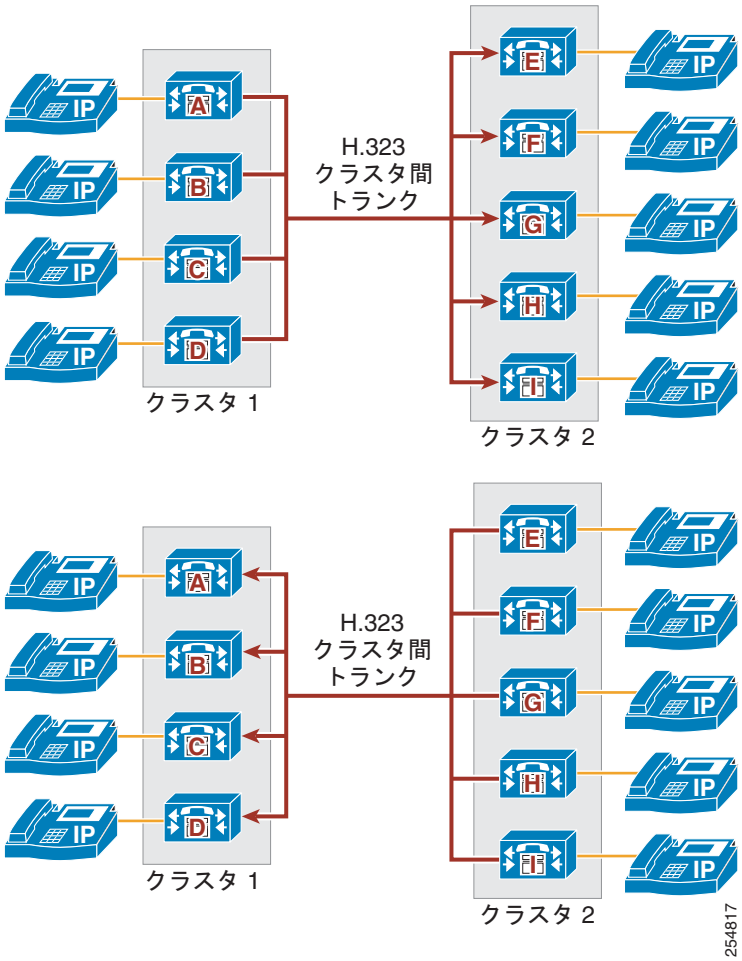
この種類の配置では、各クラスタ内の H.323 非ゲートキーパー クラスタ間トランクによって [Run on all Active Unified CM Nodes] が使用されます。この種類のトランクを定義する場合、同一の宛先クラスタに最大 16 個のリモート Unified CM サーバを定義できます（必要なリモート サーバの数は、宛先クラスタ内のアクティブな Unified CM ノード数によって変わります）。トランクによって、定義済みリモート宛先 Unified CM サーバ全体のコールが自動的にロード バランシングされます。リモート クラスタの場合、[Run on all Active Unified CM Nodes] が設定された対応するクラスタ間トランク（非ゲートキーパー制御）を設定することが重要です。この場合、これらのノードは、最初のクラスタのリモート宛先 Unified CM サーバとして定義されます。

たとえば、クラスタ 1（4 ノード）にクラスタ 2 へのトランクがあり、クラスタ 2（5 ノード）にクラスタ 1 へのトランクがある場合は、次の設定が必要になります（図 14-18 を参照）。

- クラスタ 1 には、4 つのアクティブな Unified CM ノードがあります（A、B、C、および D）。
  - [Run on all active Unified CM Nodes] をイネーブルにすると、サーバ A、B、C、および D では、アクティブな H.323 トランク デーモンがクラスタ 2 に対する非ゲートキーパー制御トランクと関連付けられます。

  - 非ゲートキーパー制御トランクには、宛先としてクラスタ 2 のリモート サーバ E、F、G、H、および I が設定されています。
- クラスタ 2 には、5 つのアクティブな Unified CM ノードがあります（E、F、G、H、および I）。
  - [Run on all active Unified CM Nodes] をイネーブルにすると、サーバ E、F、G、H、および I では、アクティブな H.323 トランク デーモンがクラスタ 2 に対する非ゲートキーパー制御トランクと関連付けられます。
  - 非ゲートキーパー制御トランクに、クラスタ 1 のリモート サーバ A、B、C、および D を設定します。

図 14-18　[Run on All Active Unified Nodes] を使用する H.323 非ゲートキーパー クラスタ間トランク



H.323 非ゲートキーパー クラスタ間トランクによる標準の Unified CM Group および [Run on All Active Unified CM Nodes] の使用

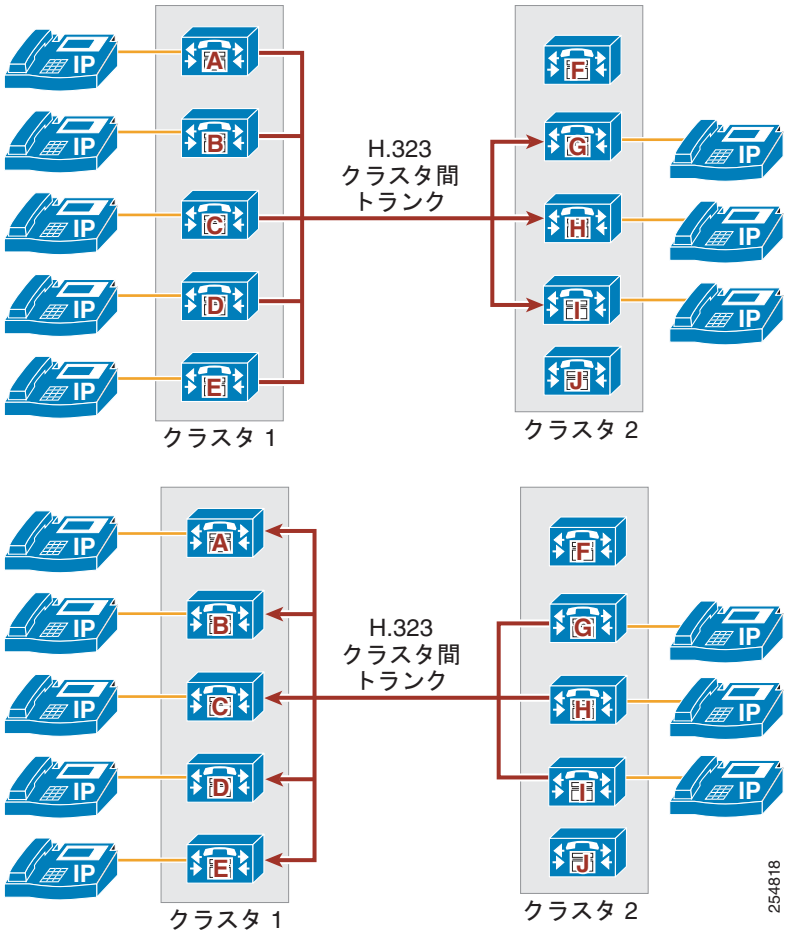
この種類の配置では、1 つのクラスタ内の H.323 非ゲートキーパー クラスタ間トランクで [Run on all Active Unified CM Nodes] が使用され、他のクラスタ内の H.323 非ゲートキーパー クラスタ間トランクでは標準の Unified CM Group が使用されます。このようなトランクを設定する場合、定義するリモート Unified CM サーバの宛先の数は、宛先クラスタの対応するトランクのアクティブな Unified CM ノードの数と一致する必要があります。トランクによって、定義されているすべてのリ

モート宛先 Unified CM サーバでコールが自動的にロード バランシングされます。リモート クラスタの場合、アクティブな H.323 デーモンを持つ Unified CM ノードがある、対応するクラスタ間トランク（非ゲートキーパー制御）を設定することが重要です。この場合、これらのノードは、最初のクラスタのリモート宛先 Unified CM サーバとして定義されます。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります（図 14-19 を参照）。

- クラスタ 1 には、5 つのアクティブな Unified CM ノードがあります（A、B、C、D、および E）。
  - [Run on all Active Unified CM Nodes] をイネーブルにすると、サーバ A、B、C、D、および E では、アクティブな H.323 トランク デーモンがクラスタ 2 に対する非ゲートキーパー制御トランクと関連付けられます。
  - 非ゲートキーパー制御トランクには、宛先としてクラスタ 2 のリモート サーバ G、H、および I が設定されています。
- クラスタ 2 には 5 つのアクティブな Unified CM ノードがあり、ノード G、H、および I を含む Unified CM Group と共にクラスタ間トランクを使用しています。
  - サーバ G、H、および I を、クラスタ 1 への非ゲートキーパー制御トランクに関連付けられたデバイス プールで定義されている Unified CM Group のメンバーとして設定します。
  - H.323 非ゲートキーパー クラスタ間トランクには、宛先としてクラスタ 1 のリモート サーバ A、B、C、D、および E が設定されています。

図 14-19　標準の Unified CM Group と [Run on All Active Unified CM Nodes] を使用する H.323 非ゲートキーパー クラスタ間トランク



非ゲートキーパー制御クラスタ間トランクのハイ アベイラビリティ

H.323 非ゲートキーパー クラスタ間トランクのハイ アベイラビリティと冗長性を提供するには、発信に複数の送信元 Unified CM サーバと、トランクごとに複数の宛先 IP アドレスを使用します。

H.323 非ゲートキーパー クラスタ間トランク コールに対する複数の送信元 Unified CM サーバ

- 標準の Unified CM Group の使用

  個々のトランクに関連付けられている Unified CM Group 内に定義されたノードによって、トランク経由でコールを送受信できるサーバのセットが構成されます。1 つの Unified CM グループには 3 つまでノードを定義できるため、トランク自体のハイ アベイラビリティが確保されます。

- [Run on all Active Unified CM Nodes] の使用

  [Run on all Active Unified CM Nodes] 機能を使用すると、クラスタ内の各コール処理サブスクライバで H.323 トランク インスタンスが作成され、イネーブルになるため、そのノードのトランク上で発信または着信できます。

- 発信の H.323 非ゲートキーパー クラスタ間トランクに関する Unified CM ルート ローカル機能とサブスクライバの選択の影響

  Unified CM のルート ローカル機能は、クラスタ内トラフィックを減らすために設計されています。この機能の動作について説明します。電話機などのデバイスが H.323 クラスタ間トランク ICT 1 上で発信すると、H.323 ICT 1 のインスタンスが、電話機の登録先と同じノードでアクティブな場合、クラスタ内の別のノード上にある別の H.323 ICT 1 インスタンスに対してコールを内部的にルーティングするのではなく、常にこの同居する H.323 ICT 1 インスタンスを使用します。

  ノードの選択に関するルート ローカル機能の影響は、Unified CM Group と [Run on all Active Unified CM Nodes] のいずれがトランクに設定されているかによって変わります。[Run on all Active Unified CM Nodes] を設定したトランクの場合、発信デバイスの登録先ノードは、発信 H.323 クラスタ間トランク コールの発信に使用されます。Unified CM Group がトランクに使用されているときに、発信デバイスが、トランクの Unified CM Group のノードの 1 つに登録されている場合、ルート ローカル ルールが適用されます。発信デバイスが、トランクの Unified CM Group のノードの 1 つに登録されていない場合、Unified CM は、トランクの Unified CM Group のノード上でコールをランダムに分配します。

一般的に、H.323 クラスタ間トランクの場合、[Run on all Active Unified CM Nodes] の使用を推奨します。この方法を使用すると、ノード間のコールの分配が発信元デバイスによって決定され、クラスタ内のトラフィックが最小限に抑えられるためです。

1 つの H.323 非ゲートキーパー クラスタ間トランクあたりの複数の宛先 IP アドレス

単一の H.323 非ゲートキーパー クラスタ間トランクには、最大 16 の宛先 IP アドレスを設定できます。H.323 非ゲートキーパー クラスタ間トランク上で発信するときに、Unified CM では設定済み宛先 IP アドレスにラウンドロビン式の分配を使用します。

[Run on All Active Unified CM Nodes] を使用するときの設計の考慮事項

[Run on All Active Unified CM Nodes] と複数の宛先アドレスを併用する場合、着信を受け入れるには、H.323 トランクで受信した着信の送信元 IP アドレスが、着信トランクに設定されている宛先 IP アドレスと一致する必要があることに注意してください。WAN 設計上にクラスタリングを配置し、地理的なコールの分配およびフェールオーバーが必要な場合、複数のクラスタ間トランク（それぞれ最大 3 つの宛先 IP アドレスを使用）上で標準の Unified CM Group を使用し、さらにルート リストとルート グループを併用します。

H.323 非ゲートキーパー クラスタ間トランクのロード バランシング

H.323 非ゲートキーパー クラスタ間トランクのロード バランシングを設計する場合、コールの送信元ノードと宛先の両方について考慮します。H.323 非ゲートキーパー クラスタ間トランクでは、発信に使用されるノードは、ルート ローカル ルール、発信トランクがアクティブなノード数、およびルート リストを複数の発信トランクと併用するかどうかによって決定されます。次に、これらの考慮事項について説明します。

単一の H.323 非ゲートキーパー クラスタ間トランク上の発信

単一の H.323 非ゲートキーパー クラスタ間トランクは、Unified CM Group で最大 3 つの Unified CM ノードを実行できます。または、クラスタ内のすべてのアクティブな Unified CM ノードで実行できます。発信の送信元ノードを選択するために、Unified CM は次の決定プロセスを適用します。

トランクのインスタンスがすべてのノードで実行される場合、ルート ローカル ルールが適用され、各発信に使用されるノードはコールが到達するノードによって決定されます（たとえば、発信元電話が登録されているノードや、着信トランク コールが到達したノード）。Unified CM Group を使用する場合、ルート ローカル ルールは、トランクの Unified CM Group と同じノードに登録されている発信元デバイスに適用されます。クラスタ内の他のサーバに登録されている発信元デバイスの場合、Unified CM は、トランクの Unified CM Group のノード間でコールを分配します。

Unified CM は、トランクの設定済み宛先アドレス間でラウンドロビン式コールの分配を使用します。1 つの H.323 非ゲートキーパー クラスタ間トランクには、最大 16 の宛先 IP アドレスを設定できます。

複数の H.323 非ゲートキーパー クラスタ間トランク上の発信

H.323 非ゲートキーパー クラスタ間トランクはすべてのアクティブな Unified CM ノードで実行でき、最大 16 の宛先アドレスを設定できるので、一般的に、2 つの Unified Communications システム間でコールを均等に分配するために、複数の H.323 非ゲートキーパー クラスタ間トランクを使用する必要はありません。複数のトランクと、ルート リストおよびルート グループを併用する場合、すべてのアクティブな Unified CM ノードで実行するには、ルート リストをイネーブルにする必要があります。多くの場合、PSTN に対して、または WAN 上のクラスタリング配置の一部として異なるサイトにある Unified CM サーバのグループに対してフェールオーバー機能を提供するために、複数の H.323 トランクとルート リストが併用されます。発信 トランク コールの発信に使用される Unified CM ノードの選択、およびトランクの設定済み宛先 IP アドレス上のコールの分配は、単一のトランクの場合と同様の方法で決定されます。WAN 設計上にクラスタリングを配置し、地理的なコールの分配およびフェールオーバーが必要な場合、複数のクラスタ間トランク（それぞれ最大 3 つの宛先 IP アドレスを使用）と標準の Unified CM Group を、ルート リストおよびルート グループと併用します。

クラスタ間トランク（ゲートキーパー制御）

非ゲートキーパー制御トランクの代わりにクラスタ間ゲートキーパー制御トランクを使用することで、大量の Unified CM クラスタを相互接続できます。ゲートキーパー制御トランクを使用する主な利点は、クラスタとフェールオーバー時間を全体的に管理できることです。非ゲートキーパー制御トランクでは、クラスタ内のサブスクライバ サーバが到達不能になると、コールの試行時に 5 秒（デフォルト）のタイムアウトがあります。クラスタ全体が到達不能になった場合、コール障害または公衆網を介した再ルーティングのいずれかが発生するまでの試行回数は、トランク用に定義されたリモート サーバの数と、ルート リストまたはルート グループ（存在する場合）内のトランクの数によって異なります。リモート サーバと非ゲートキーパー制御トランクの数が多いと、コール遅延が過剰になることがあります。

H.323 ゲートキーパー制御トランクを使用する場合は、ゲートキーパーに登録されている他のすべてのクラスタとゲートキーパーを介して通信できるトランクを 1 つだけ設定します。クラスタまたはサブスクライバが到達不能になった場合、ゲートキーパーは自動的に、コールをクラスタ内の別のサブスクライバに送信するか、または他のサブスクライバが存在しなければコールを拒否します。その結果、ほとんど遅延させることなく、公衆網を介して（必要な場合）コールを再ルーティングできます。単一の Cisco ゲートキーパーを使用すると、100 のクラスタすべてが、それぞれ 1 つのトランクを、相互にコールできるすべてのクラスタに登録できます。クラスタ間ゲートキーパー制御トランクは、他の Unified CM と通信する場合だけ使用する必要があります。これは、このトランクを他の H.323 デバイスで使用すると、付加サービスに問題が発生することがあるためです。

（注） ゲートキーパー制御トランクは、[Run on All Active Unified CM Nodes] 機能をサポートしません。標準の Unified CM Group のみがサポートされます。宛先アドレスは、ゲートキーパーによって Unified CM に返されます。ゲートキーパー制御トランクをルート リストで使用する場合、ルート リストで [Run on All Active Unified CM Nodes] 機能をイネーブルにすることを推奨します。

H.225 トランク（ゲートキーパー制御）

H.225 ゲートキーパー制御トランクは、本質的にはクラスタ間ゲートキーパー制御トランクと同じですが、Unified CM クラスタのほか、ゲートウェイ、会議システム、およびクライアントなどの他の H.323 デバイスと連携動作する機能を持つ点が異なります。この機能は、コールごとに検出メカニズムを通じて実現されます（この検出プロセスの詳細については、「Unified CM における H.323 の動作」（P.14-53）を参照してください）。

（注）　ゲートキーパー制御トランクは、[Run on All Active Unified CM Nodes] 機能をサポートしません。標準の Unified CM Group のみがサポートされます。宛先アドレスは、ゲートキーパーによって Unified CM に返されます。ゲートキーパー制御トランクをルート リストで使用する場合、ルート リストで [Run on All Active Unified CM Nodes] 機能をイネーブルにすることを推奨します。

ゲートキーパー制御トランクのハイ アベイラビリティ

冗長性は、設計の要件に応じて、複数の方法で実現できます。最も簡単に実現するには、ゲートキーパー制御トランクを設定し、そのトランクに割り当てられたデバイス プールに関連付けられている Unified CM Group に、最大 3 つのサブスクライバを割り当てます。この設定により、すべてのサーバが、同じテクノロジー プレフィックスとともに、同じゾーン内の同じゲートキーパーに登録されます。ただし、h323_id に使用される H.323 トランクの名前には、「*_n*」というサフィックスが付加されます。ここで、*n* はクラスタ内のノード番号です。この ID は自動的に生成され、変更できません。単一のトランクを設定しても、ゲートキーパーは、複数のトランク、つまり Unified CM Group 内のサブスクライバごとに 1 つのトランクを登録します。

追加の冗長性要件がある場合は、別のゲートキーパー制御トランクに、Unified CM Group にある別の名前と別のサブスクライバを設定できますが、それ以外のパラメータはすべて最初のトランクと同じになります。この 2 つめのトランクによって、追加のサブスクライバがゲートキーパーに登録されます。

標準のサブスクライバ ペアを構成する 2 台のサーバから Unified CM Group を構成し、このグループを含むデバイス プールを割り当てることを推奨します（サブスクライバの冗長性の詳細については、「コール処理サブスクライバの冗長性」（P.8-18）を参照してください）。各クラスタ全体で完全な冗長性を実現するには、4 つの異なるデバイス プールを使用する 4 つのトランクが必要になります。結果的に、8 つのサブスクライバがゲートキーパーに登録されます（3 つのトランクとさらに大きい Unified CM Group を使用しても同じ結果となります）。

登録時、Unified CM とゲートキーパー間では複数のパラメータが受け渡しされます。Unified CM は、ゲートキーパーの Registration Admission Status（RAS）メッセージ用に、一時的なユーザ データグラム プロトコル（UDP）ポートを使用します。このポートは、通常であれば、UDP 1719 です。ただし、Unified CM は、特定のサーバからの RAS メッセージの発信元での H.323 デーモンを正確に特定できる必要があります。したがって、Unified CM は一定範囲の UDP ポートを使用して、動的に割り当てます。

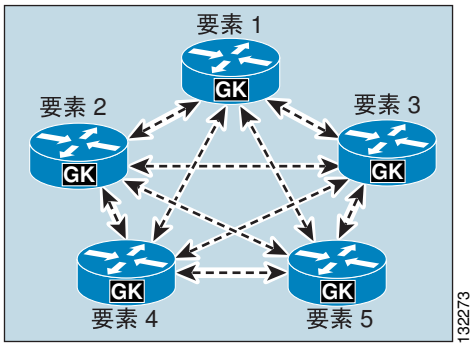
登録プロセス時、トランクは、その Unified CM Group にある他のサブスクライバに関する次の情報を登録します。

- H.225 コール シグナリング ポート
- h323_id
- CanMapAlias サポート
- テクノロジー プレフィックス
- H.225 コール シグナリング アドレス

推奨されるクラスタ化ゲートキーパーが使用されている場合、ゲートキーパーは、代替ゲートキーパー アドレスのリストを返します。このリストは、プライマリ ゲートキーパーで障害が発生した場合や使用可能なリソースが不足した場合に使用されることがあります。

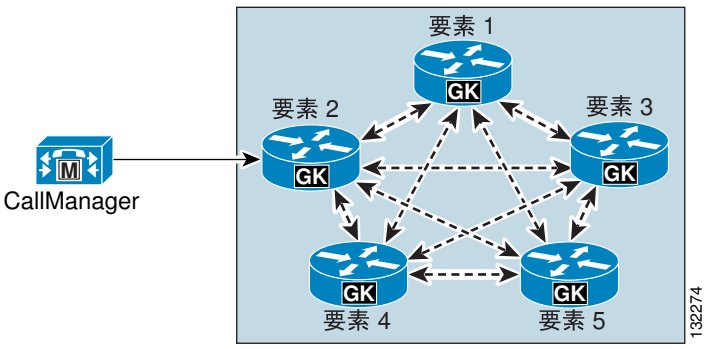
図 14-20 は、Gatekeeper Update Protocol（GUP）を使用して通信する、ゲートキーパーのクラスタを示しています（ゲートキーパーの詳細については、「コール処理」（P.8-1）の章を参照してください）。

図 14-20　ゲートキーパー クラスタ



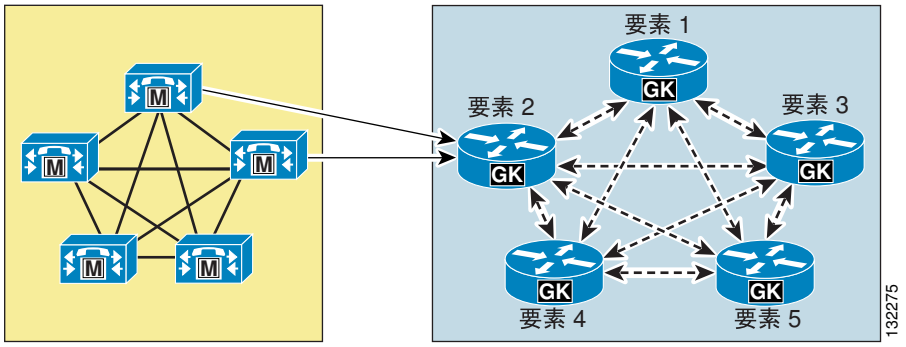
H.323 トランクの Unified CM Group にサブスクライバが 1 つだけ含まれている場合、Unified CM の設定済みゲートキーパーとゲートキーパー クラスタの間の接続は 1 つだけになります（図 14-21 を参照）。

図 14-21　単一の Unified CM サブスクライバを使用する H.323 トランク



トランクに関連付けられた Unified CM Group に複数のサブスクライバが含まれている場合、Unified CM クラスタとゲートキーパー クラスタ間には追加の接続が確立されます（図 14-22 を参照）。

図 14-22　複数の Unified CM サブスクライバを使用する H.323 トランク



このアプローチによってサブスクライバ障害やゲートキーパー障害に対する冗長性が確保されるのは、登録完了後です。これは、トランクの登録時に代替ゲートキーパーの通信が行われるためです。ただし、このアプローチでは、設定済みのゲートキーパーが初期登録時やリセット後に使用不能である場合には、冗長性が確保されません。これは、代替ゲートキーパーのリストがダイナミックであり、データベースに格納されないためです。冗長性のレベルを上げたりロード バランシングを追加したりするには、ゲートキーパー クラスタにある追加のゲートキーパーを Unified CM で設定します。たとえば、元のトランクがエレメント 2 に登録されている場合は、追加のゲートキーパーをエレメント 4 として設定できます（図 14-23 を参照）。

図 14-23　ロード バランシングと追加の冗長性のために設定された追加のゲートキーパー

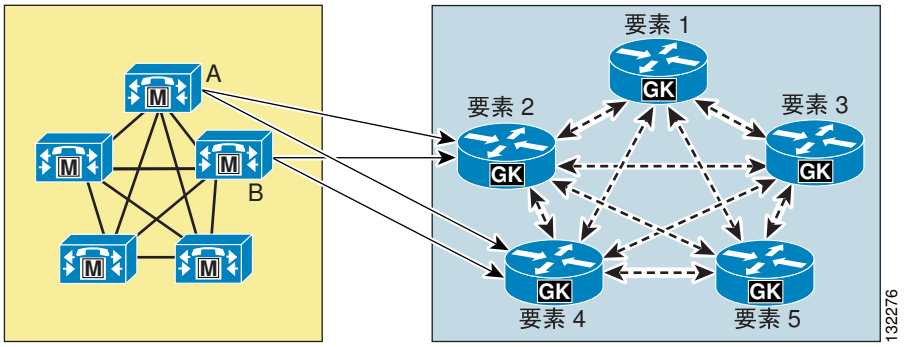


図 14-23 の例の場合、Unified CM の設定には次のコンポーネントが含まれます。

- エレメント 2 とエレメント 4 の 2 つのゲートキーパー
- サブスクライバ サーバ A および B を含む Unified CM Group に対して定義された 2 つの H.323 トランク

このアプローチを使用すると、初期設定時にエレメント 2 またはエレメント 4 が到達不能であっても（つまり、起動中またはトランクのリセット中でも）、引き続き Unified CM クラスタが登録できるようになります。

Unified CM クラスタに着信するコールのロード バランシングは、デフォルトで自動的に行われます。これは、ゲートキーパーが、ゾーン内の登録済みサブスクライバのいずれかをランダムに選択するためです。この動作が期待と異なる場合は、ゲートキーパーで **gw-priority** コンフィギュレーション コマンドを使用して、このデフォルト動作を変更できます（例 14-3 を参照）。

例 14-3　gw-priority コマンドを使用してコールを特定のトランクに送信する

```
gatekeeper
 zone local SJC cisco.com 10.0.1.10
 zone prefix SJC 1408....... gw-priority 10 sjc-trunk_2
 zone prefix SJC 1408....... gw-priority 9 sjc-trunk_3
 zone prefix SJC 1408....... gw-default-priority 0
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
 endpoint ttl 60
```

例 14-3 では、H.323 トランクは Unified CM で sjc-trunk として設定されています。また、クラスタ内のサブスクライバのノード番号を示すために、「_2」と「_3」のサフィックスが Unified CM サブスクライバによって自動的に付加されています。したがって、この例では、最初の選択肢としてノード 2 を使用します。このノードは、このトランクの Unified CM Group において最もプライオリティの高い Unified CM となる必要があります。このケースでは、ノード 3 は 2 番めの選択肢となります。

gw-default-priority 0 を使用するかどうかは任意です。この例で使用したのは、このゾーンで登録するよう不用意に設定される可能性のある他のトランクが一切使用されないようにするためです。

H.323 ゲートキーパー制御トランク上の発信のロード バランシング

Unified CM H.323 ゲートキーパー制御トランクでは、発信に使用されるノードは、ルート ローカル ルール、発信トランクがアクティブなノード数、およびルート リストを複数の発信トランクと併用するかどうかによって決定されます。次に、これらの考慮事項について説明します。

単一の H.323 ゲートキーパー制御トランクを配置する場合の発信のロード バランシング

単一の H.323 ゲートキーパー制御トランク上で発信を開始する場合、ルート ローカル ルールが適用され、Unified CM クラスタ内の次の要素によって、選択されるサーバが決定されます。

- どの Unified CM サーバに、選択されたトランクのアクティブ H.323 デーモンがあるか
- 選択されたサーバのアクティブ H.323 デーモンがある Unified CM サーバに、コールを発信する電話が登録されているか

単一の H.323 ゲートキーパー制御トランクの場合、発信のサーバ選択のルート ローカル プロセスは次のように動作します。

- 選択されたトランクのアクティブ H.323 デーモンが、コールを発信する電話またはデバイスが登録される Unified CM サーバにある場合（つまり、このサーバがトランクの Unified CM Group にリストされているサーバに含まれる場合）、H.323 コールを発信するサーバとして、この Unified CM サーバを使用します。
- 選択されたトランクのアクティブ H.323 デーモンが、コールを発信する電話またはデバイスが登録される Unified CM サーバにない場合、選択されたトランクの Unified CM Group から、ラウンドロビン方式でサーバを 1 台選択します。

ルート リストを H.323 ゲートキーパー制御トランクと共に配置する場合の発信のロード バランシング

発信のトランクを選択するためにルート リストを採用する設定では、すべてのルート リストで [Run on all Active Unified CM Nodes] をイネーブルにします。ルート ローカル ルールを使用してすべてのノードでルート リストを実行すると、発信の分配が改善され、不要なクラスタ内トラフィックを回避できます。ルート リストの場合、ルート ローカル ルールは次のように動作します。

> ルート リスト（および関連するルート グループとトランク）を使用する発信の場合、（登録されている電話または着信トランク）からのコールが、発信トランク コールに関連付けられたルート リスト インスタンスがあるノードに到達したときに、選択した発信トランク コールのインスタンスがルート リストと同じノードに存在するかどうかが Unified CM によって確認されます。存在する場合、Unified CM はそのノードを使用して発信トランク コールを確立します。

ルート リストで [Run on all Active Unified CM Nodes] がイネーブルの場合：Unified CM Group を使用するゲートキーパー制御トランクでは、選択した発信トランクのインスタンスが、着信が到達した同じノードに存在する場合にルート ローカル ルールが適用されます。トランクのインスタンスがそのノードに存在しない場合、Unified CM は（クラスタ内の）コールをトランクがアクティブなノードに転送します。

ルート リストで [Run on all Active Unified CM Nodes] をイネーブルにしていない場合、ルート リストはクラスタ内の 1 つのノード（ルート リストの Unified CM Group のプライマリ ノード）でアクティブになり、ルート ローカル ルールはそのノードに適用されます。

H.323 発信 Fast Start コール接続

長い遅延がある大規模な WAN トポロジを介して IP Phone から発信されるコールに対して、着信側がオフフックで応答する場合、音声クリッピングが発生します。H.323 トランクまたはゲートウェイが、Unified CM サーバから分離されている場合、コールのセットアップ時に大量の H.245 メッセージが交換されるため、著しい遅延が発生します。

Fast Start 機能を使用すると、2 つのパーティ間でメディア接続を確立するために必要な情報が、コール セットアップの H.225 段階で交換されるため、H.245 メッセージが不要になります。この接続では、コール セットアップ時に 1 回のラウンドトリップ WAN 遅延が発生しますが、着信側がコールに応答するときに、発信側で音声クリッピングが発生することはありません。

Unified CM は、H.323 発信 Fast Start コールを確立するために、Media Termination Point（MTP; メディア ターミネーション ポイント）を使用します。Unified CM は、MTP を割り当て、受信チャネルを開くことで、発信 Fast Start コールを開始します。次に、H.323 Fast Connect プロシージャにより、Fast Start 要素を含む SETUP メッセージが着信側エンドポイントに送信されます。この Fast Start 要素には、MTP の受信チャンネルに関する情報が含まれています。

デフォルトでは、H.323 Fast Start は無効になります。H.323 Fast Start を有効にするには、H.323 トランクで [MTP Required] および [Enable Outbound FastStart] のチェックボックスをオンにし、目的の [Codec For Outbound Fast Start] を選択します。また、[Enable Inbound FastStart] チェックボックスとは別に、着信 Fast Start が有効になっていることに注意してください（着信 Fast Start に MTP またはコーデックの選択は必要ありません）。

（注）　H.323 Fast Start が有効の場合、各発信 H.323 トランク コール用に MTP が割り当てられます。H.323 Fast Start に使用される MTP は単一の音声コーデックのみをサポートするため、音声コールおよび暗号化されたコールはサポートされません。デフォルトでは、H.323 Fast Start は H.323 トランクで無効になっています。MTP は、発信コールまたは着信コールには必要ありません。原則として、音声コール、ビデオ コール、および暗号化されたコールが H.323 トランク接続上でサポートされるように、このデフォルトの H.323（Slow Start）トランクの設定が適切です。

メディア ターミネーション ポイントを使用する H.323 トランク

メディア ターミネーション ポイント（MTP）は、一般に、H.323 トランクの通常動作には必要ありません。ただし、通信相手のデバイスが、H.323 Version 1 である場合、付加サービス用に Empty Capabilities Set（ECS）をサポートしていない場合、または H323 Fast Start を必要とする場合には必要です。

MTP が必要かどうかをテストするには、次の簡単な手順を使用します。

1. 電話機から H.323 トランクを介して他のデバイスにコールを発信します。このコールは通常どおりに発信する必要があります。
2. コールを保留にしてから、保留解除します。コールがドロップする場合は、Unified CM と他のデバイス間の相互運用性を保証するために MTP を使用することを推奨します。

DTMF Transport

H.323 トランクは、H.245 を使用したアウトオブバンド DTMF と RTP Named Telephone Event（RFC 2833）を使用したインバンド DTMF の両方で DTMF シグナリングをサポートします。設定オプションはありません。必要に応じて、アウトオブバンド DTMF リレーとインバンド DTMF リレーを変換するために、動的に MTP が割り当てられます。H.323 トランクがどのような場合にどの方式を使用するか、MTP がどのような場合に必要かについては、「メディア リソース」（P.17-1）を参照してください。

H.323 トランク トランスポート プロトコル

H.323 トランクは、H.225 呼制御および H.245 メディア制御シグナリングに TCP を使用し、ゲートキーパー H.225 Registration Admission Status（RAS）シグナリングには UDP を使用します。

安全な H.323 トランク

H.323 トランクをセキュリティで保護するには、メディアを暗号化するためのトランクの設定と、シグナリングを暗号化するためのトランクの設定という 2 つのプロセスがあります。

メディア暗号化

メディア暗号化を H.323 トランクで設定するには、トランクの [SRTP allowed] チェックボックスをオンにします。[SRTP allowed] チェックボックスをオンにすると、コールのメディアは暗号化されますが、トランクのシグナリングは暗号化されない点に注意してください。結果として、安全なメディア ストリームの確立に使用されるセッション キーは暗号化されていない状態で送信されます。そのため、Unified CM と宛先 H.323 トランク デバイス間のシグナリングも暗号化し、キーや他のセキュリティ関連の情報がコールのネゴシエーション中に漏洩しないようにすることが重要です。

シグナリング暗号化

H.323 トランクはシグナリング暗号化に IPSec を使用します。ネットワーク インフラストラクチャで IPSec を設定するか、Cisco Unified Communications Manager（Unified CM）およびリモート ゲートウェイまたはトランク間で IPSec を設定できます。IPSec を設定するために 1 つの方式を実装する場合、他の方式を実装する必要はありません。Unified CM サーバで IPSec を使用すると、サーバのパフォーマンスに大きな影響が生じる可能性があるため、Unified CM 自体ではなく、ネットワーク インフラストラクチャに IPSec をプロビジョニングすることが推奨されます。

システムが安全なメディアまたはシグナリング パスを確立でき、さらにエンド デバイスが SRTP をサポートする場合、システムは SRTP 接続を使用します。システムが安全なメディアまたはシグナリング パスを確立できないか、1 つ以上のデバイスが SRTP をサポートしない場合、システムは RTP 接続を

使用します。SRTP から RTP へのフォールバック（またはその逆）は、安全なデバイスから安全ではないデバイスへの転送、会議、トランスコーディング、保留音などの場合に発生する可能性があります。

SRTP が設定されたデバイスでは、デバイスの [SRTP Allowed] チェックボックスがオンで、そのコールでデバイスの SRTP 機能が正常にネゴシエートされた場合、Unified CM はコールを暗号化済みと分類します。前述の条件を満たさない場合、Unified CM はコールを安全ではないと分類します。デバイスが、セキュリティ アイコンを表示できる電話に接続されている場合、コールが暗号化されているときは電話機に鍵アイコンが表示されます。

[MTP Required] チェックボックスを使用して、スタティックに H.323 トランクに割り当てられている MTP は、パススルー コーデックをサポートしないため、SRTP をサポートしません。すべてのコールで SRTP をサポートするには、H.323 発信 Fast Start に H.323 トランクを設定しないでください（つまり、[MTP Required] は選択しないでください）。SRTP は着信 Fast Start でサポートされます（着信 Fast Start に MTP またはコーデックの選択は必要ありません）。

Unified CM における H.323 の動作

この項では、H.323 プロトコルを Unified CM で使用および実装する方法、および特定の機能が所定どおりに動作する仕組みとその理由について説明します。

理解するうえで最も重要な点は、どのサブスクライバがコール シグナリング デーモンを実行するかということです。このデーモンは、H.323 コールを発信および受信する部分的なコードです。通常、このデーモンは H.323 デーモンまたは H.225 デーモン（H.323D または H.225D）と呼ばれます。H.225 は、H.323 プロトコルの一部で、主に呼制御を担当します。H.245 は、H.323 のもう 1 つの主要コンポーネントで、コールのメディア制御を担当します。

多くの H.323 デバイスでは、特定の H.323 デバイスの Unified CM Group に含まれるサブスクライバによって、デーモンを実行するサブスクライバと実行するタイミングが決定されます。H.323 非ゲートキーパー制御クラスタ間トランクの場合、標準の Unified CM Group を使用するか、[Run on All Active Unified CM Nodes] をイネーブルにできます。この場合、デーモンはすべてのアクティブなノードで実行されます。

Unified CM Group を使用するデバイスの場合、不適切なサブスクライバに送信されたコールは拒否される可能性があるため、H.225 デーモンを実行するノードを認識することが重要です。たとえば、この状況が発生するのは、Cisco IOS H.323 ゲートウェイに、Unified CM クラスタ内のサブスクライバ C にコールを送信するダイヤル ピアが設定されているものの、そのゲートウェイの Unified CM Group のリストにはサブスクライバ A および B しか含まれていない場合です。そのような場合、コールは失敗するか、またはデーモンがサブスクライバ上に設定されていれば H.323 トランク デーモンによって処理されます。

次のシナリオは、H.225D がサブスクライバ上に作成される仕組みとその時期について説明しています。

- H.323 クライアント

  H.225D は、H.323 クライアントに関連付けられた Unified CM Group で使用可能な、最もプライオリティの高いサブスクライバ上だけでアクティブになります。

  H.323 クライアントがゲートキーパー制御の場合、RasAggregator デバイスは、ゲートキーパー制御の H.323 クライアントに関連付けられた Unified CM Group で使用可能な、最もプライオリティの高いサブスクライバから登録されます。

  RasAggregator は、次の 2 つの特殊機能を提供するためにゲートキーパー ゾーンで登録される特殊なデバイスです。

  - H.323 クライアントが DHCP を使用している場合は、DNS を使用している Unified CM でそのクライアントを使用できません。ただし、クライアントが Dynamic DNS をサポートしている場合は除きます。RasAggregator を使用すると、Unified CM は、コールを発信するたびに、ゲートキーパーに登録されている特定の H.323 クライアントの IP アドレスを取得できます。ゲートキーパー登録は、H.323 クライアントの E.164 アドレスを含む標準の RAS ARQ メッセージを使用して行われます。ゲートキーパーは、E.164 アドレスを解決し、IP アドレスを ACF メッセージで Unified CM に返します。
  - また、RasAggregator を使用すると、H.323 クライアントによるコールはすべて Unified CM を経由するようになり、クライアント自身の間では直接やり取りされないことが保証されます。これにより、ダイヤリング規則とコーデック制限が適用されることが保証されます。

- H.323 ゲートウェイ

  H.225D は、H.323 ゲートウェイに関連付けられた Unified CM Group にあるすべてのサブスクライバ上でアクティブになります。

- H.323 ゲートキーパー制御トランク

  H.225D は、H.323 トランクに関連付けられた Unified CM Group にあるすべてのサブスクライバ上でアクティブになります。RAS デーモンは、関連付けられている Unified CM Group にあるすべてのサブスクライバから、トランクをゲートキーパーに登録します。

- Unified CM Group を使用する H.323 非ゲートキーパー制御トランク

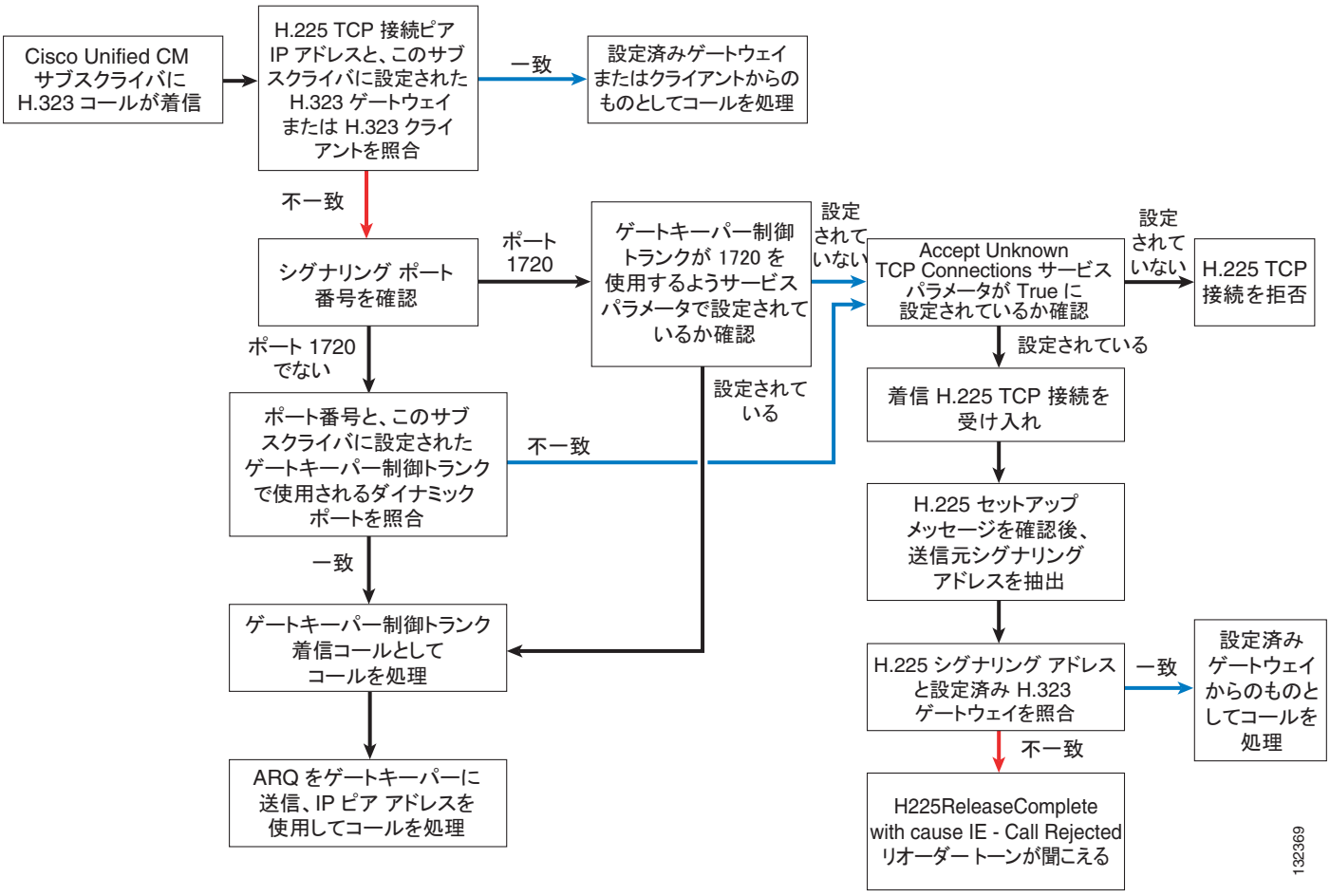
  H.225D は、H.323 トランクに関連付けられた Unified CM Group にあるすべてのサブスクライバ上でアクティブになります。

- [Run on All Active Unified Nodes] を使用する H.323 非ゲートキーパー制御トランク

  H.225D は、クラスタ内のすべてのアクティブな Unified CM サブスクライバでアクティブです。

Unified CM クラスタ内のサブスクライバに H.323 コールが着信すると、コールを受け入れるかまたは拒否するか、受け入れる場合はどの H.225D がコールを受信するかなど、さまざまな決定が下されます。図 14-24 は、このプロセスの仕組みを示しています。

図 14-24　H.323 コールの受け入れまたは拒否を判別するプロセス



Unified CM の H.323 プロトコルには、次の追加機能が含まれています。

- Protocol Auto Detect

  この機能では、コールごとに、発信側デバイスが Cisco Unified CM を使用しているかどうかを判別できます。コールを受信するたびに、Unified CM は H.225 User-to-User Information Element（UUIE）を検索します。この UUIE は、もう一方の側が別の Unified CM であるかどうかを示します。UUIE が見つかった場合、Cisco Unified CM は常に Intercluster Trunk Protocol を使用します。UUIE が見つからない場合は、設定済みのプロトコルをそのデバイスに対して使用します。この機能を使用すると、H.225 ゲートキーパー制御トランクは、コールごとに Intercluster Trunk Protocol と H.225 を切り替えることができます。これにより、Unified CM クラスタと他の H.323 デバイスを組み合せてゲートキーパーを使用できます。Intercluster Trunk Protocol は、H.225 と類似していますが、特定の機能を Unified CM クラスタ間で正しく動作させる仕組みが異なります。

- Tunneled QSIG または H.323 Annex M1（トランクごとにサポートされる ISO および ECMA バリエーション）

  この機能は、すべての H.323 トランクでイネーブルにできます。これにより、特定の H.323 Annex M1 機能を、Unified CM クラスタと、同じく H.323 Annex M1 をサポートする他の確認済みシステムとの間に実装できます。これらの機能には、次のものがあります。

  - パス交換
  - メッセージ待機インジケータ（MWI）
  - コールバック

- 代替エンドポイント

  この機能をサポートするゲートキーパー、たとえば Cisco Multimedia Conference Manager（MCM）Gatekeeper などに登録する場合、Unified CM はゲートキーパーに対し、H.323 トランクへのコールの代替宛先を通知できます。この代替エンドポイントまたは代替宛先は、この H.323 トランクが呼び出されたときに、ゲートキーパーによって発信側デバイスに送信されます。代替エンドポイントは、ゲートキーパーに登録されている H.323 トランクに関連付けられた Unified CM Group のリストに含まれている他のサブスクライバです。

- 代替ゲートキーパー

  この機能をサポートするゲートキーパーに H.323 トランクが登録される場合（たとえば、Cisco ゲートキーパー クラスタ）、Unified CM には、このゲートキーパーが失敗した場合や独自のリソースを使い果たした場合に、登録、コール アドミッション要求、および他の RAS 機能を処理できる他のゲートキーパーに関する情報が動的に通知されます。

- CanMapAlias

  H.323 トランクは、ゲートキーパーに Admission Request（ARQ; 許可要求）を送信すると、Admission Confirmation message（ACF; アドミッション確認）で異なる E.164 番号を受信する場合があります。このことは、元の着信番号をこの新しい番号で置き換える必要があることを示しています。この機能では、Gatekeeper Transaction Message Protocol（GKTMP）を使用して Cisco ゲートキーパーと通信するルート サーバが必要になります。

  （注） CanMapAlias は、着信番号に関してだけサポートされます。

- 帯域幅要求

  H.323 トランクは、ゲートキーパーの帯域幅情報をアップデートし、特定のコールに割り当てられた帯域幅の要求量が変更されたことを示すことができます。この機能は、デフォルトでは無効になっています。この機能を制御するには、H.323 セクションにある Unified CM サービス パラメータ **BRQ Enabled** を **True** に設定します。この機能は、H.323 トランク上でビデオを使用するときに特に重要です。これは、元の帯域幅要求が許容最大限の量を要求するためです。この機能を有効にすると、コール アドミッション制御が、コールのセットアップ中にネゴシエートされた実際の帯域幅を使用することが保証されます。

その他の H.323 トランクの設計上の考慮事項

Unified CM SIP トランクは H.323 クラスタ間トランクと比較すると機能数が多いため、クラスタ間トランク接続のプロトコルとしては SIP が選択されています。ただし、以前のソフトウェア バージョンを使用した Unified CM クラスタとのクラスタ間トランク接続の場合は、H.323 Annex M1 の方が推奨されます。マルチクラスタにクラスタ間トランクを配置する方法、および WAN 環境でのクラスタリングの詳細については、「SIP トランクの設計上の考慮事項」（P.14-27）を参照してください。

一般的な SIP および H.323 トランク設計の考慮事項

この項では、次の一般的な設計上の考慮事項について取り上げます。

Unified CM トランク上の確定的な発信ロード バランシング

多くの場合、[Run on all Active Unified CM Nodes] を使用するか、Unified CM Group をデバイスに割り当てることで、コール処理サブスクライバからトランク上で発信されるコールの分割を十分に処理できます。ルート ローカル ルールのために、トランク コールはコール処理サブスクライバからランダムに開始されるように見える場合がありますが、このようにコールがランダムに開始される見返りとして、クラスタ内のコール処理と Intra-Cluster Communication Signaling（ICCS）トラフィックが減ります。

コール処理サーバにおける発信 IP トランク コールの確定的ロード バランシングは可能ですが、逆効果となることがあります。これは、クラスタ内での予測可能なコール発信によりもたらされるメリットよりも、発信 IP トランク コールを発信させるためにクラスタ内の別のサーバに通信を拡張する 1 つのサブスクライバの登録電話からのコールにより増加する ICCS トラフィック量によるデメリットが上回るためです。

予測可能で確定的なサブスクライバに基づいた発信 IP トランク コールのロード バランシングは、次のように実現できます。

- 発信トランク コールをクラスタのコール処理サーバの 1 つのサブセットで確定的にロード バランシングするには、複数のトランクを定義して、各トランクの Unified CM Group にサブスクライバを 1 つだけ割り当てます。これらのトランクをルート グループに配置し、循環コール分配を使用します。

  たとえば、発信トランク コールをクラスタの 4 つのサブスクライバに分散するには、次のタスクを実行します。

  - 個々に Unified CM Group を持つ 4 つの H.323 トランクまたは 4 つの SIP トランクを設定し、これらすべてを、循環コール分配を使用するルート グループに含めます。
  - Unified CM Group は、次のように定義されます。

    グループ A: サブスクライバ A

    グループ B: サブスクライバ B

    グループ C: サブスクライバ C

    グループ D: サブスクライバ D

バックアップ サブスクライバが定義されていない場合、指定されたトランクのプライマリ サブスクライバで障害が発生すると、Unified CM は、ルート グループの次のトランクに発信コールを再ルーティングします。

- 発信トランク コールをクラスタの 8 つのすべてのサブスクライバに分散するには、次のタスクを実行します。
  - 個々に Unified CM Group を持つ 8 つの H.323 トランクまたは 8 つの SIP トランクを設定し、各グループにサブスクライバを 1 つだけ含め、すべてのトランクを循環ルート グループに含めます。
  - Unified CM Group は、次のように定義されます。

    グループ A: サブスクライバ A

    グループ B: サブスクライバ B

    グループ C: サブスクライバ C

    グループ D: サブスクライバ D

    グループ E: サブスクライバ E

    グループ F: サブスクライバ F

    グループ G: サブスクライバ G

    グループ H: サブスクライバ H

IP トランク上でのコーデック選択

通信エンティティ間でメディアを確立するには、これらのエンティティが、使用する 1 つ以上のコーデックに同意する必要があります。このコーデック（音声とビデオの両方が使用される場合には複数のコーデック）は、該当する通信エンティティでサポートされているコーデックのうち共通するもの、および設定されている Unified CM のポリシーから導出されます。Unified CM のポリシーは、リージョン設定で指定されます。音声のリージョン間の最大オーディオ ビット レート設定、およびビデオ（音声を含む）のリージョン間のビデオ コールの最大ビット レート設定により、それぞれのリージョンに含まれるデバイス間で使用されるコーデックのセットが決まります。このビット レート設定では、これらのリージョン間で通信を行うデバイスに許可される最大帯域幅だけが決定され、すべてのコールで使用される具体的なコーデックが指定されるわけではありません。エンティティ間に共通するコーデックが複数あり、リージョン間のビット レート設定を考慮してもそれらのコーデックから複数のコーデックを選択できる場合、Unified CM では、コーデックの実際のビット レートには関係なく、最も品質の高いコーデックが選択されます。

たとえば、トランクと IP Phone 間のリージョン間音声ビット レート設定が 8 kbps（G.729）に設定されていて、両方のエンドポイントで G.729 がサポートされている場合、このコーデックが選択されます。ただし、リージョン間音声ビット レートが 64 kbps（G.722 と G.711）に設定されていて、両方のエンドポイントで G.711、G.722、および G.729 がサポートされている場合、G.722 が最高の音質を提供するため、Unified CM ではこのコーデックが選択されます。リージョンの [Link Loss Type] が [Lossy] と設定されている場合は、コーデック選択ルールは若干異なります。この場合は、iSAC コーデックが通信の両側でサポートされており、リージョン間ビット レート設定で許可されていると、iSAC コーデックが他のコーデックよりも優先されます。これは、iSAC コーデックでは、低ビット レートにおいて高い品質が提供されるためです。

SIP および H.323 トランク上のコールの場合、トランク上のコールに使用するために選択されるコーデックは、コール セットアップ メッセージから取得したリモート エンドポイントの機能、ローカル エンドポイントの機能、トランクとローカル エンドポイント リージョン間のリージョン間ビット レート設定によって決定されます。

（注）　リージョン間で損失リンク数が少ない場合、可能であれば、G.729 などの低品質なコーデックよりも、G.722 や G.711 などの高品質なコーデックが選択されます。このルールの例外は、リージョン間のリンクが lossy としてマークされている場合です。この場合は、可能であれば iSAC コーデックが使用されます。

（注）　[MTP Required] がトランクで選択されている場合、他の設定に関係なく、MTP に指定されるコーデックが使用されます。この場合、リージョン間ビット レート設定は、このコーデックを許可するように適切に設定される必要があります。

その他の MTP の使用

MTP は、トランク上でコールを発信する他のデバイスからのメディア ストリームを終端させる場合や、同じ音声ペイロードでメディア ストリームを再発信する場合に非常に役立ちます。ただし、そのような場合、IP アドレスは MTP のアドレスに変更されます。この事実に留意して、次のシナリオで MTP を使用します。

- 企業内の電話機、ゲートウェイ、および他のデバイスがすべて RFC 1918 プライベート アドレスを使用する場合は、すべての音声およびビデオ デバイスにネットワーク アドレス変換（NAT）を使用しなくても、引き続きパブリック ネットワーク上の他のシステムに接続できます。パブリック ネットワークと通信する Unified CM サブスクライバがパブリック IP アドレスを使用している場合、シグナリングはルーティングされます。また、すべての MTP もパブリック アドレスを使用している場合、RFC 1918 アドレスを持つデバイスからのメディアは MTP で終端され、再度発信されます。ただし、今度は、パブリック ネットワーク上でルーティング可能なパブリック アドレスが割り当てられます。このアプローチを使用すると、RFC 1918 アドレスを持つ何万台ものデバイスが、パブリック ネットワークと通信できるようになります。この同じ方式を使用すると、企業ネットワークにあるデバイスが他の企業またはサービス プロバイダーと通信するときに、そのデバイスの実際の IP アドレスを隠すことができます。
- 信頼性境界を設定すると、ファイアウォールを通過させることや、アクセス コントロール リスト（ACL）を使用したアクセスを許可できます。通常、メディアがファイアウォールを通過できるようにするには、アプリケーション レイヤ ゲートウェイ（ALG）またはフィックスアップを使用して、動的にメディア ストリームにアクセス許可を与えるか、または、ファイアウォールを越えて通信する必要のある音声デバイスすべてで使用するための広範囲のアドレスおよびポートを割り当てます。トランクを使用し、ファイアウォールまたは ACL を通過するすべてのコールには、MTP から発信されるメディアが割り当てられます。このメディアでは、単一の IP アドレスまたは狭い範囲の IP アドレスを使用できます。

これらの方法を両方使用する場合、[MTP Required] チェックボックスをオンにすると、デフォルトで、SIP および H.323 トランク上のコールが許可されます。このことは、MTP リソースが使用不能の場合や、使い果たされた場合でも同様です。このデフォルト動作により、コールの音声パスが使用不能になる場合があります。この動作を変更するには、SIP および H.323 セクションにある Unified CM サービス パラメータ **Fail Call if MTP allocation fails** を **True** に設定します。

Cisco Unified CM トランクおよび緊急サービス

IP トランクは、緊急 911 コールを送信できない場合があります。また、中央集中型 PSTN トランクのように、発信側のロケーションに適した Public Safety Answering Point（PSAP）に緊急 911 コールを送信できない場合があります。そのため、お客様は、緊急 911 コールおよび発信側のロケーションを

適切な PSAP に送信できるかどうか、IP トランク サービス プロバイダーの機能を注意して調査する必要があります。Cisco Emergency Responder を使用すると、緊急 911 コールに対する、ロケーションに固有な発番号を IP トランク サービス プロバイダーに提供できる場合があります。

また、中央集中型 IP または PSTN トランクが、WAN 輻輳または障害のために、リモート ロケーションからの緊急 911 コールに一時的に応答できなくなることもあります。そのため、リモート ロケーションでは、常に、緊急 911 コールを送信できる PSTN へのローカル ゲートウェイを使用できなければなりません。詳細については、「緊急サービス」（P.10-1）を参照してください。

Unified CM IP トランクのキャパシティ プランニング

Cisco 7800 Series Media Convergence Server では、次のトランク容量がサポートされます。

- MCS-7845 クラスタまたは Cisco Unified Computing System（UCS）と同等のクラスタでは、最大 2100 トランクがサポートされます。
- MCS-7835 クラスタでは、最大 1100 のトランクがサポートされます。
- MCS-7825 クラスタでは、最大 1100 のトランクがサポートされます。
- MCS-7816 クラスタでは、最大 200 のトランクがサポートされます。

上記の値は通常の最大容量を表していますが、実際のトランクのスケーラビリティおよびパフォーマンスは、最終的には、個々のサブスクライバで処理されている他のすべてのアプリケーションおよびタスクや、トランクにおける Busy Hour Call Attempts（BHCA; 最繁時呼数）などのいくつかの要因によって決定されます。全体的なシステム容量を決定するには、Cisco Unified Communications Sizing Tool（Unified CST）を使用します。このツールは、シスコ従業員と代理店が適切なログイン認証を経て次の Web サイトから入手できます。

http://tools.cisco.com/cucst

クラスタのトランクのスループットを最大にするには、着信と発信の両方におけるトランクの負荷が、可能なかぎりクラスタ内のすべてのサブスクライバに均等に分散されるようにします。

サービス プロバイダー ネットワークに対する IP PSTN および IP トランク

サービス プロバイダーは、企業の顧客に対して非 TDM PSTN 接続のサービスを増やしています。非 TDM インターフェイスを配置することで得られるコスト削減という重要なメリットのほかに、これらの IP ベース PSTN 接続では、従来の PSTN インターフェイスと比較して優れた音声機能が提供されます。

SIP ベースのサービスは使用可能なサービスの中で優位を占め、旧 H.323 サービスは特定の地域で使用できましたが、段階的に使用されなくなっています。これは主として、企業内で SIP の人気が高まっていることに加え、プレゼンスなどの追加機能や多くのリッチ メディア アプリケーション（インスタント メッセージングなど）のサポートが提供されることが背景にあります。長期的に見ると、SIP は、Unified Communications プロトコルとして最も幅広く使用されるようになると思われます。

サービス プロバイダーの IP PSTN ネットワークに接続する場合、エンタープライズ エッジ Session Border Controller として Cisco Unified Border Element を使用し、企業ネットワークとサービス プロバイダーのネットワーク間に制御された境界およびセキュリティ ポイントを用意することが強く推奨されます。

Cisco Unified Border Element

Cisco Unified Border Element は、企業およびサービス プロバイダーの Cisco Unified Communications ネットワーク間に、多用なシグナリングおよびメディア機能があります。Cisco Unified Border Element は、次のものを対象として、Session Border Controller のネットワーク間インターフェイス ポイントを提供します。

- アドレスおよびポート トランスレーション（プライバシーおよびレベル 7 のトポロジ隠蔽）
- SIP ディレイド オファーからアーリー オファーへの変換
- プロトコルのインターワーキング（H.323 および SIP）および正規化
- メディアのインターワーキング（DTMF、Fax、コーデックのトランスコーディング、および音量と制御取得のトランスコーディング）
- コール アドミッション制御（合計のコール、メモリ、コール到達のスパイク検出、または宛先あたりの最大コール数）
- セキュリティ（SIP の不正パケット検出、非ダイアログの RTP パケット ドロップ、SIP リスニング ポートの設定、ダイジェスト認証、同時コール数制限、コール レート制限、料金詐欺の防止、および複数のシグナリングとメディアの暗号化オプションなど）
- サービス プロバイダーとの PPI/PAI/プライバシーおよび RPID インターワーキング
- QoS および帯域幅管理（ToS/DSCP を使用した QoS マーキング、および RSVP やコーデック フィルタリングによる帯域幅拡張）
- 複数のサービス プロバイダーからの SIP トランクに対する同時接続

ボックス内またはボックス間のフェールオーバー オプションによるハイ アベイラビリティ（プラットフォームおよびリリースによって変わります）

- 請求の統計情報と CDR の収集

Cisco Unified Border Element は、Cisco Integrated Service Routers Generation 2（ISR G2）、Cisco AS5000XM Media Gateways、および Cisco 1000 シリーズ Aggregation Services Router（ASR ; アグリゲーション サービス ルータ）で使用できる正規の Cisco IOS アプリケーションです。選択したハードウェア プラットフォームに応じて、Cisco Unified Border Element は、ボックス内またはボックス間のフェールオーバー オプションで、最大 16,000 の同時音声コールについてセッション スケーラビリティを提供できます。

Cisco Unified Border Element の詳細については、次のサイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/go/cube

トランクの集約プラットフォーム

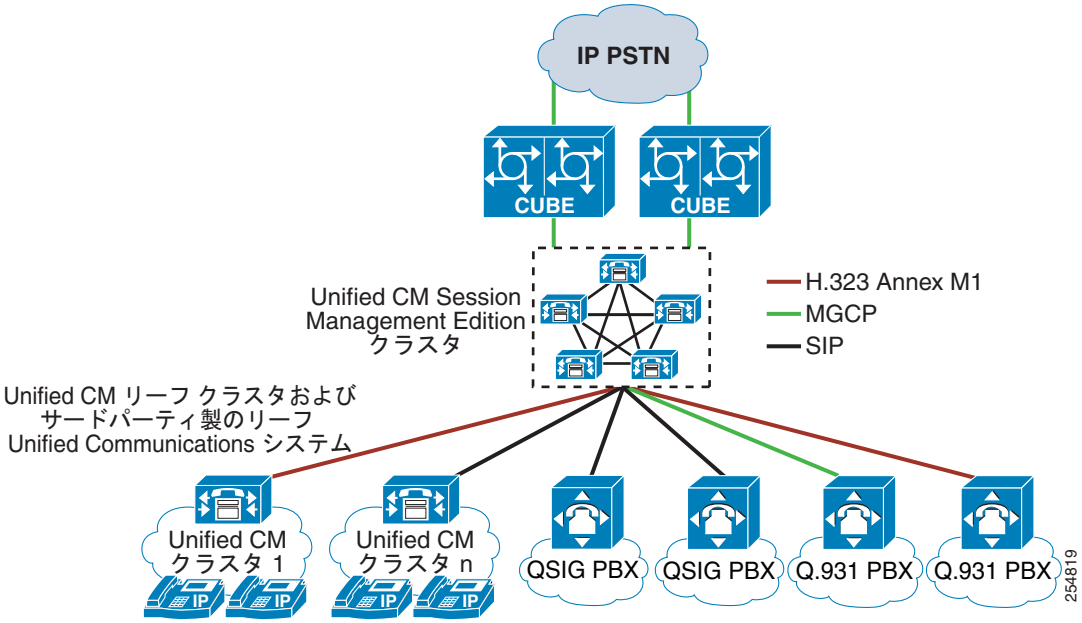
多くの場合、大規模な IP PSTN 展開では、多数の Unified Communications システムからトランクを集約してから、サービス プロバイダーの IP PSTN に対して Cisco Unified Border Element を使用して接続する必要があります。ほとんどの場合、集約プラットフォームの選択は、エンド システムが使用しているプロトコルによって変わります。Cisco Unified CM Session Management Edition および Cisco Unified SIP Proxy は 2 つの共通して使用される集約プラットフォームです。詳細については、この項で説明します。シスコの H.323 ゲートキーパーも選択肢の 1 つですが、IP PSTN 接続には SIP が選択されるようになったので、現在ではあまり広く使用されていません（シスコの H.323 ゲートキーパー オプションについては、「H.323 トランク タイプ」（P.14-38）の項で説明されています）。

Session Management Edition

Unified CM Session Management Edition を使用する Unified Communications の配置は、マルチサイトの分散型コール処理の配置モデルにおけるバリエーションで、通常、大量の Unified Communications システムと相互接続するため、および IP PSTN に対して接続を提供するために採用されます。

Cisco Unified CM Session Management Edition は基本的に、トランク インターフェイスだけを使用し、IP エンドポイントを使用しない Unified CM クラスタです。このクラスタには、リーフ システムと呼ばれる、複数のユニファイド コミュニケーション システムを集約できます（図 14-25 を参照）。

図 14-25　Cisco Unified CM Session Management Edition



Unified CM Session Management Edition の配置は、複数の PBX 配置とそれに関連する電話を、IP 電話があり比較的少数のトランクを持つ Unified CM クラスタに移行するために使用できます。Unified CM Session Management Edition クラスタをサードパーティの PBX を相互接続する多数のトランクで開始し、何千もの IP 電話を持つ Unified CM クラスタ配置に徐々に移行することも可能です。また、Unified CM Session Management Edition を使用して、IP PSTN 接続、集中型のユニファイド コミュニケーション アプリケーションなど、サードパーティのユニファイド コミュニケーション システムに接続できます

Cisco Unified CM 8.5 以降のリリースでは、Unified CM Session Management Edition で次の機能がサポートされています。

- SIP トランク（ディレイド オファー推奨）
- H.323 トランク（Slow Start 推奨）
- MGCP トランク
- 音声コール
- ビデオ コール
- 暗号化されたコール

- FAX コール

Unified CM Session Management Edition は Unified CM と同じソフトウェアを使用するため、スケーラビリティ、可用性、ロード バランシング、SIP メッセージの正規化、コール ルーティング、番号の変更などのすべての Unified CM 機能は、Unified CM Session Management Edition クラスタに対して使用できます。

Cisco Unified CM Session Management Edition の詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

Cisco Unified SIP Proxy

Cisco Unified SIP Proxy は、Cisco 3800 シリーズの Integrated Services Router（ISR; 統合サービス ルータ）のネットワーク モジュール スロットに差し込むことができる Cisco NME-522 ネットワーク モジュールで SIP プロキシ機能を提供します。この ISR は、ネットワーク モジュールのホスティングやプロキシの実行専用にする必要はなく、上記の Cisco Unified Border Element の実行など、その他のネットワーク機能にも同時に使用できます。

Cisco Unified SIP Proxy は、Unified CM SIP トランクを使用するネットワークに次のような利点を提供します。

- 集約とルーティング

  Unified SIP Proxy は、各サーバがフルメッシュ構成で他のすべてのサーバに接続する必要なしに、SIP サーバを相互に接続できます。

- スケーラビリティ

  Unified SIP Proxy は、企業や IP PSTN サービス プロバイダーとのコールを終端するために使用できます。プロキシは次に、そのコールを Unified Border Element のプールに分配します。Unified Border Element を追加して容量を増やすこともできます。

- 可用性とロード バランシング

  Unified SIP Proxy は、使用可能な Unified Border Element のプールにコールを分配し、各 Unified Border Element のステータスをモニタリングすることで、信頼できるコールの完了を実現します。

- メッセージの正規化

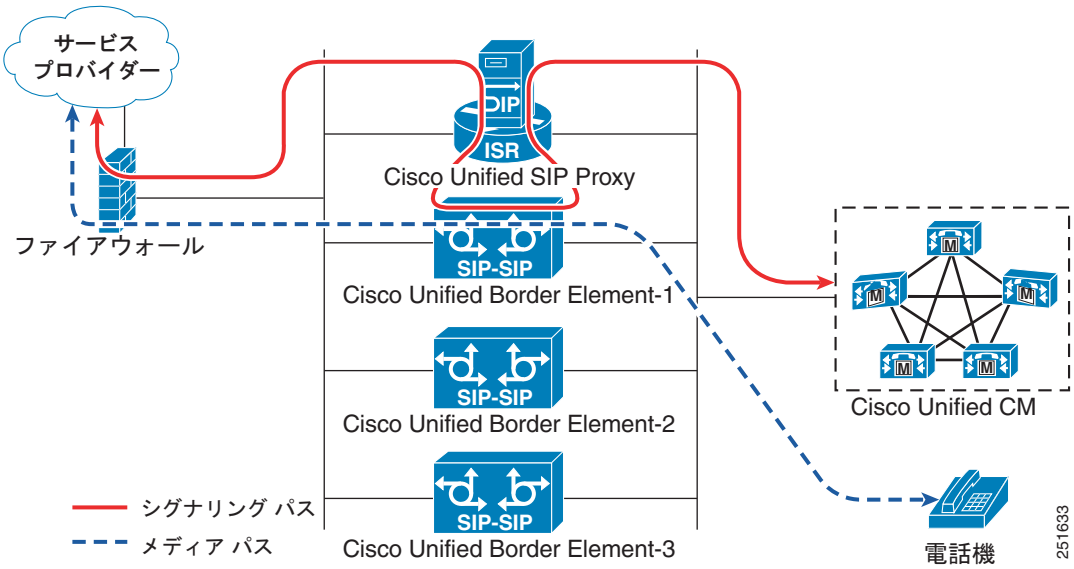
  Unified SIP Proxy は、メッセージが Unified SIP Proxy を通過する際に、そのヘッダーや内容を操作する手段を提供することにより、SIP プロトコルのメッセージングにおける違いを隠す役割を果たします。

Cisco Unified SIP Proxy と Cisco Unified Border Element を配置する場合は、次の設計上の考慮事項を検討する必要があります。

- 接続されている Unified Border Element がいずれも過負荷にならないように、Unified SIP Proxy 上でロード バランシングの方式を設定します。
- Unified CM または Unified Border Element の障害を検出して対処できるように、Unified SIP Proxy にトランクのモニタリングをセットアップします。

図 14-26 に、Cisco Unified SIP Proxy と Cisco Unified Border Element を使用したコール フローを示します。

図 14-26　Cisco Unified SIP Proxy と Cisco Unified Border Element のコール フロー



サービス プロバイダーへのコールを発信するために、Unified CM は Unified SIP Proxy にコールを送信します。Unified SIP Proxy は要求が Unified CM から発信されたと判断し、Unified Border Element にコールを転送します。Unified Border Element はコールを終端および再発信して Unified SIP Proxy に戻します。Unified SIP Proxy はコールが Unified Border Element から発信されたと判断し、今度はサービス プロバイダーにコールを転送します。このように、メディアは Unified Border Element を介して、発信した電話機からサービス プロバイダーまで直接確立されます。

大規模な Session Border Controller

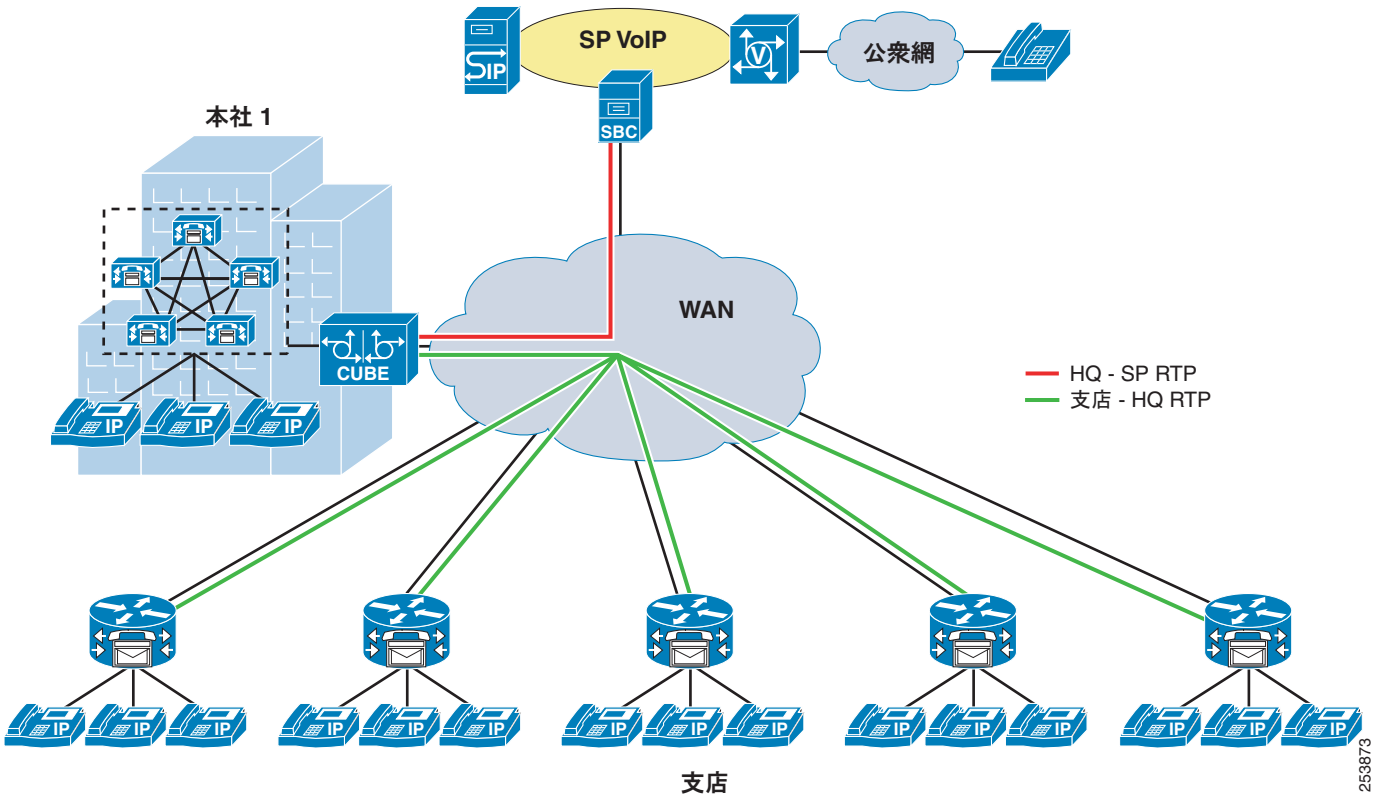
ハードウェア プラットフォームに応じて、単一のハードウェア シャーシ上の Cisco Unified Border Element は、1 つまたは複数のプロバイダーから、SIP トランク上で同時に 16,000 コールを集約できます。また必要に応じて、冗長シャーシ間にステートフル フェールオーバーを使用できます。

トランク IP-PSTN 接続モデル

トランクは、必要なアーキテクチャに応じて、さまざまな方法で IP PSTN サービス プロバイダーに接続されます。この接続における最も一般的なアーキテクチャには、中央集中型トランクと分散型トランクの 2 つがあります。

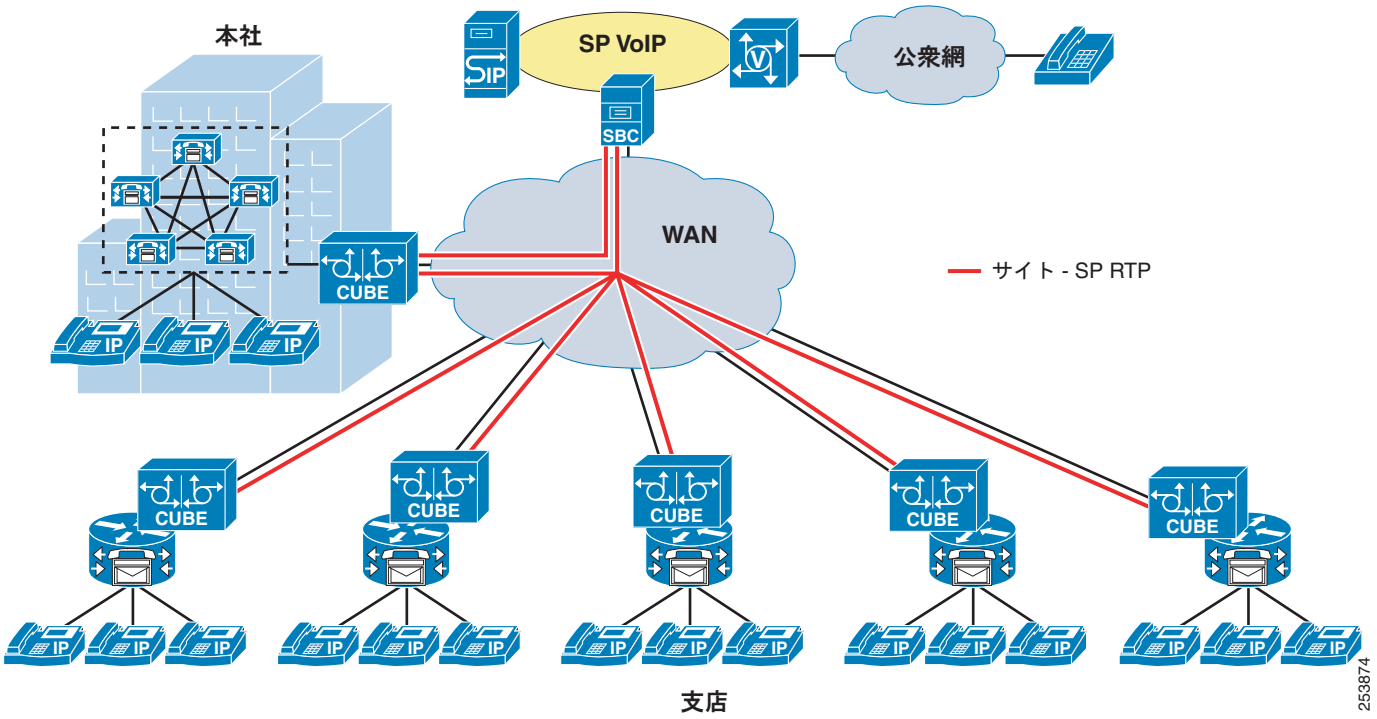
中央集中型トランクは、Cisco Unified Border Element などの Session Border Controller（SBC; セッション ボーダー コントローラ）を使用し、1 つの論理接続を通して Service Provider（SP; サービス プロバイダー）に接続します（ただし、冗長性を確保するために複数の物理接続が存在する場合があります）（図 14-27 を参照）。会社へのすべてのコール、および会社からのすべてのコールでは、このトランクのセットが使用されます。会社において、中央の Unified CM クラスタが 1 つ本社にホストされており、リモートの支店が WAN 経由で本社に接続する場合、各サイト間の公衆網コールのメディアおよびシグナリングは WAN を通過します。

図 14-27　中央集中型または集約型 SIP トランク モデル



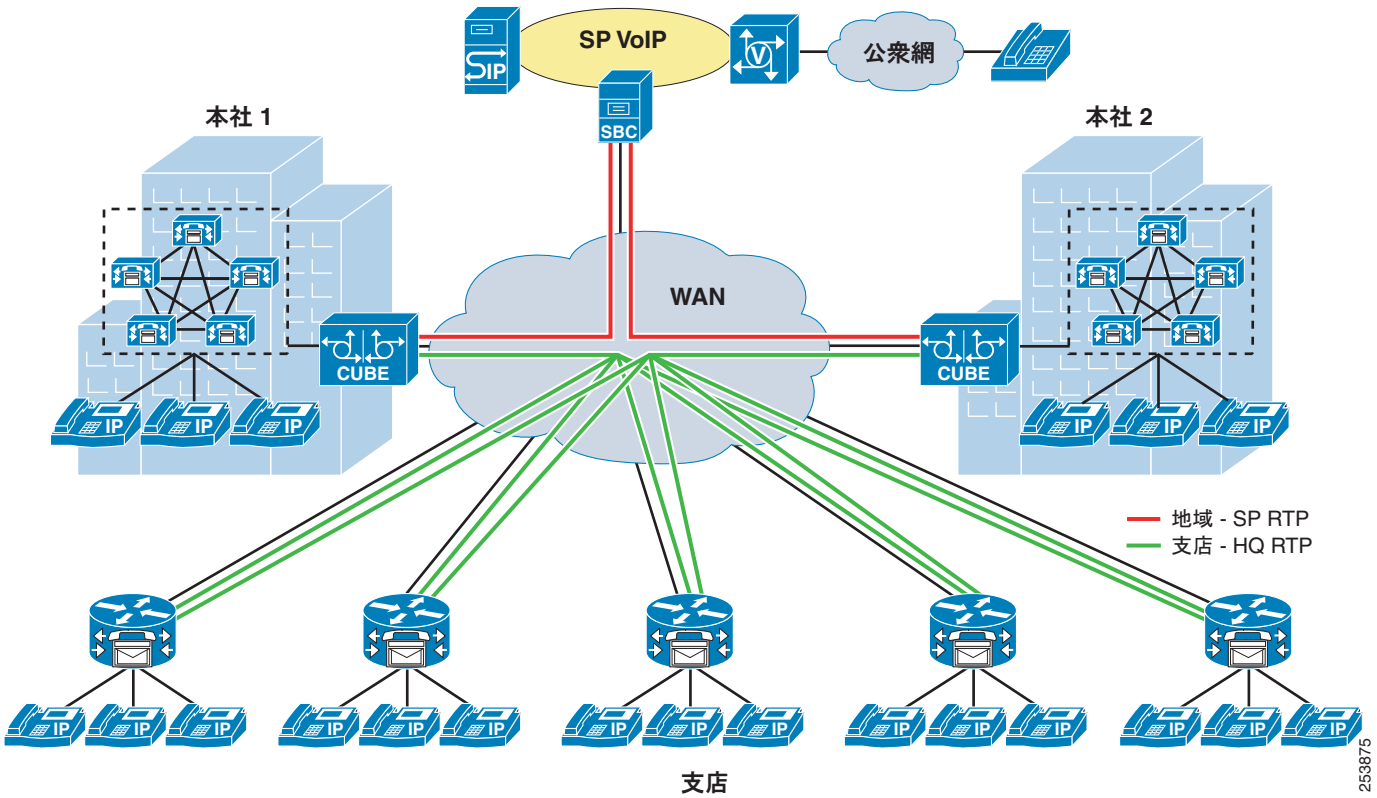
分散型トランクは、複数の論理接続経由でサービス プロバイダーに接続します（図 14-28 を参照）。会社の各支店は、サービス プロバイダーへの独自のローカル トランクを保有しています。支店からのメディアは WAN を通過する必要はなく、ローカル SBC 経由でサービス プロバイダー インターフェイスへと送信されます。

図 14-28　分散型 SIP トランク モデル



これらの接続モデルには、それぞれ利点と欠点があります。通常、中央集中型トランクは、物理的な機器および設定の複雑さの面でより容易に展開できます。分散型トランクには、メディアをローカル ハンドオフできる利点があり、またローカル プロバイダーからの番号の可搬性が高まります。図 14-29 に示すように、いくつかの支店をグループ化して接続したり、マルチクラスタ配置で各 Unified CM クラスタからトランクを提供したりするハイブリッド接続モデルでは、両方の配置形式の利点が実現されます。

図 14-29　リージョンによる集約を行ったハイブリッド SIP トランク モデル



PART 3

Unified Communications 呼制御

CHAPTER 15

Cisco Unified Communications の呼制御の概要

Cisco Unified Communications システム用にネットワーク インフラストラクチャおよびコール ルーティングを適切に設計して配置したあと、次の段階としてコアの呼制御コンポーネントのグループを配置します。これらの呼制御コンポーネントを使用すると、ユーザはより簡単にコールを発信し、ユーザ機能を向上させ、さらにリモート発信者の使用体験も向上させることができます。Unified Communications の呼制御コンポーネントに不可欠な要素は、次のとおりです。

- 中心となる Lightweight Directory Access Protocol（LDAP）ディレクトリとの統合
- 音声会議またはコーデック トランスコーディングなどのメディア リソースへのアクセス
- Unified Communications システムに対する発信者用の保留音機能
- Unified Communications エンドポイント用の機能セット
- クリックコール ダイヤル、マネージャ支援アプリケーション、任意の電話機にログインできるユーザ機能など、コール ルーティングに組み込みのアプリケーション

SRND のこの部分は、上記のさまざまな呼制御コンポーネントのすべてに対応しています。各章では、呼制御コンポーネントの概要を説明し、続いてアーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。各章の内容は、製品固有のサポートおよび設定の情報ではなく、設計関連の情報に重点を置いています。

SRND のこの部分に含まれる章は、次のとおりです。

- 「LDAP ディレクトリ統合」（P.16-1）

  この章では、Cisco Unified Communications Manager のディレクトリ アーキテクチャ自体や LDAP の同期化および認証に関する設計上の考慮事項など、Unified Communications と LDAP ディレクトリとの統合について説明します。また、Unified Communications エンドポイントからのディレクトリ アクセスおよびセキュリティ上の考慮事項についても説明します。

- 「メディア リソース」（P.17-1）

  この章では、Unified Communications メディア リソースとして分類されるすべてのコンポーネントについて説明します。Digital Signal Processor（DSP; デジタル シグナル プロセッサ）とそれらの音声インターフェイス用の展開、会議機能とトランスコーディング機能、および Music on Hold（MoH; 保留音）のすべてについて説明します。Media termination point（MTP; メディア ターミネーション ポイント）、その機能方法、および SIP トランクと H.323 トランクに関する設計上の考慮事項についても説明します。さらに、Trusted Relay Point、RSVP Agent、Annunciator、MoH、およびセキュア会議に関する設計上の考慮事項についても、この章で説明します。

- 「Unified Communications エンドポイント」（P.18-1）

  この章では、シスコのポートフォリオで使用可能なすべての Unified Communications エンドポイントについて説明し、簡単に比較できるように表形式でこれらの機能を一覧します。無線および有線の電話機に加えて、ソフトウェアベースのエンドポイントについても説明します。また、アナログ接続に Foreign Exchange Station（FXS）ポートを提供するビデオ テレフォニー エンドポイントおよびゲートウェイについても説明します。

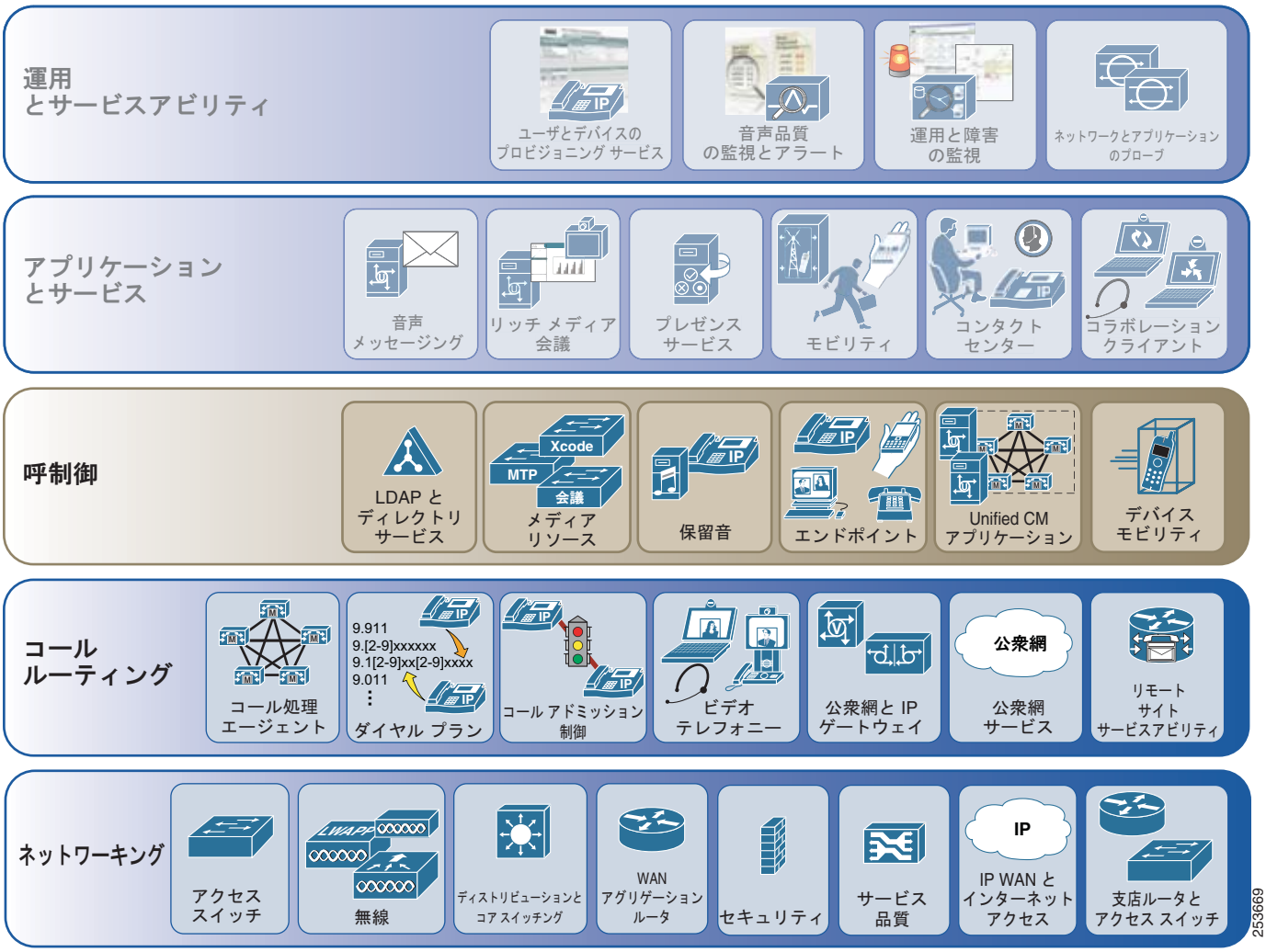
- 「Cisco Unified CM アプリケーション」（P.19-1）

  この章では、IP Phone サービス、WebDialer、Unified CM Assistant、Extension Mobility（EM; エクステンション モビリティ）など、Cisco Unified Communications Manager（Unified CM）に組み込まれている固有のアプリケーションについて説明します。加えて、アテンダント コンソール アプリケーションとそれらの CTI を通した Unified CM への統合についても説明します。最初にアプリケーションの背後にあるアーキテクチャについて説明し、次に設計上の考慮事項について説明します。また、Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）などのアプリケーションのバリエーション、および Unified CM Assistant プロキシ回線モードとシェアド ライン モードについても説明します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムと同様に、Unified Communications の呼制御コンポーネントは、基礎となるネットワークおよびシステム インフラストラクチャの上に構築されます。図 15-1 に、Cisco Unified Communications システム全体のアーキテクチャにおける Unified Communications 呼制御コンポーネントの論理的位置を示します。

図 15-1　Cisco Unified Communications の呼制御アーキテクチャ



会議リソース、保留音、ディレクトリ統合、エンドポイントなどの Unified Communications の呼制御コンポーネントでは、Unified Communications のネットワーキング インフラストラクチャおよび Unified Communications のコール ルーティング アーキテクチャが適切に設計され、すでに配置済みであることが必要です。これらの呼制御コンポーネントが Unified Communications システム上に構築されて、拡張（および通常必要とされる）ユーザ機能を提供します。

ハイ アベイラビリティ

ネットワークおよびコール ルーティングと同様に、呼制御インフラストラクチャは、ネットワーク内またはコール処理エンティティで障害が発生している間でも、必要な機能をそのまま使用できるように高い可用性を備えている必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解しておくことが重要です。多くの Unified Communications コンポーネントが他のコンポーネントに依存しているため、場合によっては、単一のサーバまたは機能の障害が複数のサービスに影響を与えることもあります。たとえば、Cisco Unified Communications Manager（Unified CM）アプリケーションのさまざまなサービス コンポーネントが適切に機能している一方で、Unified CM のコール処理サービスの損失により、事実上 Unified CM アプリケーションが

使用不可になることがあります。これは、コールを発信または受信する Unified CM に配置が依存しているためです。多くの場合、機能のすべてまたは一部は冗長リソースで処理できるため、ある程度の障害が発生しても、エンド ユーザは継続してサービスを利用できます。

メディア リソースおよび保留音では、ハイ アベイラビリティに関する考慮事項に、ネットワーク障害やサーバまたは DSP プラットフォーム障害による一時的な機能損失が含まれます。このことは、ユーザ エクスペリエンスの低下（たとえば、会議を開始しても「Resources Not Available」または同様のメッセージが電話機に表示されるだけになる）や、システムに発信する発信者の使用体験の低下（たとえば、保留中に特定の通知メッセージが流れず無音になることがある）を招く可能性があります。設定のベスト プラクティスおよび冗長リソースの配置に関する設計の詳細については、それぞれの章で説明します。

Unified CM アプリケーションは、クラスタ内の Unified CM ノードで特定のサービスを有効にすることによって配置されます。サービス障害があると、結果的にユーザ エクスペリエンスが低下したり、まったく機能しないというユーザ エクスペリエンスになったりします。電話機にログインしているユーザまたは IP Phone サービスにアクセスしているユーザは長い遅延を体験することになり、一般的に何回も接続をやり直すため、さらに問題が悪化します。SRND のこの部分の章では、アプリケーションのアーキテクチャについて説明し、アプリケーション固有の機能のために有効にするクラスタ内のノードやノードの数に関する設計上の考慮事項を示します。

同様に、LDAP ディレクトリの統合では、LDAP ディレクトリ サーバがオフラインになったり、LDAP 間の接続とコール処理エンティティが使用不可になったりする可能性があります。LDAP 認証またはユーザ ディレクトリ ルックアップが代替サーバまたは代替パスを使用して機能を続行できるようにするための、設計上の考慮事項が必要です。

キャパシティ プランニング

ネットワーク、コール ルーティング、および呼制御インフラストラクチャは、個々のコンポーネントとシステム全体のキャパシティおよびスケーラビリティを理解したうえで、設計および展開する必要があります。さまざまな Unified Communications の呼制御コンポーネントを展開する場合、コンポーネント自体のスケーラビリティだけでなく、基盤となるインフラストラクチャも考慮する必要があります。ネットワーク インフラストラクチャに使用可能な帯域幅があり、これらのコンポーネントが作成するトラフィック ロードを処理できる必要があります。同様に、コール ルーティング インフラストラクチャは、ユーザとデバイスの設定および登録のほかに、呼制御要素に関連付けられたプロトコルおよび接続にかかわる追加の負荷も処理できる必要があります。

SRND のこの部分のすべての章に、キャパシティ プランニングに関する考慮事項があります。LDAP ディレクトリの統合の場合、最も一般的な考慮事項は、Unified Communications データベース内で同期化できるユーザの数と更新のポーリングおよび更新のポーリングがシステム パフォーマンスに与える影響です。個々の DSP メディア リソースで処理できる会議またはトランスコーディング セッション数には限度があるため、優れた設計には DSP の適切なサイジングおよび割り当てが不可欠です。各 Unified CM アプリケーションには、サポートされているエクステンション モビリティのログイン レートにしても、システム内で設定可能な IP Manager Assistant の数にしても、それぞれに専用の上限セットがあります。呼制御に関する各章には、キャパシティ設計のガイドラインを提示して Unified Communications の適正設計を支援するキャパシティ プランニングの項が含まれています。

CHAPTER 16

LDAP ディレクトリ統合

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、ユーザ ポリシー、ユーザ特権、グループ メンバシップなど、頻繁に変更されないデータが企業ネットワーク上に保存されます。

ディレクトリは拡張可能です。つまり、ディレクトリに保存された情報のタイプを変更し、拡大できます。「*ディレクトリ スキーマ*」という語は、保存されている情報のタイプ、そのコンテナ（または属性）、およびユーザやリソースとの関係を定義します。

Lightweight Directory Access Protocol（LDAP）は、ディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。この機能により、企業は、すべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

この章では、Cisco Unified Communication Manager（Unified CM）に基づく Cisco Unified Communications システムを社内 LDAP ディレクトリと統合する場合の、設計上の主な原則について説明しています。この章の構成は、次のとおりです。

- 「ディレクトリ統合とは」（P.16-2）

  ここでは、一般的な企業の IT 部門における社内 LDAP ディレクトリとの統合に関して、さまざまな要件を分析します。

- 「Unified Communications エンドポイントのディレクトリ アクセス」（P.16-3）

  ここでは、Cisco Unified Communications エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションについて説明し、そのソリューションに基づく設計上のベスト プラクティスを示します。

- 「Unified CM とのディレクトリ統合」（P.16-5）

  ここでは、LDAP 同期機能や LDAP 認証機能などを含む、Cisco Unified CM でのディレクトリ統合に関して、技術的なソリューションについて説明し、設計上の考慮事項を示します。

この章で説明する考慮事項は、Cisco Unified CM とそれにバンドルされているアプリケーション（Cisco エクステンション モビリティ、Cisco Unified Communications Manager Assistant、WebDialer、Bulk Administration Tool、および Real-Time Monitoring Tool）に適用されます。

Cisco Unity については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各ホワイト ペーパーを参照してください。

http://www.cisco.com

この章の新規情報

表 16-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

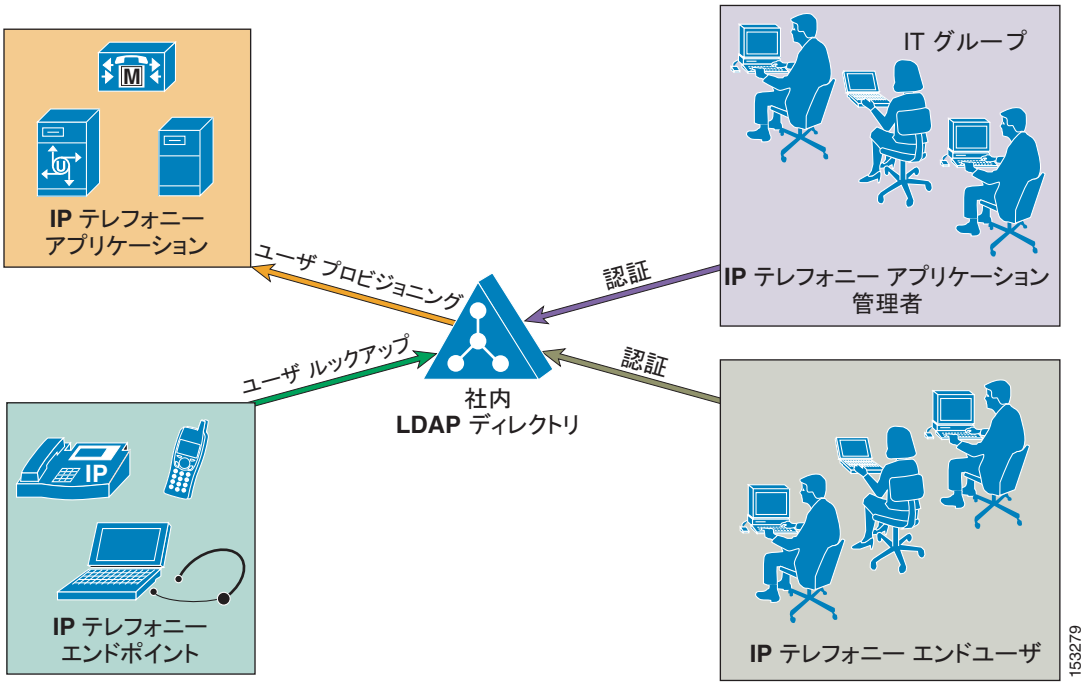
表 16-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
マルチフォレスト LDAP 同期	「Unified CM マルチフォレスト LDAP 同期」（P.16-18）	2010 年 11 月 15 日
フィルタリング	「ディレクトリ同期および認証のユーザ フィルタリング」（P.16-23）	2010 年 4 月 2 日

ディレクトリ統合とは

音声アプリケーションと社内 LDAP ディレクトリとの統合は、多くの企業の IT 部門にとって一般的な作業です。ただし、統合の正確な範囲は企業によって異なるため、図 16-1 に示すように、1 つ以上の具体的かつ独立した要件として表すことができます。

図 16-1　ディレクトリ統合のさまざまな要件



たとえば、1 つの一般的な要件は、IP 電話またはその他の音声エンドポイントやビデオ エンドポイントからユーザ ルックアップ（「個人別電話帳」サービスと呼ばれることもあります）を有効にし、ユーザがディレクトリで番号を検索した後に、連絡先に迅速にダイヤルできるようにすることです。

もう 1 つの要件は、社内ディレクトリからアプリケーションのユーザ データベースを、ユーザに自動的に提供することです。この方法により、社内ディレクトリの変更のたびにコア ユーザ情報を手動で追加、削除、または修正する必要がなくなります。

一般に、社内ディレクトリ クレデンシャルを使用して、音声アプリケーションやビデオ アプリケーションのエンド ユーザと管理者を認証することも必要です。ディレクトリ認証を有効にすることで、IT 部門は 1 つのログイン機能を提供し、さまざまな企業アプリケーションに対して各ユーザが保持する必要のあるパスワードの数を減らすことができます。

表 16-2 に示すように、Cisco Unified Communications システムに関係する場合、*ディレクトリ アクセス*という用語は、Cisco Unified Communications エンドポイントのユーザ ルックアップの要件を満たすメカニズムおよびソリューションを意味します。また、*ディレクトリ統合*という用語は、ユーザ プロビジョニングおよび（エンド ユーザと管理者の両方の）認証の要件を満たすメカニズムおよびソリューションを意味します。

表 16-2　ディレクトリの要件とシスコのソリューション

要件	シスコのソリューション	Cisco Unified CM の機能
エンドポイントのユーザ ルックアップ	ディレクトリ アクセス	Cisco Unified IP Phone Services SDK
ユーザ プロビジョニング	ディレクトリ統合	LDAP 同期
Unified Communications エンド ユーザの認証	ディレクトリ統合	LDAP 認証
Unified Communications アプリケーション管理者の認証	ディレクトリ統合	LDAP 認証

この章では、これ以降、Cisco Unified CM に基づく Cisco Unified Communications システムで、これらの要件にどのように対処するかについて説明します。

（注）「*ディレクトリ統合*」という用語については、管理ポリシーおよびセキュリティ ポリシーを集中化するために、Microsoft Active Directory ドメインにアプリケーション サーバを追加する機能といった解釈もあります。Cisco Unified CM は、カスタマイズした組み込みオペレーティング システムで実行するアプライアンスであり、Microsoft Active Directory ドメインに追加できません。Cisco Unified CM のサーバ管理は、Cisco Real-Time Monitoring Tool（RTMT）によって行われます。アプリケーションに合わせた強力なセキュリティ ポリシーが組み込みオペレーティング システム内にすでに実装されています。

Unified Communications エンドポイントのディレクトリ アクセス

この項では、Cisco Unified Communications エンドポイント（Cisco Unified IP Phone など）からユーザ ルックアップを実行するように、LDAP 準拠のディレクトリ サーバへの社内ディレクトリ アクセスを設定する方法について説明します。Unified CM やその他の Unified Communications アプリケーションがユーザ プロビジョニングおよび認証のために社内ディレクトリに統合されているかどうかに関係なく、この項で説明しているガイドラインが適用されます。

ディスプレイ画面を持つ Cisco Unified IP Phone では、ユーザが電話機の Directories ボタンを押すと、ユーザ ディレクトリを検索できます。IP Phone は、Hyper-Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示する特定の Extensible Markup Language（XML）オブジェクトが含まれています。

デフォルトでは、Cisco Unified IP Phone は、Unified CM の組み込みデータベースに対してユーザ ルックアップを実行するように設定されます。ただし、社内 LDAP ディレクトリでルックアップを実行するように、この設定を変更できます。変更した場合、電話機は HTTP 要求を外部 Web サーバに送信します。このサーバはプロキシとして動作し、要求を LDAP 照会に変換します。その後、その LDAP 照会は社内ディレクトリによって処理されます。LDAP 応答は、Web サーバによって XML オブジェクトにカプセル化され、HTTP を使用して電話機に返信されて、エンド ユーザに伝えられます。

図 16-2 では、Unified CM が社内ディレクトリに統合されていない配置において、このメカニズムを示しています。このシナリオでは、Unified CM がメッセージ交換にかかわっていないことに注意してください。図 16-2 の右側に表示されている Unified CM Web ページの認証メカニズムは、ディレクトリ ルックアップの設定とは関係ありません。

図 16-2　Cisco Unified IP Phone Services SDK を使用する Cisco Unified IP Phone のディレクトリ アクセス

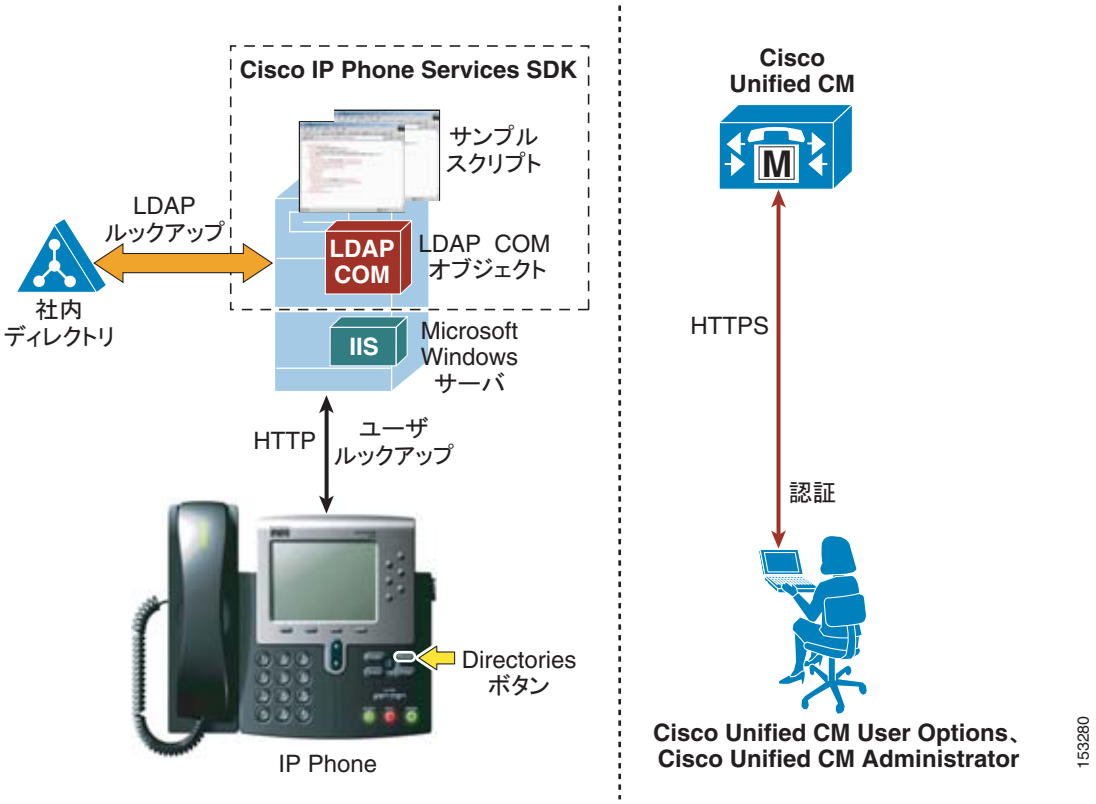


図 16-2 に示す例では、Web サーバのプロキシ機能は、Cisco Unified IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）に組み込まれている Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバによって提供されます。次の Web サイトの Cisco Developer Community から最新の Cisco Unified IP Phone Services SDK をダウンロードできます。

http://developer.cisco.com/web/ipps/home

IP Phone Services SDK は、IIS 4.0 以降を実行する Microsoft Windows Web サーバにはインストールできますが、Unified CM サーバにはインストールできません。SDK には、単純なディレクトリ ルックアップ機能を提供するサンプル スクリプトが入っています。

IP Phone Services SDK を使用する社内ディレクトリ ルックアップ サービスを設定するには、次の手順を実行します。

ステップ 1　社内 LDAP ディレクトリを指すようにサンプル スクリプトのいずれかを修正するか、SDK に付属の『LDAP Search COM Programming Guide』を使用して独自のスクリプトを作成します。

ステップ 2　Unified CM で、外部 Web サーバ上のスクリプトの URL を指すように URL Directories パラメータ（[System] > [Enterprise Parameters]）を設定します。

ステップ 3　変更を有効にするために電話機をリセットします。

（注）　ユーザのサブセットだけにサービスを提供する場合は、[Enterprise Parameters] ページではなく、[Phone Configuration] ページ内で URL Directories パラメータを直接設定します。

まとめると、Cisco Unified IP Phone Services SDK によるディレクトリ アクセスには、次の設計上の考慮事項が適用されます。

- ユーザ ルックアップは、LDAP 準拠の社内ディレクトリに対してサポートされる。
- Microsoft Active Directory に照会する場合、スクリプトがグローバル カタログ サーバを指すようにし、スクリプト設定でポート 3268 を指定することにより、グローバル カタログに対してルックアップを実行できる。この方法では、通常はルックアップが高速化します。グローバル カタログに記載されているユーザの属性がすべてではないことに注意してください。詳細については、Microsoft Active Directory のマニュアルを参照してください。
- この機能が有効であっても Unified CM に影響はなく、LDAP ディレクトリ サーバに最小限の影響しか及ばない。
- SDK に付属のサンプル スクリプトでは、最小限のカスタマイズだけが可能である（たとえば、返送されたすべての番号の前に番号ストリングを付けられる）。もっと高度な操作のためには、カスタム スクリプトを作成する必要があり、スクリプトの作成に役立つプログラミング ガイドが SDK に付属しています。
- この機能は、社内ディレクトリに対する Unified CM ユーザのプロビジョニングまたは認証を必要としない。

Unified CM とのディレクトリ統合

この項では、社内 LDAP ディレクトリに対するユーザ プロビジョニングと認証を考慮した、Cisco Unified CM でのディレクトリ統合のメカニズムおよびベスト プラクティスについて説明します。この項では、次のトピックについて取り上げます。

- 「Cisco Unified Communications Directory のアーキテクチャ」（P.16-7）

  ここでは、Unified CM ユーザ関連アーキテクチャの概要を示します。

- 「LDAP 同期」（P.16-10）

  ここでは、LDAP 同期の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

- 「LDAP 認証」（P.16-19）

  ここでは、LDAP 認証の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

表 16-3 に、Cisco Unified Communication Manager での同期と認証用に現在サポートされている LDAP ディレクトリを示します。

表 16-3　LDAP ディレクトリのサポート

LDAP ディレクトリのタイプ	Cisco Unified CM 6.*x*	Cisco Unified CM 7.*x*	Cisco Unified CM 8.*x*
Microsoft AD 2000 Microsoft AD 2003 Microsoft AD 2008 Microsoft ADAM 2003 Microsoft LDS 2008	あり	あり Microsoft ADAM および LDS には、Cisco Unified CM 7.1(3) 以降のリリースが必要です。	あり ただし、Microsoft AD 2000 は、Unified CM 8.*x* ではサポートされていません。
Netscape 4.x	あり	サポート終了[1]	サポート終了[1]
iPlanet 5.0	あり	サポート終了[1]	サポート終了[1]
iPlanet 5.1 SunOne 5.2	あり	あり	あり
SunOne 6.x	あり	あり	あり
OpenLDAP 2.3.39 OpenLDAP 2.4	なし	あり[2]	あり

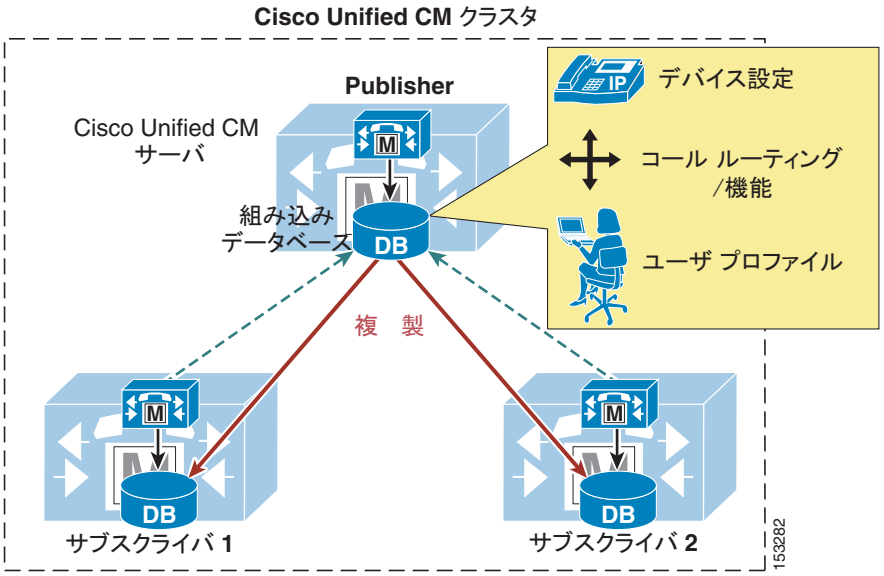
1. ディレクトリ ベンダーによると、このソリューションは販売終了になりました。
2. このディレクトリ タイプは、Cisco Unified CM 7.1(2) 以降のリリースだけでサポートされています。

（注）　表 16-3 に示されているすべての Microsoft Directory 製品には、Cisco Unified CM による同等のサポートがあります。この文書内の AD の参照はすべて、この表内のすべての Microsoft 製品に適用できます。

Cisco Unified Communications Directory のアーキテクチャ

図 16-3 は、Unified CM クラスタの基本アーキテクチャを示しています。組み込みデータベースには、デバイス関連データ、コール ルーティング、機能のプロビジョニング、およびユーザ プロファイルなど、すべての設定情報が保存されます。データベースは CM クラスタ内のすべてのサーバ上に存在し、パブリッシャ サーバからすべてのサブスクライバ サーバに自動的に複製されます。

図 16-3　Cisco Unified CM のアーキテクチャ



デフォルトでは、Unified CM Administration Web インターフェイスを介してすべてのユーザを手動でパブリッシャ データベースにプロビジョニングします。Cisco Unified CM には、次の 2 つのユーザ タイプがあります。

- エンド ユーザ：実在の人間でかつ対話形式のログインに関連付けられているすべてのユーザ。このカテゴリには、すべての Unified Communications ユーザのほか、User Groups and Roles 設定（以前のバージョンの Unified CM にある Cisco Multilevel Administration 機能に相当）を使用する場合の Unified CM 管理者も含まれます。
- アプリケーション ユーザ：Cisco Unified Communications の他の機能またはアプリケーション（Cisco Attendant Console、Cisco Unified Contact Center Express、Cisco Unified Communication Manager Assistant など）に関連付けられているすべてのユーザ。これらのアプリケーションは Unified CM に対して認証する必要がありますが、この内部「ユーザ」は対話形式のログインを行わず、単にアプリケーション間の内部通信だけを処理します。

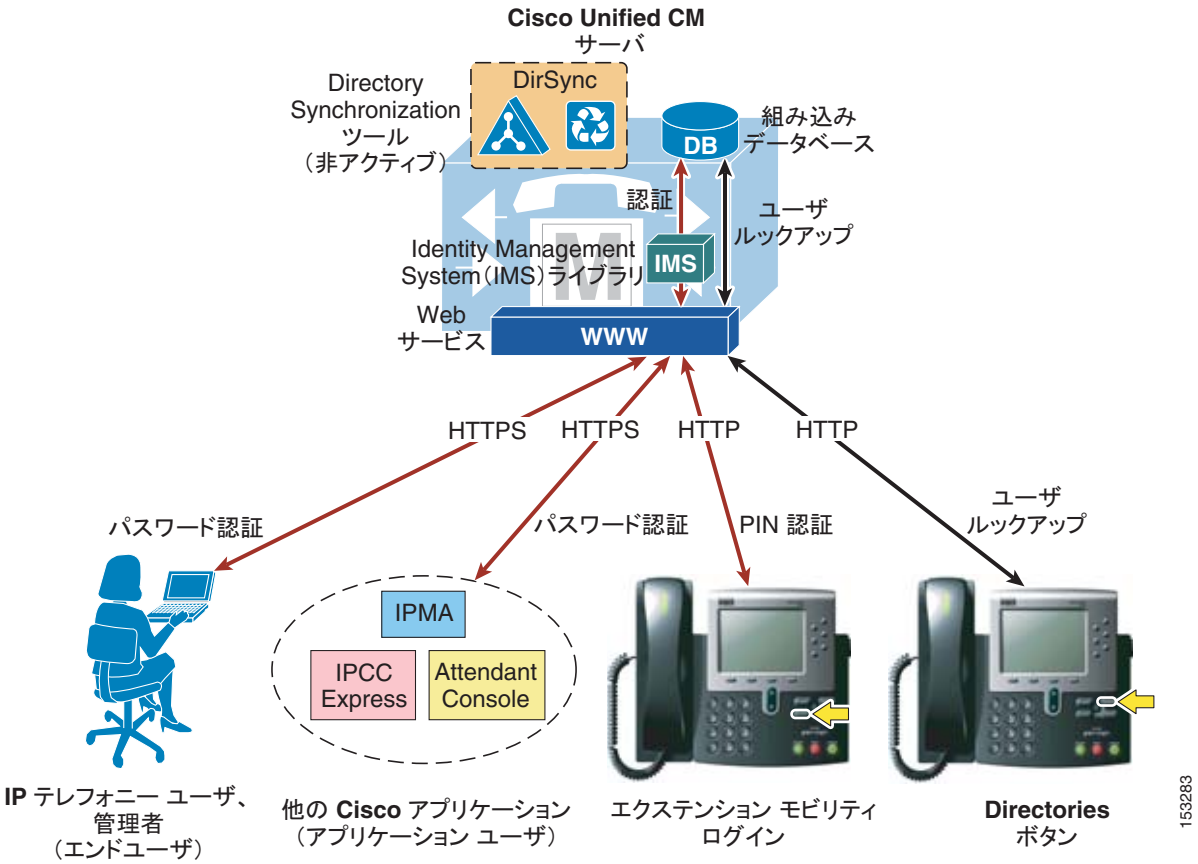
表 16-4 では、Unified CM データベースにデフォルトで作成されるアプリケーション ユーザのリストを、それらのユーザが使用される機能またはアプリケーションと共に示しています。Cisco Unified Communications の他のアプリケーションを統合する場合に、追加のアプリケーション ユーザを手動で作成できます（たとえば、Cisco Attendant Console の **ac** アプリケーション ユーザ、Cisco Unified Contact Center Express の **jtapi** アプリケーション ユーザなど）。

表 16-4　Unified CM のデフォルトのアプリケーション ユーザ

アプリケーション ユーザ	使用される機能またはアプリケーション
CCMAdministrator	Unified CM Administration（デフォルトは「スーパー ユーザ」）
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	シスコ エクステンション モビリティ
IPMASecureSysUser	Cisco Unified Communications Manager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

これらの考慮事項に基づいて、図 16-4 に、ルックアップ、プロビジョニング、認証などのユーザ関連操作に対する Unified CM でのデフォルト動作を示します。

図 16-4　Unified CM のユーザ関連操作に対するデフォルト動作



エンド ユーザは、HTTPS 経由で [Unified CM User Options] ページにアクセスし、ユーザ名およびパスワードで認証します。ユーザ グループと役割によって管理者として設定されている場合、エンド ユーザは同じクレデンシャルで Unified CM Administration のページにもアクセスできます。

同様に、シスコの他の機能とアプリケーションは、それぞれのアプリケーション ユーザに関連付けられたユーザ名およびパスワードで、HTTPS 経由で Unified CM に対して認証します。

HTTPS メッセージによって伝送される認証確認は、Unified CM の Web サービスにより、Identity Management System（IMS）という内部ライブラリにリレーされます。デフォルト設定では、IMS ライブラリは、組み込みデータベースに対してエンド ユーザとアプリケーション ユーザの両方を認証します。このように、Unified Communications システムにおける「現実の」ユーザと内部アプリケーション アカウントの両方が、Unified CM に設定されたクレデンシャルを使用して認証されます。

エンド ユーザは、IP Phone からエクステンション モビリティ サービスにログインするときに、ユーザ名と数値パスワード（PIN）で認証することもできます。この場合、認証確認は HTTP 経由で Unified CM に伝送されますが、やはり Web サービスにより IMS ライブラリにリレーされ、IMS ライブラリは組み込みデータベースに対してクレデンシャルを認証します。

さらに、Directories ボタンを介して Unified Communications エンドポイントによって実行されるユーザ ルックアップでは、HTTP 経由で Unified CM の Web サービスと通信し、組み込みデータベースのデータにアクセスします。

エンド ユーザとアプリケーション ユーザの区別の重要性は、社内ディレクトリとの統合が必要な場合に明らかになります。前の項で説明したように、この統合は次の 2 つの独立したプロセスによって実現されます。

- LDAP 同期

  このプロセスでは、Unified CM の Cisco Directory Synchronization（DirSync）という内部ツールを使用して、社内 LDAP ディレクトリから多数のユーザ属性を（手動または定期的に）同期します。この機能を有効にすると、ユーザは社内ディレクトリから自動的にプロビジョニングされます。この機能はエンド ユーザだけに適用され、アプリケーション ユーザは独立したままで、引き続き Unified CM Administration インターフェイスを介してプロビジョニングされます。要約すると、エンド ユーザは社内ディレクトリで定義され、Unified CM データベースに同期されますが、アプリケーション ユーザは Cisco Unified CM データベースに保存されるだけで、社内ディレクトリで定義する必要はありません。

- LDAP 認証

  このプロセスは、LDAP の標準的なシンプルバインド操作を使用して、IMS ライブラリによる社内 LDAP ディレクトリに対するユーザ クレデンシャルの認証を可能にします。この機能を有効にすると、エンド ユーザ パスワードは社内ディレクトリに対して認証されますが、アプリケーション ユーザ パスワードは引き続きローカルで Unified CM データベースに対して認証されます。Cisco エクステンション モビリティの PIN も引き続きローカルで認証されます。

Unified CM データベースに対して内部でアプリケーション ユーザを維持および認証すると、社内 LDAP ディレクトリの可用性とは無関係に、これらのアカウントを使用して Unified CM と通信するすべてのアプリケーションと機能に対して復元性が提供されます。

Cisco エクステンション モビリティの PIN も Unified CM データベース内で維持されます。これは、これらの PIN はリアルタイム アプリケーションの必須部分であり、リアルタイム アプリケーションは社内ディレクトリの応答性に依存しないようにする必要があるためです。

次の 2 つの項では、LDAP 同期と LDAP 認証についてさらに詳しく説明し、両方の機能に関して設計上のベスト プラクティスを示します。

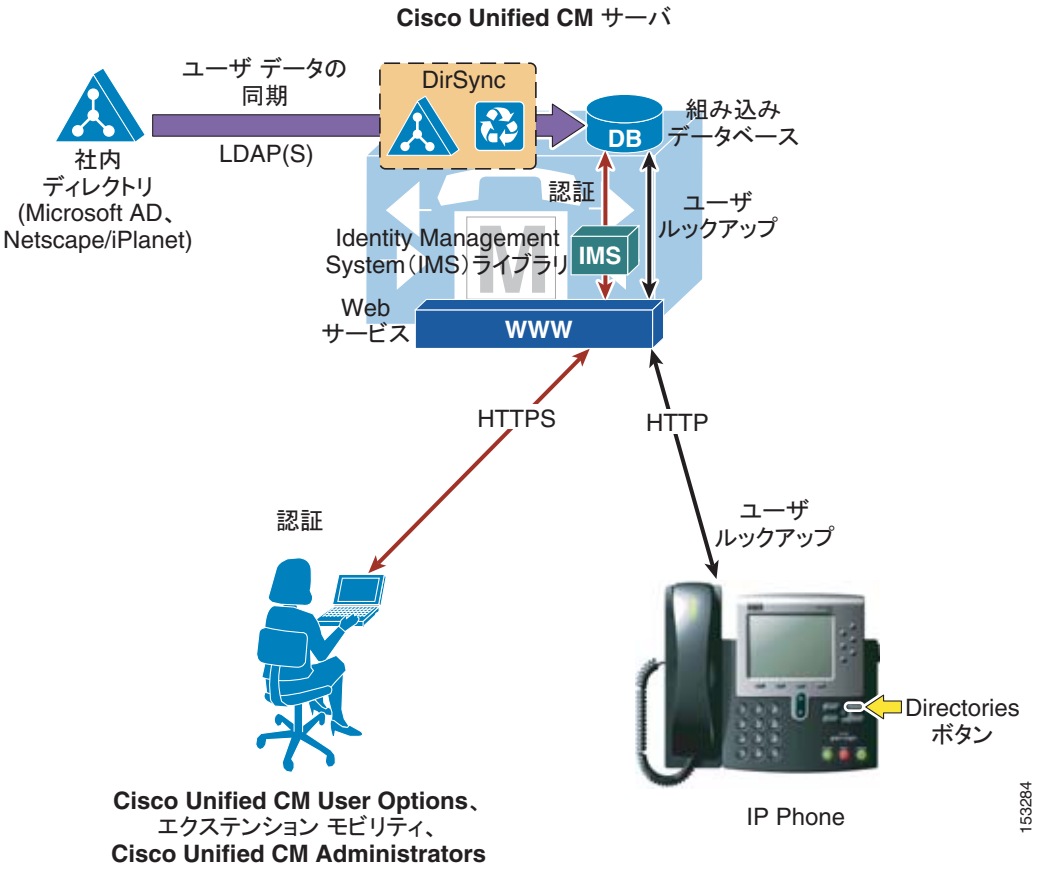
（注）　「Unified Communications エンドポイントのディレクトリ アクセス」（P.16-3）の項で説明したように、外部 Web サーバで Cisco Unified IP Phone Services SDK を設定することにより、エンドポイントからのユーザ ルックアップを社内ディレクトリに対して実行することもできます。

LDAP 同期

Unified CM を社内 LDAP ディレクトリに同期すると、管理者は Unified CM データ フィールドをディレクトリ属性にマッピングすることにより、ユーザを容易にプロビジョニングできるようになります。LDAP ストアに保持されている重要なユーザ データは、スケジュールまたはオンデマンド ベースで Unified CM データベース内の対応する適切なフィールドにコピーされます。社内 LDAP ディレクトリのステータスは、中央リポジトリのままとなります。Unified CM は、ユーザ データを保存するための統合データベースを備え、またユーザ アカウントおよびデータを作成して管理するための Web インターフェイスを、Unified CM Administration 内に備えています。LDAP 同期を有効にすると、ローカル データベースは引き続き使用されますが、エンド ユーザ アカウントを作成する Unified CM ファシリティが無効になります。その後、エンド ユーザ アカウントの管理は、LDAP ディレクトリのインターフェイスを介して実施されます（図 16-5 を参照）。アプリケーション ユーザのアカウントは引き続き、Unified CM Administration Web インターフェイスを使用して作成し、管理できます。

ユーザ アカウント情報は、LDAP ディレクトリから Unified CM パブリッシャ サーバにあるデータベースにインポートされます。LDAP ディレクトリからインポートされた情報は、Unified CM から変更できません。Cisco Unified Communications に固有の追加のユーザ情報は、Unified CM によって管理され、ローカル データベースだけに保存されます。たとえば、デバイスとユーザのアソシエーション、スピード ダイヤル、自動転送設定、およびユーザ PIN はすべて Unified CM が管理するデータの例であり、社内 LDAP ディレクトリには存在しません。次に、ユーザ データは組み込みデータベース同期メカニズムによって、Unified CM パブリッシャ サーバからサブスクライバ サーバに伝達されます。

図 16-5　ユーザ データ同期の有効化



LDAP 同期をアクティブにすると、一度に 1 つのタイプの LDAP ディレクトリだけをクラスタ用にグローバルに選択できます。また、LDAP ディレクトリ ユーザの 1 つの属性が選択されて [Unified CM User ID] フィールドにマッピングされます。Unified CM はデータへのアクセスに標準 LDAPv3 を使用します。

Cisco Unified CM は、標準属性からデータをインポートします。ディレクトリ スキーマの拡大は必要ありません。表 16-5 に、Unified CM の各フィールドへのマッピングに使用できる属性を示します。[Unified CM User ID] フィールドにマッピングされるディレクトリ属性のデータは、そのクラスタのすべてのエントリ内で一意のものである必要があります。[Cisco UserID] フィールドにマッピングされる属性はディレクトリに格納される必要があり、**sn** 属性はデータと一緒に格納される必要があります。そうしないと、このインポート処理時にこれらのレコードはスキップされます。エンド ユーザ アカウントのインポート中に使用するプライマリ属性が Unified CM データベースのいずれかのアプリケーション ユーザと一致する場合、そのエンド ユーザはスキップされます。

表 16-5 では、LDAP ディレクトリから対応する Unified CM ユーザ フィールドにインポートされた属性を示していて、またこれらのフィールド間のマッピングについて説明しています。Unified CM ユーザ フィールドの中には、複数の LDAP 属性の 1 つからマッピングされるものもあります。

表 16-5　同期化された LDAP 属性と対応する Unified CM フィールド名

Unified CM のユーザ フィールド	Microsoft Active Directory	Active Directory Application Mode（ADAM; Active Directory アプリケーション モード）または Active Directory Lightweight Directory Service（AD LDS; Active Directory ライトウェイト ディレクトリ サービス）	Netscape、iPlanet、または Sun ONE	OpenLDAP
User ID	*次のいずれか* sAMAccountName mail employeeNumber telephoneNumber userPrincipalName	*次のいずれか* uid mail employeeNumber telephoneNumber userPrincipalName	*次のいずれか* uid mail employeeNumber telephonePhone	*次のいずれか* uid mail employeeNumber telephonePhone
First Name	givenName	givenName	givenname	givenname
Middle Name	*次のいずれか* middleName initials	*次のいずれか* middleName initials	initials	initials
Last Name	sn	sn	sn	sn
Manager ID	manager	manager	manager	manager
Department	department	department	departmentnumber	departmentnumber
Phone Number	次のいずれか telephoneNumber ipPhone	次のいずれか telephoneNumber ipPhone	telephonenumber	telephonenumber
Mail ID	*次のいずれか* mail sAMAccountName	*次のいずれか* mail uid	*次のいずれか* mail uid	*次のいずれか* mail uid

表 16-6 に、Dirsynch プロセスによってインポートされ、Unified CM データベースにコピーされるが、管理者ユーザの設定 Web ページには表示されない追加属性のリストを示します。Microsoft OCS を使用する場合、属性 msRTCSIP-PrimaryUserAddress は AD に格納されます。この表は、完全な情報を提供する目的で記載されています。

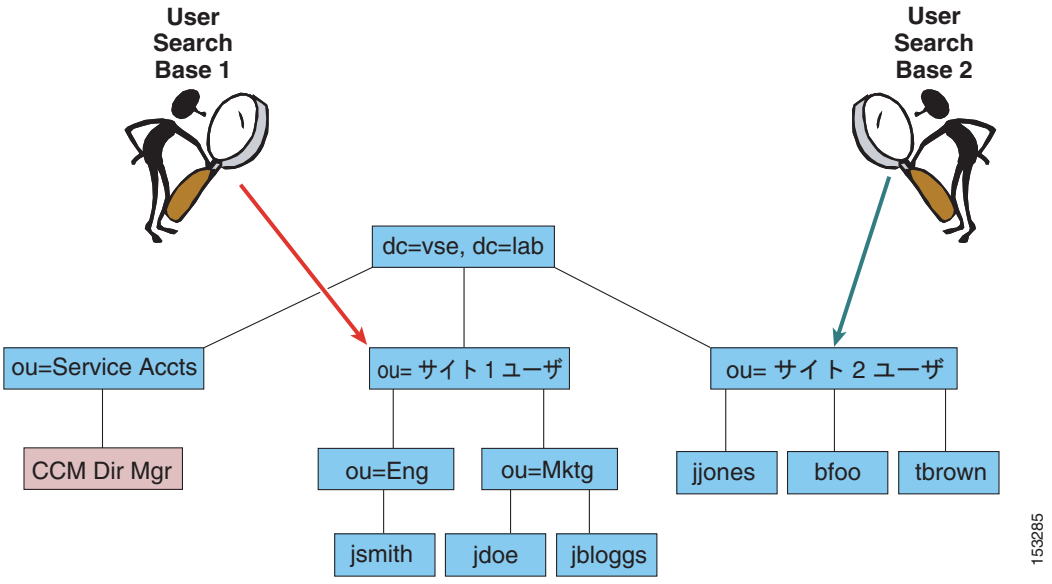
表 16-6　表示されない同期化 LDAP 属性

Unified CM のユーザ フィールド	Microsoft Active Directory	Netscape、iPlanet、または Sun ONE	OpenLDAP
objectGUID	objectGUID	適用されない	適用されない
OCSPrimaryUserAddress	msRTCSIP-PrimaryUserAddress	適用されない	適用されない
Title	title	Title	title
Home Phone Number	homePhone	Homephone	hometelephonenumber
Mobile Phone Number	mobile	Mobile	Mobiletelephonenumber
Pager Number	pager	Pager	pagertelephonenumber

同期は、Serviceability Web ページで有効にする Cisco DirSync というプロセスによって実行されます。このプロセスを有効にすることで、システムに 1 ～ 5 つの同期アグリーメントを設定できます。アグリーメントでは、LDAP ツリー内で Unified CM がインポートするユーザ アカウントの検索を開始する場所となる検索ベースを指定します。Unified CM は、特定の同期アグリーメントについて検索ベースで指定したドメインの領域に存在するユーザだけをインポートできます。

図 16-6 は、2 つの同期アグリーメントを示しています。一方の同期アグリーメントでは、User Search Base 1 を指定し、ユーザ jsmith、jdoe、jbloggs をインポートします。もう一方の同期アグリーメントでは、User Search Base 2 を指定し、ユーザ jjones、bfoo、tbrown をインポートします。CCMDirMgr アカウントは、ユーザ検索ベースで指定した場所の下位に存在しないので、インポートされません。ユーザを LDAP ディレクトリの構造に編成すると、その構造を使用して、どのユーザ グループをインポートするかを制御できます。この例では、単一の同期アグリーメントを使用してドメインのルートを指定することもできましたが、その検索ベースでは Service Accts もインポートしていたと考えられます。検索ベースではドメイン ルートを指定する必要はなく、ツリーのどの場所でも指定できます。

図 16-6　ユーザ検索ベース



データを Unified CM データベースにインポートするために、LDAP Manager Distinguished Name として設定で指定されたアカウントを使用して、システムが LDAP ディレクトリへのバインドを実行し、データベースの読み取りがこのアカウントで実行されます。Unified CM のログインのために、LDAP ディレクトリでアカウントが使用可能である必要があります。ユーザ検索ベースで指定したサブツリー内のすべてのユーザ オブジェクトの読み取り可能な権限を持つ、固有のアカウントを作成することを推奨します。同期アグリーメントでは、そのアカウントがドメイン内の任意の場所に存在できるように、アカウントの完全認定者名を指定します。図 16-6 の例では、CCMDirMgr が同期に使用するアカウントです。

アカウントのインポートは、LDAP Manager Distinguished Name アカウントの権限を使用して制御できます。この例では、ou=Eng への読み取りアクセスはできるが ou=Mktg への読み取りアクセスはできないようにこのアカウントを制限した場合、Eng の下位にあるアカウントだけがインポートされます。

同期アグリーメントには、複数のディレクトリ サーバを指定して冗長性を実現する機能があります。同期の試行時に使用するディレクトリ サーバを 3 つまで、順序付きのリストにして設定に指定できます。これらのサーバでの試行が、リストの最後まで順に行われます。どのディレクトリ サーバも応答しない場合、同期には失敗しますが、設定済みの同期スケジュールに従って再試行されます。

同期のメカニズム

同期アグリーメントでは、同期を開始する時刻を指定し、再同期の期間を時間、日、週、月のいずれかの単位（最小値は 6 時間）で指定します。同期アグリーメントは、特定の時刻に 1 回だけ実行するように設定することもできます。

Unified CM パブリッシャ サーバで同期を初めて有効にすると、社内ディレクトリに存在するユーザ アカウントが Unified CM データベースにインポートされます。そして、その後のプロセスに従って、既存の Unified CM エンド ユーザ アカウントがアクティブになってデータが更新されるか、新しいエンド ユーザ アカウントが作成されます。

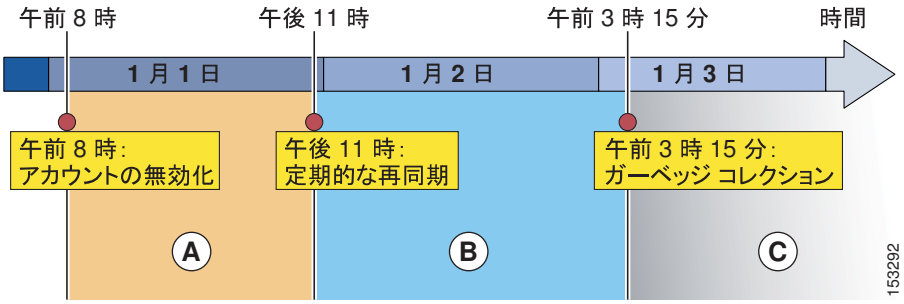
1. エンド ユーザ アカウントがすでに Unified CM データベースに存在するときに同期アグリーメントを設定した場合、Unified CM ですべての既存のアカウントは非アクティブとマークされます。同期アグリーメントの設定で、Unified CM UserID への LDAP データベース属性のマッピングを指定します。同期中に LDAP データベースのアカウントが既存の Unified CM アカウントと一致すると、その Unified CM アカウントは再びアクティブとマークされます。
2. 同期の完了後、アクティブに設定されなかったアカウントは、ガーベッジ コレクション プロセスの実行時に Unified CM から永続的に削除されます。ガーベッジ コレクションは、午前 3 時 15 分の定時に自動的に実行されるプロセスで、設定はできません。Unified CM は同期が設定されている間はアカウントを管理できないので、LDAP ディレクトリ アカウントと一致しない Unified CM アカウントの削除が必要です。
3. 後で社内ディレクトリに変更を加えると、スケジューリングされた次回の同期期間に、完全な再同期として Microsoft Active Directory から同期が行われます。これに対して、iPlanet および Sun ONE の各ディレクトリ製品は、ディレクトリに変更が加えられると差分同期を実行します。次の項では、2 つのシナリオのそれぞれの例を示します。

（注）　ユーザを LDAP から Unified CM データベースに同期した後で同期設定を削除すると、その設定によってインポートされたユーザには、データベース内で非アクティブのマークが付きます。その後、これらのユーザはガーベッジ コレクションによって削除されます。

Active Directory でのアカウント同期

図 16-7 は、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、イベントのスケジュールの例を示しています。再同期は、毎日午後 11 時に設定されています。

図 16-7　Active Directory での変更の伝達



最初の同期の後、アカウントの作成、削除、または無効化は、図 16-7 に示すスケジュールに従って、次の手順で説明するように Unified CM に伝達されます。

1. 1 月 1 日の午前 8 時に、AD でアカウントを無効にするか削除します。これ以降、期間 A 中は、Unified CM が認証を AD にリダイレクトするため、このユーザのパスワード認証（たとえば、[Unified CM User Options] ページ）は失敗します。ただし、PIN は Unified CM データベースに保存されているため、PIN 認証（たとえば、エクステンション モビリティ ログイン）は今までどおり成功します。
2. 定期的な再同期が 1 月 1 日 午後 11 時にスケジュールされています。このプロセス中に、Unified CM がすべてのアカウントを検証します。AD で無効にするか削除したアカウントは、この時点で Unified CM データベースでは非アクティブとしてタグ付けされます。1 月 1 日の午後 11 時より後に、アカウントが非アクティブとマークされると、Unified CM による PIN 認証とパスワード認証は両方とも失敗します。
3. アカウントのガーベッジ コレクションは毎日午前 3 時 15 分の定時に発生します。このプロセスは、24 時間以上非アクティブとマークされたレコードの Unified CM データベースからユーザ情報を永続的に削除します。この例では、1 月 2 日の午前 3 時 15 分に実行するガーベッジ コレクションでは、アカウントが非アクティブになってまだ 24 時間が経過していないので、アカウントを削除しません。したがって、アカウントは 1 月 3 日の午前 3 時 15 分に削除されます。この時点で、ユーザ データは Unified CM から永続的に削除されます。

期間 A の開始時にアカウントを AD で作成していた場合、そのアカウントは期間 B の開始時に実行される定期的な再同期で Unified CM にインポートされ、Unified CM ですぐにアクティブになります。

iPlanet または Sun ONE でのアカウント同期

iPlanet および Sun ONE 製品は差分同期アグリーメントをサポートし、Microsoft Active Directory とは異なる同期スケジュールを使用します。同期には、Internet Engineering Task Force（IETF）ドラフトで定義され、多くの LDAP 実装でサポートされている永続検索メカニズムが使用されます。図 16-8 では、LDAP 同期と LDAP 認証の両方を有効にした Unified CM 配置について、この同期スケジュールの例を示しています。

図 16-8　　iPlanet および Sun ONE での変更の伝達

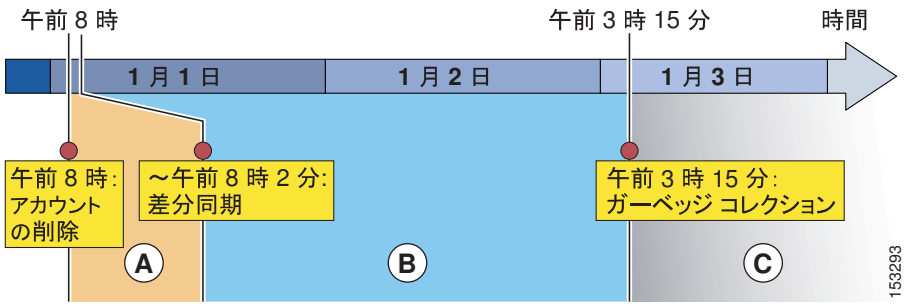


図 16-8 の例は、次の手順から構成されます。

1. 1 月 1 日の午前 8 時にアカウントが社内ディレクトリから削除され、これにより、差分更新データが LDAP サーバから Unified CM に送信されます。Unified CM は、データに対応するコピーを非アクティブに設定します。LDAP 認証が設定されているので、LDAP サーバがレコードを削除するとすぐに、ユーザはパスワードによるログインができなくなります。また、Unified CM レコードが非アクティブとマークされると、PIN をログインに使用できません。
2. 期間 B 中は、ユーザのレコードは非アクティブですが、まだ Unified CM に存在します。
3. 1 月 2 日の午前 3 時 15 分にガーベッジ コレクションが実行されるときは、レコードが非アクティブになってまだ 24 時間が経過していません。データは 1 月 3 日の期間 C の開始時まで Unified CM データベースに残り、ガーベッジ コレクション プロセスがこの日の午前 3 時 15 分に再び実行され、レコードが 24 時間以上にわたって非アクティブであったことを確認します。その結果、レコードはデータベースから永続的に削除されます。

ディレクトリで新規に作成したアカウントは、差分更新データによって同様に Unified CM に同期し、差分更新データが受信されるとすぐに使用できます。

セキュリティの考慮事項

アカウントのインポート中は、LDAP ディレクトリから Unified CM データベースに、パスワードも PIN もコピーされません。Unified CM で LDAP 同期が有効でない場合、エンド ユーザのパスワードは Unified CM Administration を使用して管理されます。パスワードと PIN は、暗号化形式で Unified CM データベースに保存されます。PIN は常に Unified CM で管理されます。LDAP ディレクトリ パスワードを使用してエンド ユーザを認証する場合は、「LDAP 認証」（P.16-19）の項を参照してください。

Unified CM および LDAP サーバで Secure LDAP（SLDAP）を有効にすることにより、Unified CM パブリッシャ サーバとディレクトリ サーバ間の接続を保護できます。Secure LDAP を使用すると、Secure Socket Layer（SSL）接続で LDAP 送信ができます。Unified CM Platform Administration 内で SSL 証明書をアップロードすることにより、Secure LDAP を有効にできます。詳細な手順については、http://www.cisco.com で入手可能な Unified CM の製品マニュアルを参照してください。SLDAP を有効にする方法については、LDAP ディレクトリ ベンダーのドキュメンテーションを参照してください。

LDAP 同期に関する設計上の考慮事項

Cisco Unified CM で LDAP 同期を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内で特定のアカウントを使用し、Unified CM 同期アグリーメントがそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを最低限の「読み取り」権限を 設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することを推奨します。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。サービス アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定をアップデートしてください。
- 所定のクラスタにあるすべての同期アグリーメントは、同じ LDAP サーバ ファミリと統合する必要がある。
- 複数のアグリーメントが同時に同じ LDAP サーバに照会することがないように、同期アグリーメントのスケジューリングに時間差を設ける。待機期間中（オフピーク時間）の同期時刻を選択します。
- ユーザ データのセキュリティが必要である場合、Unified CM Administration の [LDAP Directory] 設定ページで [Use SSL] フィールドのチェックボックスをオンにして、Secure LDAP（SLDAP）を有効にする。
- [Unified CM UserID] フィールドへのマッピングのために選択した LDAP ディレクトリ属性が、そのクラスタのすべての同期アグリーメント内で一意であることを確認する。
- UserID として選択した属性は、Unified CM で定義したアプリケーション ユーザのいずれかの属性と同じであってはならない。
- LDAP 属性 sn（姓）は、ユーザの LDAP 同期の必須属性である。
- 同期前の Unified CM データベースにある既存のアカウントは、LDAP ディレクトリからインポートされたアカウントの属性に一致する場合だけ維持される。Unified CM UserID に一致する属性は、同期アグリーメントによって確認されます。
- エンド ユーザ アカウントは LDAP ディレクトリの管理ツールによって管理し、これらのアカウントのシスコ固有データは Unified CM Administration Web ページによって管理する。
- LDAP 同期は、Microsoft NT LAN Manager（NTLM）でのみサポートされます。Kerberos と NTLMv2 はサポートされていません。
- AD の配置については、ObjectGUID がユーザの主要属性として Unified CM で内部的に使用される。[Unified CM User ID] に対応する AD 内の属性は、AD 内で変更できます。たとえば、sAMAccountname を使用している場合、ユーザは自分の sAMAccountname を AD で変更することができ、Unified CM 内で対応するユーザ レコードは更新されます。

  その他すべての LDAP プラットフォームでは、User ID にマッピングされる属性が Unified CM におけるそのアカウントの主要属性となります。LDAP 内の属性を変更すると、Unified CM に新しいユーザが作成され、元のユーザには非アクティブのマークが付きます。

Microsoft Active Directory に関する追加の考慮事項

ドメインの同期アグリーメントでは、ドメイン外のユーザや子ドメイン内のユーザは同期されません。同期プロセス中は Unified CM が AD 照会に従わないためです。図 16-9 の例では、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。Search Base 1 ではツリーのルートを指定しますが、子ドメインのいずれかに存在するユーザはインポートしません。範囲は VSE.LAB に限定されており、残りの 2 つのドメインに対し、そのユーザをインポートするように別々のアグリーメントが設定されています。

図 16-9　複数の Active Directory ドメインでの同期

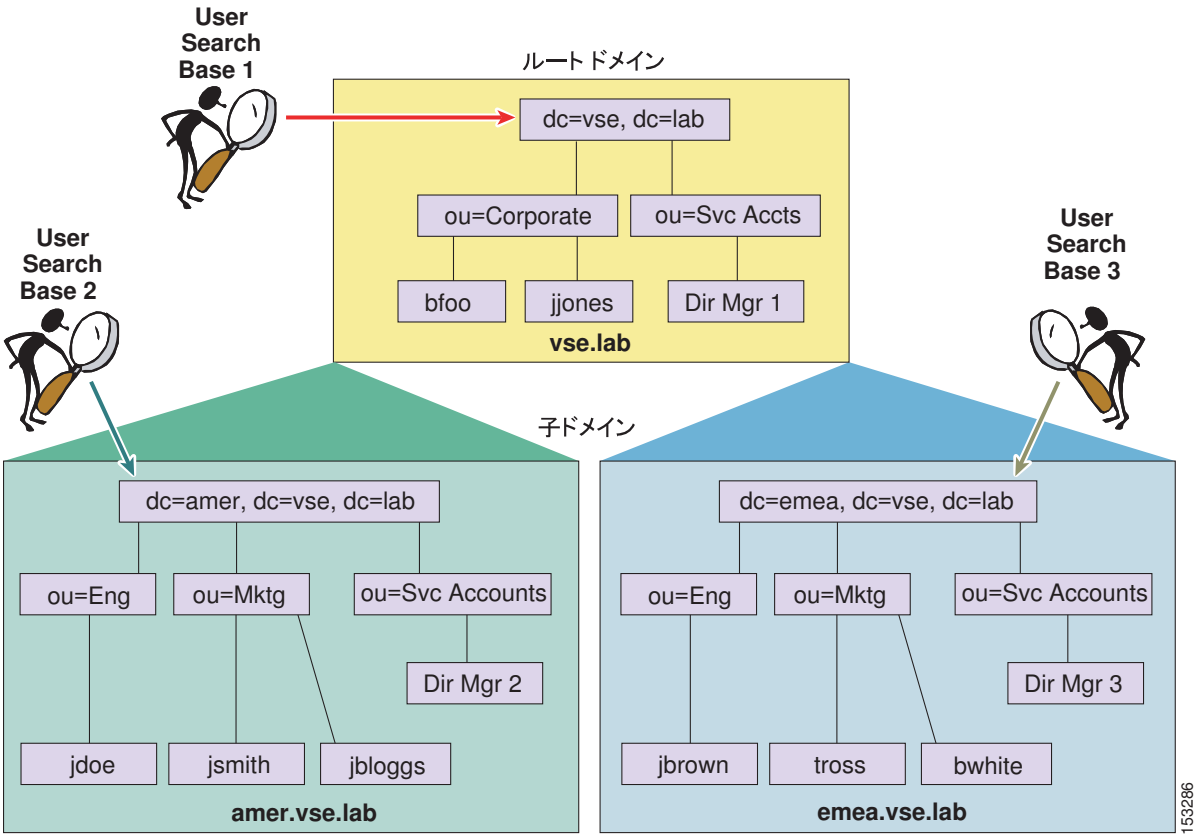
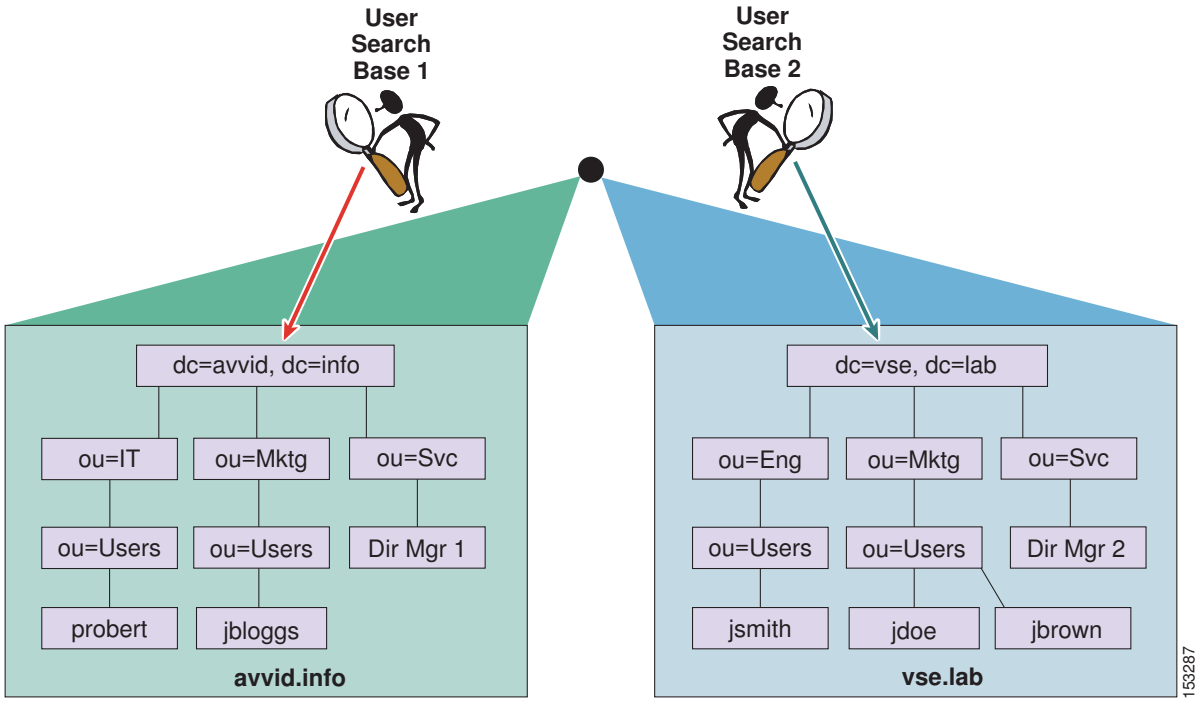


図 16-9 では、ドメインとサブドメインのそれぞれに少なくとも 1 つの Domain Controller（DC; ドメイン コントローラ）が関連付けられ、3 つの同期アグリーメントはそれぞれ適切なドメイン コントローラを指定します。DC にある情報は、その DC が存在するドメイン内のユーザの情報だけなので、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。

図 16-10 に示すように、複数のツリーを含む AD フォレストで同期を有効にした場合も、上記と同じ理由で複数の同期アグリーメントが必要です。さらに、UserPrincipalName（UPN）属性がフォレスト全体で一意であることが Active Directory によって保証され、この属性は Unified CM UserID にマッピングする属性として選択する必要があります。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、「Microsoft Active Directory に関する追加の考慮事項」（P.16-21）の項を参照してください。

図 16-10　複数の AD ツリー（不連続なネームスペース）での同期



アカウントの同期を実行すると、Unified CM から AD にデフォルトの LDAP サーチ フィルタ ストリングが送信されます。その中に、AD で無効のマークが付いているアカウントを戻さないという条件があります。ログインの失敗回数を超えた場合など、AD によって無効のマークが付けられたアカウントには、そのアカウントが無効である間に同期が実行された場合に非アクティブのマークが付けられます。

Unified CM マルチフォレスト LDAP 同期

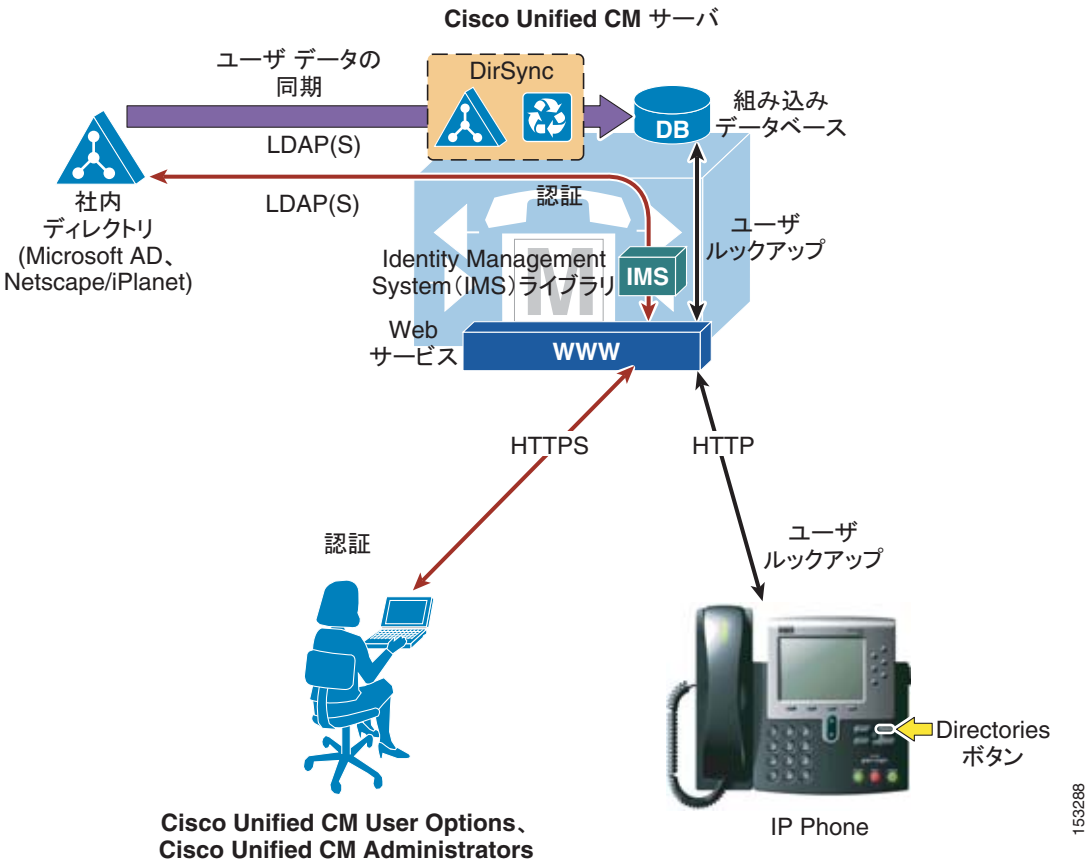
マルチフォレスト LDAP インフラストラクチャを使用した Unified CM 展開は、複数の異種フォレストを統合する単一のフォレスト ビューとして AD LDS を使用することによって、サポートできます。この統合では、LDAP フィルタリングを使用する必要があります（「ディレクトリ同期および認証のユーザ フィルタリング」（P.16-23）を参照）詳細については、次の URL で入手可能な『*How to Configure Unified Communication Manager Directory Integration in a Multi-Forest Environment*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example09186a0080b2b103.shtml

LDAP 認証

LDAP 認証機能を使用すると、組み込みデータベースを使用する代わりに、社内 LDAP ディレクトリに対して Unified CM でエンド ユーザ パスワードを認証できます。図 16-11 に示すように、Unified CM 内の IMS モジュールと社内ディレクトリ サーバ間で確立した LDAPv3 接続によって、この認証が実現されます。

図 16-11　　LDAP 認証の有効化



認証を有効にするために、クラスタ全体に単一の認証アグリーメントを定義できます。認証アグリーメントは、冗長性を得るために LDAP サーバを 3 つまで設定でき、必要に応じて保護接続 Secure LDAP（SLDAP）もサポートします。認証は、LDAP 同期が正しく設定され、使用されている場合にのみ有効にできます。

認証を有効にした場合の Unified CM の動作説明を、次に示します。

- エンド ユーザ パスワードは、シンプル バインド操作によって社内ディレクトリに対して認証される。
- アプリケーション ユーザ パスワードは、Unified CM データベースに対して認証される。
- エンド ユーザ PIN は、Unified CM データベースに対して認証される。

この動作は、リアルタイム Unified Communications システムの操作を社内ディレクトリの可用性に依存しないようにしながら、シングル ログイン機能をエンド ユーザに提供するという原則に従ったものです。図 16-12 に図示します。

図 16-12　エンド ユーザ パスワード、アプリケーション ユーザ パスワード、エンド ユーザ PIN の認証

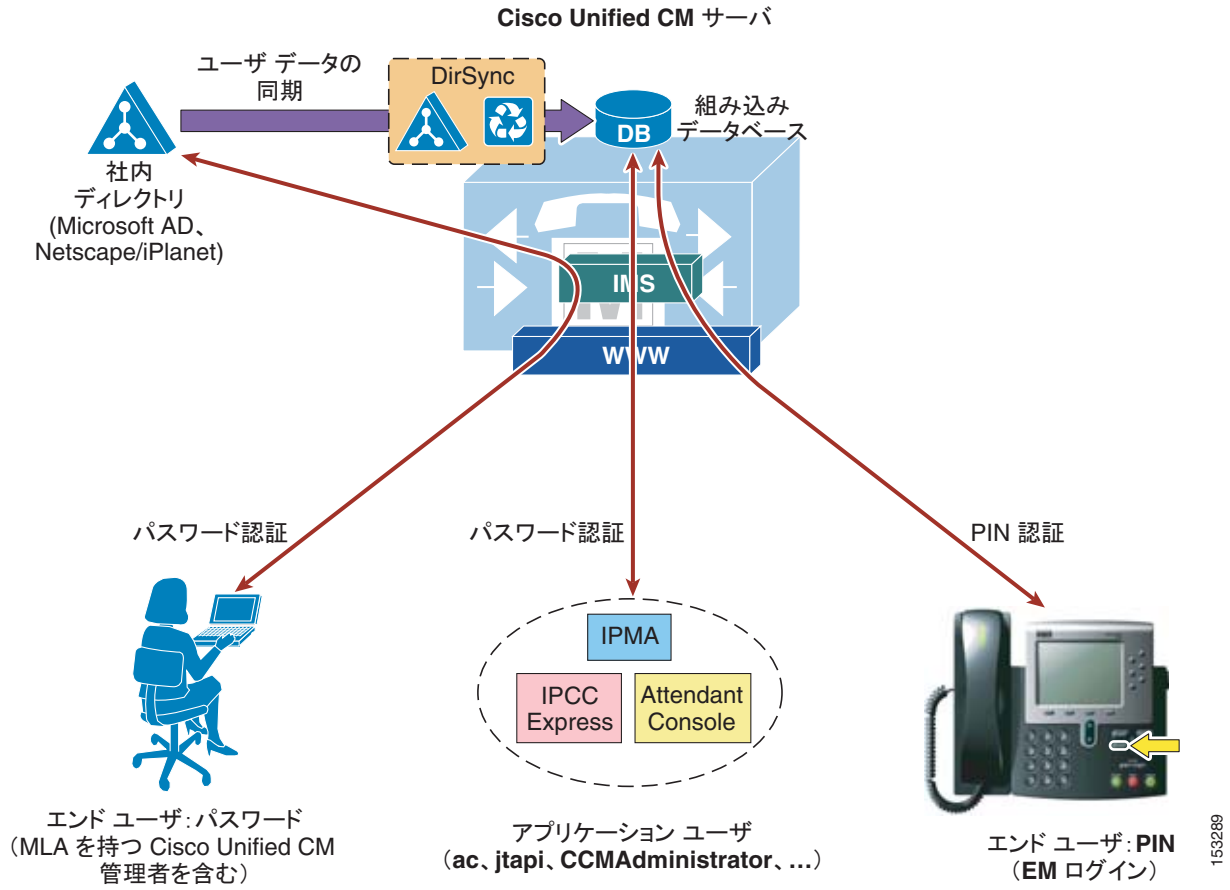
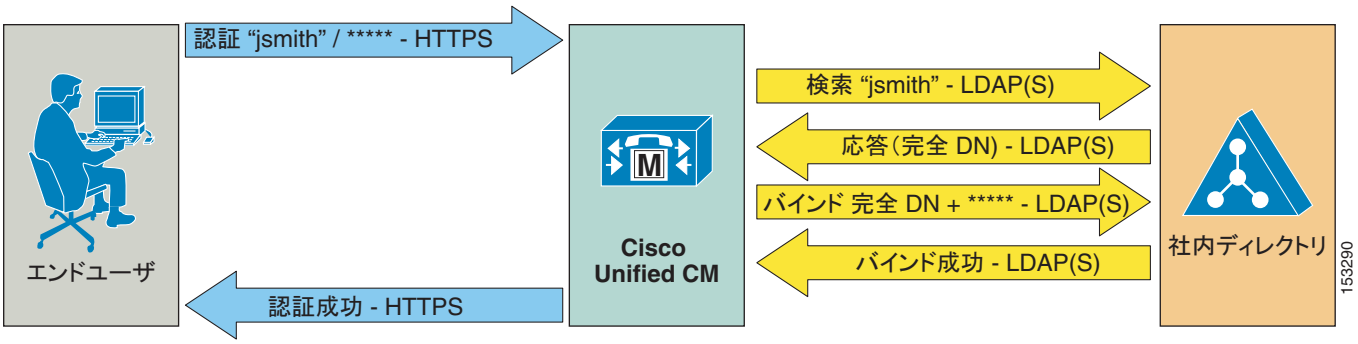


図 16-13 は、エンド ユーザを社内 LDAP ディレクトリに対して認証するために Unified CM で採用された、次のプロセスを示しています。

1. ユーザは、HTTPS 経由で [Unified CM User Options] ページに接続し、ユーザ名とパスワードで認証を試行します。この例では、ユーザ名は jsmith です。
2. Unified CM はユーザ名 jsmith に関する LDAP 照会を発行し、[LDAP Authentication] 設定ページの [LDAP Search Base] で指定された値を、この照会の範囲として使用します。SLDAP を有効にした場合、この照会は SSL 接続を通じて行われます。
3. 社内ディレクトリ サーバは、LDAP 経由で、ユーザ jsmith の完全 Distinguished Name（DN; 認定者名）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. 次に Unified CM は、LDAP バインド操作を使用して、ユーザに提供された完全な DN とパスワードを渡すことにより、ユーザのクレデンシャルの検証を試みます。
5. LDAP バインドが成功した場合、Unified CM は、要求された設定ページにユーザが進むことを許可します。

図 16-13　認証プロセス



LDAP 認証に関する設計上の考慮事項

Cisco Unified CM で LDAP 認証を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内に特定のアカウントを作成し、Unified CM がそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Unified CM 専用のアカウントを使用することを推奨します。ディレクトリ内のこのアカウントのパスワードは、Unified CM 内のアカウントのパスワード設定と同期し続ける必要があります。アカウントのパスワードがディレクトリ内で変更された場合は、必ず Unified CM でアカウント設定を更新してください。LDAP 同期も有効にする場合、両方の機能に同じアカウントを使用できます。
- LDAP Manager Distinguished Name および LDAP Password で前述のアカウントのクレデンシャルを指定し、LDAP User Search Base ですべてのユーザが存在するディレクトリ サブツリーを指定することにより、Unified CM で LDAP 認証を有効にする。
- この方法では、シングル ログイン機能をすべてのエンド ユーザに提供する。エンド ユーザは、[Unified CM User Options] ページにログインすると、社内ディレクトリ クレデンシャルを使用できるようになります。
- 社内ディレクトリ インターフェイスでエンド ユーザ パスワードを管理する。認証を有効にすると、Unified CM Administration のページにパスワード フィールドが表示されなくなります。
- Unified CM Administration の Web ページまたは [Unified CM User Options] ページでエンド ユーザ PIN を管理する。
- Unified CM Administration の Web ページでアプリケーション ユーザのパスワードを管理する。アプリケーション ユーザは他の Cisco Unified Communications アプリケーションとの通信やリモート 呼制御を容易にすること、また、実際のユーザには関連付けられないことに留意してください。
- 対応するエンド ユーザを Unified CM Administration の Web ページから Unified CM Super Users ユーザ グループに追加することにより、Unified CM 管理者のシングル ログインを有効にする。カスタマイズしたユーザ グループおよびロールを作成することにより、複数レベルの管理者権利を定義できます。

Microsoft Active Directory に関する追加の考慮事項

複数のドメイン コントローラを地理的に分散させた分散型 AD トポロジを採用している環境では、認証速度が許容されない可能性があります。認証アグリーメント用のドメイン コントローラにユーザ アカウントが保持されていない場合、他のドメイン コントローラでそのユーザの検索が実行される必要があります。この設定を適用するときに、ログイン速度が許容範囲外である場合、グローバル カタログ サーバを使用するように認証設定を設定できます。

ただし、重要な制限があります。グローバル カタログは Employee ID 属性を伝送しないので、Employee ID をログインとして使用する場合には、この方法は使用できません。この属性には、ドメイン コントローラだけを使用できます。

グローバル カタログに対する照会を有効にするには、グローバル カタログ ロールが有効になっているドメイン コントローラの IP アドレスまたはホスト名を指すように [LDAP Authentication] ページの [LDAP Server Information] を設定し、LDAP ポートを 3268 として設定するだけです。

Microsoft AD から同期するユーザが複数のドメインに属していると、認証へのグローバル カタログの使用がさらに効率的になります。Unified CM は、照会に従う必要がなく、すぐにユーザを認証できるためです。このような場合は、Unified CM がグローバル カタログ サーバを指すようにし、LDAP User Search Base をルート ドメインの最上位に設定します。

複数のツリーを含む Microsoft AD フォレストの場合には、追加の考慮事項が適用されます。単一の LDAP 検索ベースでは複数のネームスペースを扱えないので、Unified CM は別のメカニズムを使用して、これらの不連続なネームスペース間でユーザを認証する必要があります。

「LDAP 同期」（P.16-10）の項で説明したように、複数のツリーがある AD フォレストで同期をサポートするために、UserPrincipalName（UPN）属性を Unified CM 内でユーザ ID として使用する必要があります。ユーザ ID が UPN の場合、Unified CM Administration の [LDAP Authentication] 設定ページで [LDAP Search Base] フィールドへの入力はできませんが、その代わりに「LDAP user search base is formed using userid information.」という注意が表示されます。

実際には、図 16-14 に示すように、ユーザごとに UPN サフィックスからユーザ検索ベースが導き出されます。この例では、Microsoft Active Directory フォレストは avvid.info と vse.lab という 2 つのツリーで構成されます。同じユーザ名が両方のツリーに表示される場合があるため、同期プロセス中および認証プロセス中は UPN を使用してデータベースのユーザを一意に識別するように、Unified CM が設定されています。

図 16-14　複数のツリーがある Microsoft AD フォレストでの認証

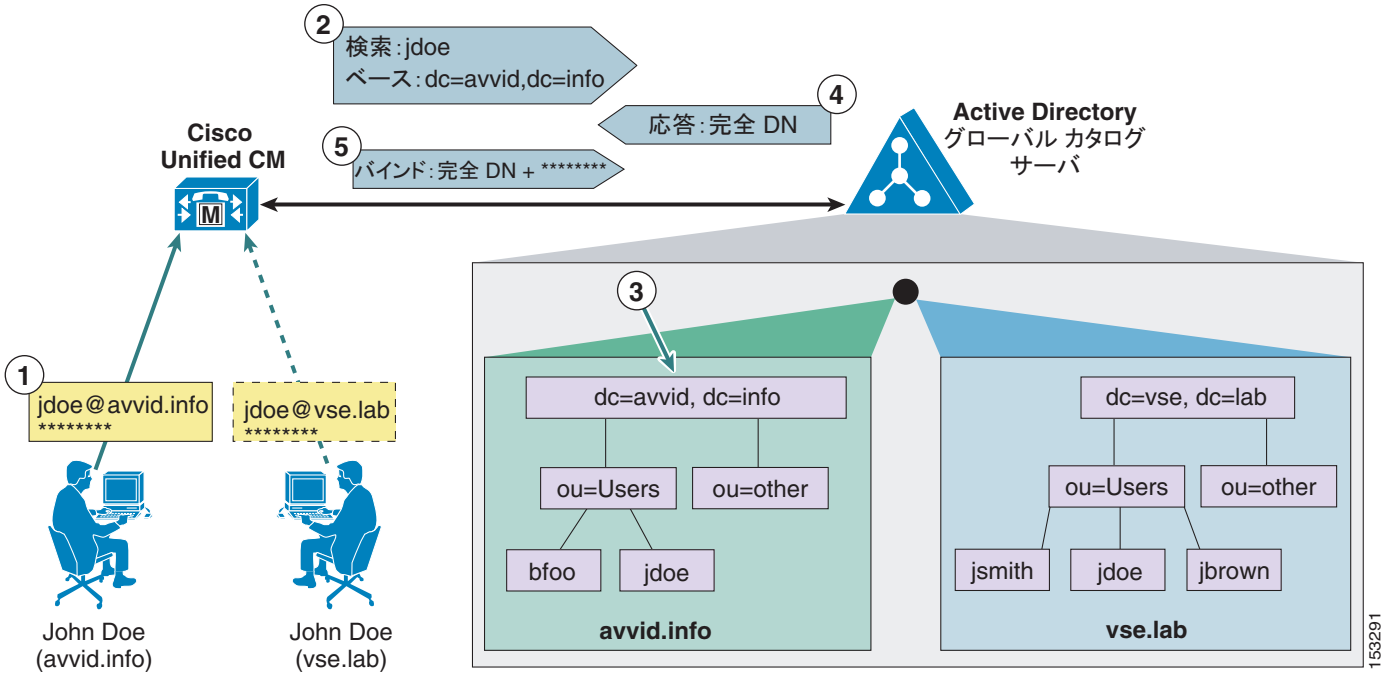


図 16-14 に示すように、John Doe という名前のユーザが avvid.info ツリーと vse.lab ツリーの両方に存在します。次の手順は、UPN が jdoe@avvid.info となる第 1 のユーザに対する認証プロセスを示しています。

1. ユーザは、ユーザ名（UPN に対応するもの）とパスワードを使用し、HTTPS 経由で Unified CM に対して認証します。
2. Unified CM は、Microsoft Active Directory グローバル カタログ サーバに対して LDAP 照会を実行し、UPN で指定したユーザ名（@ 記号よりも前の部分）を使用して、UPN サフィックス（@ 記号より後の部分）から LDAP 検索ベースを得ます。この場合、ユーザ名は jdoe で、LDAP 検索ベースは「dc=avvid, dc=info」です。
3. Microsoft Active Directory は、LDAP 照会で指定したツリーのユーザ名に対応する正しい認定者名を識別します。この場合は、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Microsoft Active Directory は LDAP 経由で、このユーザの完全認定者名を使用して Unified CM に応答します。
5. Unified CM は、提供された認定者名とユーザが最初に入力したパスワードで LDAP バインドを試行し、その後は図 16-13 に示す標準的な場合と同様に、認証プロセスが続行されます。

（注）　複数のツリーを含む Microsoft AD フォレストでの LDAP 認証のサポートは、上記の方法だけで行われます。したがってサポートは、ユーザの UPN サフィックスが、そのユーザが存在するツリーのルートドメインに対応する配置だけに限定されます。AD では、異なる UPN サフィックスが許可されたエイリアスを使用できます。UPN サフィックスがツリーの実際のネームスペースから分離されている場合は、Microsoft Active Directory フォレスト全体で Unified CM ユーザを認証できなくなります（ただし、その場合でも、別の属性をユーザ ID として使用し、統合をフォレスト内の単一のツリーに限定することはできます）。

ディレクトリ同期および認証のユーザ フィルタリング

Unified CM は、ディレクトリ同期のパフォーマンスを最適化するために、LDAP 照会フィルタを提供します。各クラスタの Unified Communications リソースに割り当てられるディレクトリ ユーザ アカウントだけをインポートすることを推奨します。ディレクトリ ユーザ アカウントの数が、各クラスタに対してサポートされている数を超える場合は、フィルタリングを使用して、そのクラスタに関連付けられるユーザのサブセットを選択する必要があります。Unified CM 同期機能は、大規模な社内ディレクトリに置き換わるものではありません。

多くの場合、同期対象のアカウントを制御するために必要となるのは、固有の検索ベースだけです。固有の検索ベースを使用できない場合は、カスタム LDAP フィルタが必要となることがあります。以降の項では、ディレクトリ同期の最適化に使用できる両方の方法について説明します。いずれかのメカニズムを使用して Unified CM へのアカウントのインポートを制限する場合、デフォルトのディレクトリ ルックアップの設定では、Unified CM データベースに存在するディレクトリ エントリだけが表示されます。ディレクトリ全体にアクセスするディレクトリ ルックアップの場合は、外部 Web サーバを使用するように Unified CM を設定する必要があります。この設定の詳細については、ここでは説明しませんが、次の Web サイトで入手可能な Unified CM 製品マニュアルで説明しています。

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/tsd_products_support_series_home.html

Unified CM データベース同期の最適化

Unified CM データベース同期機能には、LDAP ディレクトリ ストアから Unified CM パブリッシャ データベースへユーザ設定データ（属性）のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ サーバは、このクラスタから Unified Communications サービスを受けているユーザの一意のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。Unified Communications リソースが割り当てられるユーザだけが Unified CM と同期します。LDAP ディレクトリに定義されているユーザのセット全体が Unified CM クラスタにインポートされない共通の理由の一部を、次に示します。

- Unified Communications リソースが割り当てられないユーザのインポートにより、ディレクトリ同期時間が増加する。
- Unified Communications リソースが割り当てられていないユーザのインポートにより、Unified CM 検索とデータベース全体のパフォーマンスが遅くなる可能性がある。
- 多くの場合、LDAP ディレクトリ ストアのユーザ アカウント数が、Unified CM データベースの合計ユーザ容量を大幅に超過する。

Unified CM には、システムに追加できるアカウント数の制限がありません。シスコは、サポートされているエンドポイント数と同数のユーザ数に制限することを推奨します。たとえば、Cisco MCS-7845 サーバのフルサイズ クラスタは最大 30,000 エンドポイントをサポートしているので、システムで管理するユーザ数をおおよそ 30,000 に制限します。アプリケーション用のアカウントが必要な場合や、設計によっては追加のアカウントが必要な場合があります。

シスコは、ここで説明している制御メカニズムを使用して、LDAP データベース サイズに関係なく、インポートされるユーザ アカウントを最小限にすることを推奨します。これによって、最初とそれ以降の定期同期化の速度が改善され、ユーザ アカウントの管理可能性も向上します。

同期を制御するための LDAP 構造の使用

多数の LDAP ディレクトリの配置には、Organizational Unit Name（OU; 組織ユニット名）を使用して、ユーザを論理的順序や、場合によっては階層的順序でグループ化します。ユーザを複数の OU に編成する構造が LDAP ディレクトリにある場合、インポートされるユーザのグループを制御するためにこの構造を使用することもできます。各個別 Unified CM 同期アグリーメントは、単一の OU を指定します。サブ OU 内であっても、指定 OU の下にある全アクティブ アカウントがサポートされます。OU 内のユーザだけが同期されます。ユーザを含む複数の OU がクラスタで必要な場合、複数の同期アグリーメントが必要です。Unified Communications リソースを割り当てられていないユーザが OU に含まれている場合は、これらの OU をディレクトリ同期から省くことを推奨します。

AD に同じ手法を使用して、コンテナを定義できます。同期アグリーメントでは、ディレクトリ ツリーの特定のコンテナを指定でき、それによってインポートの範囲を制限できます。

使用できる同期アグリーメントは 5 つだけなので、多数の OU やコンテナを持つ LDAP の配置では、この手法はすぐに使い果たされてしまいます。複数の OU がある環境でユーザを同期するには、同期サービス アカウントに割り当てる権限を制御するという方法があります。複数のユーザが存在するツリー ノードに同期アグリーメントを設定してから、システム アカウントの読み取りアクセスをサブツリーの選択部分に制限します。このアクセスを制限する方法については、LDAP ベンダーのドキュメンテーションを参照してください。

LDAP 照会

次のいずれかの理由により、フィルタリングに対して追加の制御が必要となる場合があります。

- LDAP ディレクトリがフラット構造となっており、同期アグリーメントの設定によって適切に制御できない。すべての同期アグリーメントによってインポートされるユーザの集約数が 60,000 を超える場合は、フィルタを介してインポートされるユーザの数を制御する必要があります。
- 管理目的でユーザをセグメント化するために、ユーザ アカウントのサブセットを Unified CM クラスタにインポートし、クラスタへのアクセス権および認証を持つユーザのサブセットを制御する必要がある。クラスタにインポートされるいずれかのアカウントが、Web ページへのあるレベルのアクセス権および認証メカニズムを持ち、このことが適切でない場合があります。
- LDAP ディレクトリ構造が、Unified CM クラスタにユーザをマッピングする方法を正確に反映していない。たとえば、OU は組織階層に応じて設定されているものの、ユーザは地理的に Unified CM にマッピングされている場合、これら 2 つの間で重複する部分はほとんどありません。

このような場合、LDAP 照会フィルタを使用して、同期アグリーメントに対して追加の制御を提供できます。

LDAP 照会フィルタ構文およびサーバ側フィルタリング

Unified CM は、標準の LDAP メカニズムを使用して、LDAP ディレクトリ ストアのデータを同期します。Unified CM は、RFC 2251 の Lightweight Directory Access Protocol (v3) で規定されているように、検索メカニズムを使用して要求を送信し、LDAP サーバからデータを取得します。このメカニズムでは、検索メッセージ内のフィルタ ストリング指定する機能も定義されています。LDAP サーバはフィルタ ストリングを使用して、データを返すデータベースのエントリを選択します。フィルタ ストリングの構文は、RFC 2254 の The String Representation of LDAP Search Filters で規定されています。この RFC を参照用として使用して、より複雑なフィルタ ストリングを作成できます。

フィルタ ストリングは、Unified CM から LDAP サーバに送信される検索メッセージに組み込まれ、LDAP サーバはそれを実行して、応答で提供するユーザ アカウントを選択します。

単純なフィルタ構文

標準の属性名と、それらの属性に必要な値を指定して、フィルタを設定できます。属性は、名前の代わりに DN 要素で指定することもできます。Unified CM によって LDAP 照会で使用されるフィルタ ストリングは、ldapfilter テーブルの内部に格納され、検索メッセージに挿入されます。

フィルタは、次の構文を持つ UTF-8 形式のストリングです。

(*attribute operator value***)**

　または、

(*operator***(***filter1***)(***filter2***))**

ここで、*filter1* および *filter2* には、最初の行で示した構文が含まれ、*operator* は、表 16-7 に示す演算子のいずれかとなります。*attribute* は、ディレクトリ内に存在する LDAP 属性に対応し、*operator* は、表 16-7 に示す演算子のいずれかとなり、*value* は、その属性に必要な実際のデータ値に対応します。

表 16-7　フィルタ ストリングの基本的な演算子

演算子	機能の意味
!	論理否定
&	論理積
\| | 論理和 |

表 16-7　フィルタ ストリングの基本的な演算子 （続き）

演算子	機能の意味
*	ワイルドカード
=	等しい
>=	辞書順における以上
<=	辞書順における以下

フィルタでは、LDAP ディレクトリ ストアに存在する任意の属性を指定できます。この属性は、Unified CM によって認識およびインポートされる属性である必要はありません。属性は、LDAP サーバでデータを選択するためにだけ使用され、対応するエントリには、Unified CM にインポートされるデータのサブセットが含められます。

例 16-1　単一の条件

(givenName=Jack)

例 16-1 のフィルタでは、指定された名前 Jack を持つすべてのユーザが選択されます。

例 16-2　複数の条件（論理文字を使用して結合）

(&(objectclass=user)(department=Engineering))

例 16-2 のフィルタでは、エンジニアリング部門のすべてのユーザが選択されます。

デフォルトのフィルタ ストリング

フィルタ ストリングには、ldapfilter テーブル、typeldapserver のデフォルト値が含まれており、このデフォルト値は、次に示すように、使用される LDAP ディレクトリ ストアに応じて異なります。

- Active Directory（AD）のデフォルトのフィルタ ストリング

  (&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))

  このデフォルト フィルタでは、オブジェクト クラスがコンピュータではなくユーザであり、かつアカウントに無効のフラグが付いていないエントリが選択されます。

- SunOne または Netscape のデフォルトのフィルタ ストリング

  (objectclass=inetOrgPerson)

  このデフォルト フィルタでは、オブジェクト クラスが inetOrgPerson であるすべてのユーザが選択されます。

- OpenLDAP のデフォルトのフィルタ ストリング

  (objectclass=inetOrgPerson)

- Active Directory Application Mode（ADAM; Active Directory アプリケーション モード）または Active Directory Lightweight Directory Services（AD LDS; Active Directory ライトウェイト ディレクトリ サービス）のデフォルトのフィルタ ストリング

  (&(objectclass=user)((objectclass=Computer))(!(msDS-UserAccountDisabled=TRUE)))

デフォルト フィルタの拡張

デフォルトのフィルタ ストリングを使用して、そこに追加の条件を付加することを推奨します。次の例を参考にしてください。

(&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:1.2.840.113556.1.4.803:=2))(telephonenumber=919*))

このフィルタでは、電話番号フィールドのプレフィックスが 919 であるユーザだけが選択されます。同期アグリーメントによって、エリア コード 919 を持つユーザだけがインポートされます。この例では、すべてのエントリがエリア コードで開始されることを想定しています。

サーチ フィルタに対して、既存の任意の属性を使用できます。または、LDAP ディレクトリ ストアで定義したカスタム属性を使用することもできます。フィルタ ストリングでは、LDAP サーバによって選択され、Unified CM に返されるレコードが制御されますが、インポートされる属性は、フィルタ ストリングの影響を受けません。LDAP 照会用に Unified CM で使用されるフィルタ ストリングは、ldapfilter データベース テーブルの内部に格納されます。このストリングの最大長は 1024 文字です。Unified CM では、各 LDAP ディレクトリ同期アグリーメント用のカスタム フィルタをサポートできます。

ハイ アベイラビリティ

Unified CM LDAP 同期を使用すると、ディレクトリ同期アグリーメントごとに最大 3 つの冗長 LDAP サーバを設定できます。Unified CM LDAP 認証を使用すると、認証アグリーメントごとに最大 3 つの冗長 LDAP サーバを設定できます。冗長性を確保するには、最低限 2 つの LDAP サーバを設定する必要があります。これらの LDAP サーバでは、ホスト名の代わりに IP アドレスを設定することで、Domain Name System（DNS; ドメイン ネーム システム）の可用性への依存を排除できます。

Unified CM データベース同期のキャパシティ プランニング

Unified CM データベース同期機能には、LDAP ストアから Unified CM パブリッシャ データベースへユーザ設定データ（属性）のサブセットをインポートするメカニズムがあります。ユーザ アカウントの同期が発生すると、各ユーザの LDAP アカウント情報が、そのユーザの特定の Unified Communications 機能を有効にするために必要な追加データと関連付けられることがあります。認証も有効な場合、パスワード確認のための LDAP ストアへのバインドに、ユーザのクレデンシャルを使用します。同期や認証が有効な場合に、エンド ユーザのパスワードは Unified CM データベースには格納されません。

ユーザ アカウント情報はクラスタ固有です。各 Unified CM パブリッシャ サーバは、このクラスタから Unified Communications サービスを受けているユーザの一意のリストを保持しています。同期アグリーメントはクラスタ固有で、各パブリッシャにはユーザ アカウント情報の独自コピーがあります。

Unified CM データベースは、設定された、または同期された最大 60,000 のユーザ アカウントをサポートします。ディレクトリ同期のパフォーマンスを最適化するには、次の点を考慮してください。

- 電話機や Web ページからのディレクトリ ルックアップには、Unified CM データベースまたは IP Phone Service SDK を使用できる。ディレクトリ ルックアップ機能に Unified CM データベースを使用する場合、LDAP ストアから設定された、または同期されたユーザだけがディレクトリに表示されます。ユーザのサブセットを同期すると、ユーザのそのサブセットだけがディレクトリ ルックアップに表示されます。
- ディレクトリ ルックアップに IP Phone Services SDK を使用する場合に、LDAP に対する Unified CM ユーザの認証が不要であれば、Unified CM クラスタにログインするユーザのサブセットだけに同期を制限できます。
- クラスタが 1 つだけであり、LDAP ストア内のユーザ数が 60,000 未満である場合、Unified CM データベースにディレクトリ ルックアップを実装するには、LDAP ディレクトリ全体をインポートできます。

- 複数のクラスタが存在し、LDAP 内のユーザ数が 60,000 未満である場合、すべてのユーザをすべてのクラスタにインポートすることで、すべてのエントリがディレクトリ ルックアップに確実に含まれるようにできます。
- LDAP 内のユーザ アカウント数が 60,000 を超えており、ユーザ セット全体をすべてのユーザに表示する必要がある場合には、Unified IP Phone Services SDK を使用して Unified CM からディレクトリ ルックアップをオフロードする必要がある。
- 同期と認証の両方を有効にすると、Unified CM データベースに設定または同期されたユーザ アカウントはそのクラスタにログインできるようになる。同期するユーザの決定は、ディレクトリ ルックアップ サポートの決定に影響します。

（注） シスコでは、クラスタごとに最大 60,000 のユーザ アカウントの同期をサポートしていますが、この制限を強制していません。60,000 を超えるユーザ アカウントを同期化すると、ディスク容量のスターベージョン、データベース パフォーマンスの低速化、およびアップグレードの長時間化を招くことがあります。

CHAPTER 17

メディア リソース

メディア リソースとは、ソフトウェア ベースまたはハードウェア ベースのエンティティであり、接続中のデータ ストリームに対してメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能（会議）、ある接続から別の接続（メディア ターミネーション ポイント）にストリームを渡す機能、ある圧縮タイプから別の圧縮タイプにデータ ストリームを変換する機能（トランスコーディング）、発信者へのストリーム化された音楽の提供（保留音）、エコー キャンセレーション、シグナリング、TDM 回線からの音声ストリームの終端（コーディング/デコーディング）、ストリームのパケット化、オーディオのストリーミング（Annunciator）などが含まれます。

この章を使用して、次で説明するメディア リソースのうち、配置に必要なものがあるか判断してください。また、必要なリソースがソフトウェアベースの機能により提供されるか、またはリソースの実装に Digital Signal Processor（DSP; デジタル シグナル プロセッサ）のプロビジョニングが必要かどうかも判断してください。リソースについては個別の項で説明しますが、上位機能を実装するために、同じ基本リソース（DSP と Cisco IP Voice Media Streaming Application）が共有されることがあります。

この章では、次の機能を中心に説明します。

Cisco Unified Communications Manager（Unified CM）のメディア リソースは、メディア リソース グループおよびメディア リソース グループ リストを使用して制御できます。リソースのプールを作成すると、使用する特定のハードウェアまたはソフトウェアを制御できます。プールを使用して、物理的な場所に基づいてリソースをグループ化することを推奨します。さまざまなコール処理モデルをベースにした設計ガイドラインについては、「メディア リソースのハイ アベイラビリティ」（P.17-38）および「メディア リソースの設計に関する留意点」（P.17-40）を参照してください。

この章の新規情報

表 17-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 17-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 6 月 30 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）の機能	この章の各項で説明	2011 年 2 月 28 日
Cisco ISR ゲートウェイおよびレガシー プラットフォームの DSP サイジングのための DSP 計算ツール	この章の各項で説明	2011 年 2 月 28 日
DSP ハードウェアおよび Cisco IOS リリース バージョンへの更新	この章の各項で説明	2011 年 2 月 28 日
Music on Hold（MoH; 保留音）情報がこの章に統合され、別の MoH に関する章がこのマニュアルから削除されました。	この章の各項で説明	2010 年 11 月 15 日
Cisco Integrated Services Routers Generation 2（ISR G2; サービス統合型ルータ第 2 世代）プラットフォーム	この章の各項で説明	2010 年 4 月 2 日
PVDM3 DSP	この章の各項で説明	2010 年 4 月 2 日

メディア リソースのアーキテクチャ

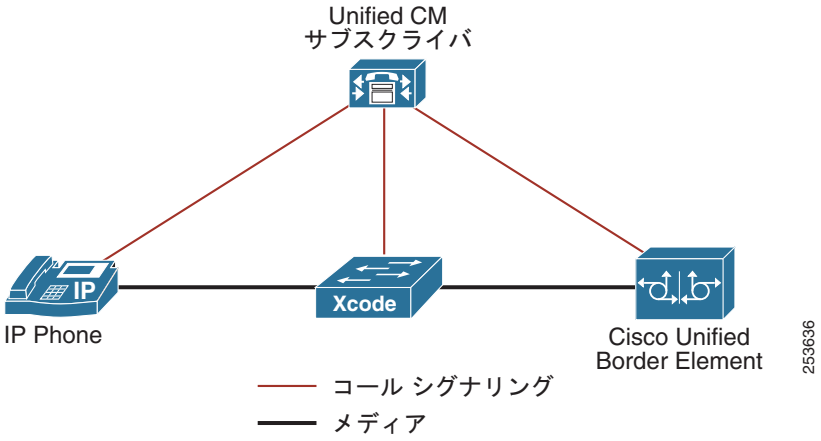
会社のメディア リソース割り当て方針を適切に策定するには、さまざまなメディア リソースコンポーネントの Cisco Unified CM アーキテクチャを理解しておくことが重要です。次の各項では、Unified CM を使用したメディア リソース設計の重要な特徴を中心に説明します。

メディア リソース マネージャ

Unified CM のソフトウェア コンポーネントである Media Resource Manager（MRM; メディア リソース マネージャ）は、メディア リソースの割り当ておよびメディア パスの挿入が必要であるかどうかを判別します。MRM は、メディア リソースのタイプを判別および特定すると、当該デバイスに関連付けられている Media Resource Group List（MRGL; メディア リソース グループ リスト）および Media Resource Group（MRG; メディア リソース グループ）の構成の設定値に応じて、使用可能なリソース全体を検索します。MRGL および MRG は、割り当てを行うためにメディア リソースの関連するグループをまとめて保持する構成概念です。詳細については、「メディア リソース グループとメディア リソース グループ リスト」（P.17-38）の項を参照してください。

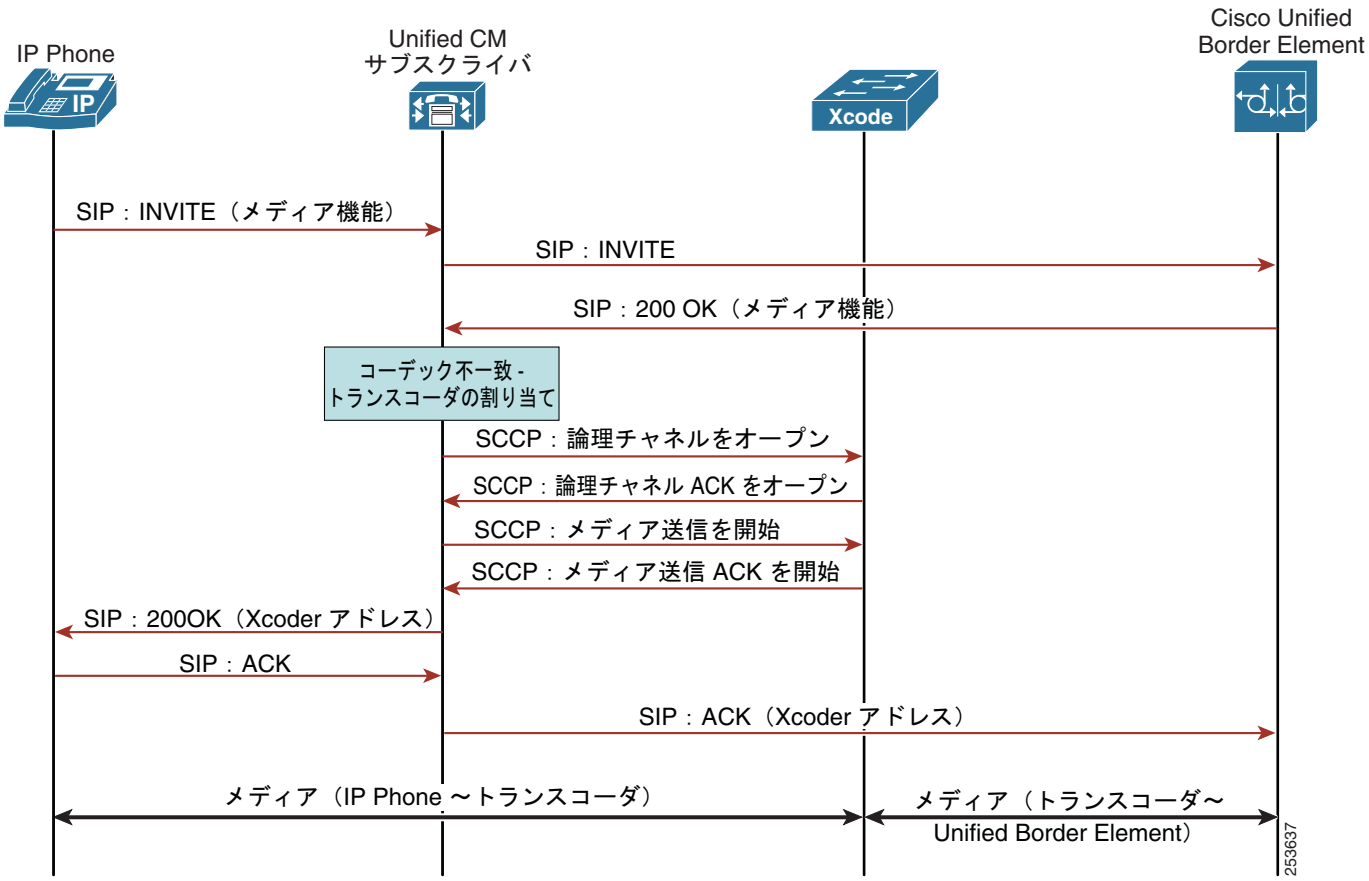
図 17-1 は、IP 電話と Cisco Unified Border Element 間で一般的なコーデックが使用できない場合に、トランスコーダなどのメディア リソースが、これらの間のメディア パスにどのように配置されるかを示しています。

図 17-1　一般的なコーデックが使用できない場合のトランスコーダの使用



Unified CM は、Skinny Client Control Protocol（SCCP）を使用して、メディア リソースと通信します。このメッセージングは、Unified CM と通信エンティティ間で使用されている可能性のあるプロトコルに依存しません。図 17-2 にメッセージ フローの例を示します。ただし、この例は、エンティティ間で交換されるすべての SCCP メッセージおよび SIP メッセージを示しているわけではありません。

図 17-2　コンポーネント間のメッセージ フロー



Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアに次のリソースを組み込みます。

- Music On Hold（MoH; 保留音）
- Annunciator
- ソフトウェア カンファレンス ブリッジ
- Media Termination Point（MTP; メディア ターミネーション ポイント）

Media Streaming Application をアクティブにすると、上記の各リソースが 1 つずつ自動的に設定されます。Annunciator、ソフトウェア カンファレンス ブリッジ、または MTP が必要ない場合は、Cisco IP Voice Media Streaming Application の Run Flag サービス パラメータを無効にして、これらのリソースを無効にすることを推奨します。

複数のリソースが必要になる状況や、それらのリソースによって Media Streaming Application にかかる負荷を慎重に検討してください。各リソースには、処理可能な接続の最大数を制御するサービス パラメータと、関連付けられたデフォルト設定があります。デフォルト設定を変更しない限り、制限付きで 4 つのリソースすべてを同じサーバ上で実行できます。ただし、配置においてデフォルトを超える数のリソースが 1 つでも必要になった場合は、そのリソースを独自の専用サーバ上で実行するように設定します（そのサーバ上では、その他すべてのリソースおよび Cisco CallManager Service を実行しないでください）。

Annunciator は、IP Voice Media Streaming Application でのみ使用できる唯一のメディア リソースです。会議、MTP、および Music On Hold（MoH; 保留音）はすべて、Unified CM サーバ以外のサーバ上に配置できます。Unified CM では MTP および会議リソースを無効にして、これらの機能には外部の専用リソースを用意することを推奨します。

また、IP Voice Media Streaming Application は、コール処理を担当するパブリッシャ、または任意の Unified CM サーバとは異なるサーバ上で実行することを強く推奨します。メディア リソースのために CPU 負荷が増加すると、コール処理のパフォーマンスに悪影響が発生する可能性があります。User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックは、Unified CM サーバ上で受信されなければならないので、セキュリティ上の問題が発生するおそれがあります。

（注）　Cisco Unified Communications Manager Business Edition（CMBE）3000 では、MoH および Annunciator 以外のソフトウェア メディア リソースは、サーバ上にプロビジョニングされません。ハードウェア リソースは、Cisco Integrated Services Router（ISR; サービス統合型ルータ）2901 から使用されます。

メディア リソースとしての保留音

Music On Hold（MoH; 保留音）機能には、2 つの重要な要件があります。

- MoH オーディオ ストリーム ソースを流す MoH サーバ（「MoH オーディオ ソース」（P.17-44）を参照）
- 通話を保留にするときに、MoH サーバが流す MoH ストリームを使用するように設定された Unified CM

MoH 機能は、Unified CM Administration インターフェイスを介して設定できます。エンド デバイスまたは機能が通話を保留にすると、Unified CM は、その保留デバイスを MoH メディア リソースに接続します。基本的に、Unified CM は、MoH サーバとの接続を確立するように、エンド デバイスに指示します。保留にされたデバイスが復帰すると、そのデバイスは MoH リソースから切り離され、通常のアクティビティを再開します。

音声インターフェイス

音声インターフェイスは、Time-Division Multiplexing（TDM; 時分割多重）インターフェイス上のレッグと VoIP（Voice over IP）接続上のレッグの 2 つのコール レッグを持つコールに適用されます。TDM レッグは、コーディング/デコーディングとストリームのパケット化を実行するハードウェアで必ず終端します。この終端機能は、同じハードウェア モジュール、ブレード、またはプラットフォーム上にあるデジタル シグナル プロセッサ（DSP）リソースによって実行されます。

Cisco TDM ゲートウェイ上の DSP ハードウェアはすべて、音声ストリームを終端できます。また、特定のハードウェアは、会議やトランスコーディングなどの他のメディア リソース機能を実行することもできます（「会議」（P.17-7）および「トランスコーディング」（P.17-12）を参照）。DSP ハードウェアには、アップグレードおよび変更ができない固定 DSP リソース、またはアップグレード可能なモジュラ DSP リソースのどちらかが搭載されています。

サポートされるコールの数は、コールに使用されるコーデックの計算の複雑度や、DSP に設定された複雑度モードによって異なります。Cisco IOS を使用すると、ハードウェア モジュールの複雑度モードを設定できます。PVDM2 や PVDM3 DSP のようなハードウェア プラットフォームは、3 つの複雑度モード（中複雑度モード、高複雑度モード、フレックス モード）をサポートします。他のハードウェア プラットフォームには、中複雑度モードと高複雑度モードのみをサポートするものもあります。

中複雑度モードと高複雑度モード

各 DSP は、中複雑度モード、高複雑度モード、またはフレックス モード（PVDM3 DSP および C5510 に基づく DSP）のいずれかとして個別に設定できます。DSP は、コールのコーデックに関する実際の複雑度に関係なく、設定されている複雑度に応じてすべてのコールを処理します。着信コールの実際の複雑度と同じかそれ以上の複雑度が設定されたリソースが使用可能になっている必要があります。そうでない場合、コールは失敗します。たとえば、コールに高複雑度コーデックが必要な場合、DSP リソースが中複雑度モードに設定されていると、コールは失敗します。ただし、高複雑度モードに設定された DSP に対して中複雑度コールが試行された場合、コールは成功し、Cisco IOS は高複雑度モードのリソースを割り当てます。

フレックス モード

フレックス モードは、C5510 チップセットを使用するハードウェア プラットフォーム上、および PVDM3 DSP 上だけで使用可能であり、このモードでは、設定時にコーデックの複雑度を指定する必要がありません。フレックス モードの DSP は、処理能力が足りる限り、サポートされているすべてのコーデック タイプのコールを受け入れます。

C5510 ベースの DSP の場合は、Millions of Instructions Per Second（MIPS）単位の処理能力を計算することで動的にトラッキングされます。Cisco IOS は、受信されたコールごとに MIPS の計算を実行し、新しいコールが開始されるたびにそのバジェットから MIPS クレジットを差し引きます。コールで消費される MIPS 数は、コールのコーデックによって異なります。着信コールに必要な MIPS 以上の MIPS クレジットが残っている限り、DSP は新しいコールを許可します。

同様に、PVDM3 DSP モジュールでは、クレジットベースのシステムを使用します。各モジュールには、メディア ストリームを処理するモジュールのキャパシティの単位を表す固定数の「クレジット」が割り当てられています。音声インターフェイス、トランスコーディングなどの各メディア動作には、クレジットによるコストが割り当てられています。DSP リソースはメディア処理用に割り当てられているため、そのコスト値は、使用可能なクレジットから差し引かれます。使用可能なクレジットが使い果たされると、DSP モジュールのキャパシティがなくなり、要求された操作に対応できなくなります。PVDM3 DSP のクレジット割り当て規則は、より複雑です。

Cisco ISR ゲートウェイの適切な DSP のサイジングを行うために、Cisco Unified Communications Sizing Tool（Unified CST）を使用できます。このツールはシスコの従業員および代理店が http://tools.cisco.com/cucst から入手できます。シスコ代理店でない場合は、http://www.cisco.com/go/dspcalculator から DSP Calculator を使用できます。他のシスコの非 ISR ゲートウェイ プラットフォーム（Cisco 1700、2600、3700、AS5000 シリーズなど）や Cisco IOS の 12.4 以前の主要なリリースについては、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl からレガシーの DSP Calculator にアクセスできます。

フレックス モードは、同じハードウェアで複数のコーデックのコールをサポートする必要がある場合に便利です。これは、フレックス モードでは、DSP が中複雑度または高複雑度として設定されている場合よりも多くのコールをサポートできるためです。ただし、フレックス モードではリソースのオーバーサブスクリプションが許可されています。オーバーサブスクリプションになると、すべてのリソースが使用された場合にコール障害が発生するリスクが生じます。フレックス モードを使用すると、物理 TDM インターフェイスを使用する場合よりも DSP リソースの数を削減できます。

中複雑度モードまたは高複雑度モードと比べると、フレックス モードには、DSP ごとに最も多くの G.711 コールをサポートできるという利点があります。たとえば、PVDM2-16 DSP は、中複雑度モードで 8 つの G.711 コールを、またはフレックス モードで 16 の G.711 コールをサポートできます。

会議

カンファレンス ブリッジとは、複数の参加者を 1 つのコールに参加させるリソースです。そのデバイス上で 1 つの会議に許可される最大ストリーム数まで、所定の会議用に任意の数の接続を受け入れることができます。会議に接続されているメディア ストリームと、その会議に接続されている参加者との間には、1 対 1 の対応があります。カンファレンス ブリッジは、ストリームを混合し、接続されている通話者ごとに一意の出力ストリームを作成します。所定の通話者の出力ストリームは、接続されている全通話者からのストリームの合成から、当事者の入力ストリームを除いたものです。一部のカンファレンス ブリッジは、会議で通話量が最も多い 3 名の通話者だけを混合し、その合成ストリーム（通話量が最も多い通話者の 1 人である場合は、当事者の入力ストリームをマイナスしたもの）を各参加者に配信します。

オーディオ会議

ハードウェア カンファレンス ブリッジは、ソフトウェア カンファレンス ブリッジのすべての機能を備えています。さらに、一部のハードウェア カンファレンス ブリッジは、G.729 や G.723 などの複数の Low Bit-Rate（LBR; 低ビット レート）ストリーム タイプをサポートできます。この機能により、一部のハードウェア カンファレンス ブリッジが混合モードの会議を処理できるようになります。混合モードの会議では、ハードウェア カンファレンス ブリッジは、G.729 および G.723 のストリームを G.711 ストリームにトランスコードし、混合します。その後、混合したストリームを、ユーザに戻すために適切なストリーム タイプにエンコードします。G.711 会議しかサポートしないハードウェア カンファレンス ブリッジもあります。

Unified CM の制御下にあるすべてのカンファレンス ブリッジは、Unified CM との通信に Skinny Client Control Protocol（SCCP）を使用します。

Unified CM は、Unified CM クラスタに登録されている会議リソースから、カンファレンス ブリッジを割り当てます。ハードウェアとソフトウェアの両方の会議リソースを同時に Unified CM に登録でき、Unified CM は、どちらのリソースからでも、カンファレンス ブリッジを割り当て、使用できます。Unified CM は、会議割り当て要求を処理するときに、これらのカンファレンス ブリッジのタイプを区別しません。

リソースがサポートできる会議の数、および 1 つの会議の最大参加者数は、リソースによって異なります。

Unified CM システムでは、次のタイプのカンファレンス ブリッジ リソースが使用されます。

- 「ソフトウェア オーディオ カンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）」（P.17-8）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、PVDM2、および PVDM3 DSP）」（P.17-8）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）」（P.17-9）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）」（P.17-9）
- 「ハードウェア オーディオ カンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）」（P.17-10）
- 「組み込み会議」（P.17-10）

ソフトウェア オーディオ カンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）

ソフトウェア ユニキャスト カンファレンス ブリッジは、G.711 音声ストリームと Cisco Wideband オーディオ ストリームを混合できる標準の会議ミキサーです。Wideband または G.711 a-law および mu-law ストリームの任意の組み合せが、同じ会議に接続される場合があります。所定の設定でサポートできる会議数は、カンファレンス ブリッジ ソフトウェアが実行されるサーバと、アプリケーションで有効になっている他の機能によって決まります。Cisco IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ではすべての機能を同時に考慮する必要があります（「Cisco IP Voice Media Streaming Application」（P.17-4）を参照）。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、PVDM2、および PVDM3 DSP）

Cisco IOS で会議リソースとして設定されている DSP は、会議機能のみに特化した DSP にファームウェアをロードします。このような DSP は、他のメディア機能には使用できません。

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- C5510 DSP チップセットに基づき、NM-HDV2 およびルータ シャーシは PVDM2 モジュールを使用して DSP を提供します。
- NM-HDV2 などの PVDM2 ベースまたは PVDM3 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。
- PVDM2 ハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つの PVDM の複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててから、必要に応じて他の機能に割り当ててください。
- NM-HDV2 には、任意の組み合せで PVDM2 モジュールを取り付け可能な 4 つのスロットがあります。その他のネットワーク モジュールの DSP 数は固定されています。
- Cisco IOS Release 12.4(15)T から、参加者数の上限は 32 に増えました。これらの DSP に基づく会議には、最大 8、16、または 32 人が参加できるように設定できます。会議用の DSP リソースは、プロファイル属性に基づいて、実際の参加者数に関係なく、設定の間予約されています。
- これらの DSP に基づく会議には、最大 8 人が参加できます。会議が始まるときに、8 つのポジションのすべてが予約されます。Cisco IOS Release 12.4(15)T から、この参加者数の上限は 32 に増えました。
- PVDM2-16 は、単一の DSP があるものとして表示されています。PVDM2-8 には、PVDM2-16 と比較して処理キャパシティが半分の DSP があるため、½ DSP と表示されています。たとえば、PVDM2-8 の DSP が G.711 用に設定されている場合、(0.5 * 8) ブリッジ/DSP = 4 カンファレンス ブリッジを提供できます。
- 各 DSP タイプによってサポートされる会議の数は、各会議の参加者数とその会議で使用されるコーデックの機能に依存します。各メディア処理機能（DSP によってホストされる会議を含む）では、使用可能な一部のクレジットを消費します。特定の会議で消費されるクレジット数は、参加者数とその会議で使用されるコーデックに依存します。Cisco IOS の DSP ファーム設定によって、ファームで受け付けることができるコーデックを指定します。G.711 コールのみを受け付ける dspfarm 設定を使用する 1 つの DSP（PVDM2-16）で、それぞれ最大 8 人が参加できる、8 つの会議が提供されます。G.711 コールと G.729 コールの両方を受け付けるように設定されている場合、ストリームのトランスコーディング用にもリソースが予約されるため、1 つの DSP で 2 つの会議が提供されます。

- NM-HDV2 の I/O は 400 ストリームに制限されています。そのため、割り当てられている会議リソースの数がこの制限を超えないように注意してください。G.711 会議が設定されている場合、（48 * 8）参加者 = 384 ストリームになるため、1 つの NM に割り当てることができる DSP は 6（参加者がそれぞれ 8 人の合計 48 の会議）までです。すべての会議を G.711 コーデックと G.729 コーデックの両方に設定した場合、各 DSP は、参加者がそれぞれ 8 人の会議を 2 つだけ提供します。この場合、NM に搭載できる最大 16 の DSP が設定されると、256 ストリームが可能になります。

（注）　Cisco Unified CMBE 3000 では、デフォルト ゲートウェイ設定は、PVDM3-128 ごとに 3 つの会議のみをサポートします。

Cisco ISR ゲートウェイの適切な DSP のサイジングを行うために、Cisco Unified Communications Sizing Tool（Unified CST）を使用できます。このツールはシスコの従業員および代理店が http://tools.cisco.com/cucst から入手できます。シスコ代理店でない場合は、http://www.cisco.com/go/dspcalculator から DSP Calculator を使用できます。他のシスコの非 ISR ゲートウェイ プラットフォーム（Cisco 1700、2600、3700、AS5000 シリーズなど）や Cisco IOS の 12.4 以前の主要なリリースについては、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl からレガシーの DSP Calculator にアクセスできます。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つのモジュールの複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててください。
- 各 ACT ポート アダプタには、個別に設定可能な 4 つの DSP が含まれています。各 DSP は、32 人の会議参加者をサポートします。CMM モジュールごとに最大 4 つの ACT ポート アダプタを設定できます。
- この Cisco Catalyst ベースのハードウェアには、ブリッジごとに 128 人まで参加できるカンファレンス ブリッジを提供できる DSP リソースが用意されています。1 つのカンファレンス ブリッジが単一の ACT ポート アダプタ上にある複数の DSP にまたがることはできますが、カンファレンス ブリッジが複数の ACT ポート アダプタにまたがることはできません。
- これらのカンファレンス ブリッジでは、追加のトランスコーダ リソースなしで、G.711 コーデックおよび G.729 コーデックがサポートされます。ただし、その他のコーデックを使用する場合は、トランスコーダ リソースが必要になることがあります。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。
- このハードウェアを使用する会議は、1 つのブリッジで 6 人まで参加可能なブリッジを提供します。
- リソースは DSP ごとにカンファレンス ブリッジとして設定されます。
- NM-HDV は 5 つまでの PVDM-256K モジュールを使用でき、Cisco 1700 シリーズ ルータは、1 つまたは 2 つの PVDM-256K モジュールを使用できます。
- 各 DSP は、G.711 コールまたは G.729 コールを受け付け可能な 1 つのカンファレンス ブリッジを提供します。

- Cisco 1751 は、シャーシ 1 つで 5 つの電話会議に制限されています。Cisco 1760 は、シャーシごとに 20 の電話会議をサポートします。

（注）　NM-HDV2 などの PVDM2 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。

ハードウェア オーディオ カンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアには、物理的にそれぞれのポートに関連付けられた 8 つの DSP があり、カードごとに 8 つのポートがあります。DSP の設定はポート レベルで行われるため、1 つのポートに関連付けられているすべての DSP が同じ機能を実行します。
- カンファレンス ブリッジには最大 32 人が参加でき、各ポートが 32 のカンファレンス ブリッジをサポートします。
- G.711 または G.723 の会議では、ポートごとに 32 の会議が可能です。G.729 コールを使用する場合は、ポートごとに 24 の会議が可能です。

組み込み会議

一部の電話機モデルには、3 方向の会議を可能にする組み込み会議リソースが用意されています。このブリッジは、割り込み機能によってのみ呼び出され、通常の会議リソースとしては使用されません。このブリッジが用意されている電話機の詳細については、「Unified Communications エンドポイント」（P.18-1）を参照してください。このブリッジは、G.711 コールのみを受け付けます。

ビデオ会議

ビデオ対応エンドポイントには、オーディオ会議と同じように使用できるビデオ会議の機能があります。ビデオ会議は、SCCP デバイスから [Conf]、[Join]、または [cBarge] ソフトキーを使用して Ad-Hoc 会議として呼び出すことができます。

会議のビデオ部分は次の 2 つのモードで操作できます。

- Voice-Activated（音声起動）

  このモードでは、主要参加者（最後に発言した参加者または最も声の大きい参加者）がビデオ エンドポイントに表示されます。この方法では、ビデオ部分は音声部分に追随（または音声部分を追跡）します。このモードは、1 人の参加者がほとんどの時間発言し続けるような場合（講師による講習やグループ トレーニングなど）に最適です。

- Continuous-Presence（連続表示）

  このモードでは、すべての（または選択した）ビデオ エンドポイントが同時に継続して表示されます。会議の音声部分は主要発言者に追随（または主要発言者を追跡）します。Continuous-Presence はより一般的なモードで、さまざまなサイトの発言者間で会議や討論を行う場合に最適です。

ビデオ会議リソースには次の 2 種類があります。

- ソフトウェア ビデオ カンファレンス ブリッジ

  ソフトウェア ビデオ カンファレンス ブリッジは、ソフトウェアだけを使用して会議のビデオと音声を処理します。Cisco Unified MeetingPlace Express メディア サーバは、Ad Hoc ビデオ会議をサポートするソフトウェア ビデオ カンファレンス ブリッジです。Cisco Unified MeetingPlace Express メディア サーバでサポートされるのは、Voice-Activated モードのビデオ会議だけです。

- ハードウェア ビデオ カンファレンス ブリッジ

  ハードウェア ビデオ カンファレンス ブリッジには、ビデオ会議に使用されるハードウェア DSP が搭載されています。Cisco 3500 シリーズ Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）および Cisco IOS Release 15.1.4M 以降では PVDM3 DSP で、このタイプのビデオ カンファレンス ブリッジが提供されます。ほとんどのハードウェア ビデオ カンファレンス ブリッジは、音声専用のカンファレンス ブリッジとしても使用できます。ハードウェア ビデオ カンファレンス ブリッジには、ビデオ トランスレーティング、高いビデオ解像度、およびスケーラビリティといった利点があります。

ビデオ カンファレンス ブリッジには、オーディオ会議のリソースと同じように、デバイス プールまたはエンドポイント用の Media Resource Group（MRG; メディア リソース グループ）および Media Resource Group List（MRGL; メディア リソース グループ リスト）について同様の特性を設定できます。

Cisco Unified CM 7.*x* には、インテリジェント ブリッジ選択機能があります。この機能を使用すると、会議でビデオ エンドポイントを使用するか、またビデオ エンドポイントが利用できるかに基づいてビデオ会議リソースを割り当てることができます。会議にビデオ エンドポイントがない場合は、使用可能なオーディオ カンファレンス ブリッジが選択されます。この機能の詳細については、「インテリジェント ブリッジ選択機能」（P.12-21）を参照してください。

セキュア会議

セキュア会議は、通常の会議機能を使用して会議用メディアのセキュリティを確保し、メディアが危険にさらされないようにする手法です。これを実現するには、まずデバイスを認証してデバイスが信頼できることを確認し、同様に会議リソースも認証してから、会議メディアを暗号化します。これにより、会議のすべての参加者が認証され、その会議に関するメディアが暗号化されて送受信されます。この会議のセキュリティ レベルはさまざまです（承認レベルや暗号化レベルなど）。ほとんどの場合、会議のセキュリティ レベルは、会議の参加者の最低のセキュリティ レベルによって決まります。たとえば、ある 1 人の参加者がセキュアなエンドポイントを使用していない場合は、その会議全体が非セキュアになります。また、いずれかのエンドポイントが、認証はされているものの暗号化に対応していない場合には、その会議は認証モードになります。

セキュア会議には次の利点があります。

- 会議機能を高度なセキュリティ レベルで提供する。
- 会議コールの不正な捕捉や暗号解読を防ぐ。

セキュア会議を設計する際は、次の要素について検討してください。

- デバイス（電話機や会議リソース）のセキュリティ レベル
- コール シグナリングのセキュリティに関するオーバーヘッド
- SRTP メディアのセキュリティに関するオーバーヘッド
- 帯域幅に対する影響（セキュアな参加者が WAN 経由で参加する場合）
- NAT やファイアウォールなどの中間デバイスがセキュア コールの通過をサポートするかどうか

セキュア会議は、次の制約や制限を受ける場合があります。

- セキュア会議は、オーディオ会議に対してのみサポートされます。ビデオ会議はサポートされません。
- セキュア会議では、Cisco IOS DSP は 1 つの会議で最大 8 人の参加者をサポートします。
- セキュア会議は、非セキュア会議よりも多くの DSP リソースを使用する可能性があります。このような配置が必要な場合は、DSP をセキュア会議用に（DSP Calculator を使用して）適切にプロビジョニングする必要があります。
- コール シグナリングのセキュリティ保護について、一部のプロトコルが IPSec に依存する場合があります。
- セキュア会議は、Unified CM と Unified CM Express の間でカスケードできません。
- MTP とトランスコーダはセキュア コールをサポートしません。したがって、会議へ参加しているいずれかのコールで MTP またはトランスコーダが使用されている場合、その会議はセキュアにはなりません。
- 細かいセキュリティ ポリシーが必要となる場合があります。
- セキュア会議は、すべてのコーデックで使用できるとは限りません。
- TLS/SRTP を使用できないメンバーがセキュア会議に参加する場合、その会議全体が非セキュア モードに戻ります。

トランスコーディング

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。Cisco IOS Release 15.0.1M から、トランスコーダは、同じコーデックを異なるパケット サイズで利用する 2 つのストリームを接続するレート変換もサポートします。

G.711 から他のコーデックへのトランスコーディングは、従来のトランスコーディングと呼ばれます。2 つの非 G.711 コーデック間のトランスコーディングは、ユニバーサル トランスコーディングと呼ばれ、Universal Cisco IOS トランスコーダが必要です。ユニバーサル トランスコーディングは、Cisco IOS Release 12.4.20T および Cisco Unified Communications Manager Release 7.1.5 以降でサポートされます。ユニバーサル トランスコーディングは、従来のトランスコーディングよりも DSP の密度が低いです。

Unified CM システムでは、通常、G.711 音声ストリームと低ビットレート圧縮音声ストリームの G729a との間の変換を行うために、トランスコーダを使用します。次の場合には、どのようなときにトランスコーダ リソースが必要かが決まります。

- システム全体で単一のコーデックが使用されている。

  システムのすべてのコールに対して単一のコーデックが設定されている場合、トランスコーダ リソースは必要ありません。G.711 コーデックは、すべてのベンダーでサポートされています。単一サイトの配置では、通常、帯域幅を節約する必要がなく、単一のコーデックを使用できます。このシナリオで最も一般的に選択されるのは G.711 です。

- システムで複数のコーデックが使用され、すべてのエンドポイントがすべてのコーデック タイプに対応している。

  複数のコーデックを使用する最も一般的な理由は、LAN コールには G.711 を使用してコール品質を最大にし、帯域幅が制限されている WAN を通過するコールには低帯域幅コーデックを使用して帯域幅効率を最大にするためです。低帯域幅コーデックには、G.729a を使用することを推奨します。G.729a は、すべての Cisco Unified IP Phone モデル、およびその他のほとんどの Cisco Unified Communications デバイスでサポートされるため、トランスコーディングの必要がなくなります。Unified CM では、リージョン間でその他の低帯域幅コーデックも設定できますが、

一部の電話機モデルはこのコーデックをサポートしないため、トランスコーダが必要になります。ゲートウェイへのコールには 1 つのトランスコーダが必要で、別の IP Phone へのコールには 2 つのトランスコーダが必要です。すべてのデバイスが G.711 と G.729 の両方をサポートし、両方で設定されている場合は、デバイスがコールごとに適切なコーデックを使用するため、トランスコーダを使用する必要はありません。

- システムで複数のコーデックが使用され、一部のエンドポイントが G.711 だけをサポートしているか、または G.711 だけを使用するように設定されている。

  この条件は、システムで G.729a を使用し、このコーデックをサポートしないデバイスがある場合、または G.729a をサポートするデバイスが G.729a を使用するように設定されていない場合に発生します。この場合はトランスコーダが必要です。サードパーティ ベンダーのデバイスは、G.729 をサポートしない場合があります。また、G.729 をサポートしていても、Cisco Unity で設定されていないということもあります。Cisco Unity は G.729a でのコールの受け付けをサポートしますが、コーデックはソフトウェアで実装され、CPU に負荷がかかります。同時に 10 のコールが発生するだけで CPU 使用率が高くなるため、多くの配置では Cisco Unity で G.729 を無効にして、Unity サーバの外にある専用のトランスコーディング リソースにトランスコーディング機能の負荷を分散します。システムに Cisco Unity が含まれている場合は、Unity で G.729a コールを受け付けるか、または G.711 だけを使用するように設定するかを決定します。

（注） Release 2.0 以前の Cisco Unified MeetingPlace Express は、G.711 だけをサポートしています。以前のバージョンの Cisco Unified MeetingPlace Express へのコールに対して G.729 が設定されている環境では、トランスコーダ リソースが必要です。

設計を最終決定するには、必要なトランスコーダの数と、トランスコーダを配置する場所を検討する必要があります。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。

トランスコーディング リソース

トランスコーディングを実行するには、DSP リソースが必要です。これらの DSP リソースは、音声モジュール、および次の項で示すトランスコーディング用のハードウェア プラットフォームに配置できます。

ハードウェア トランスコーダ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、および PVDM2 DSP）

DSP ごとにサポートされるセッション数は、ユニバーサル トランスコーディング モードで使用されるコーデックによって決定されます。これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729ab、G.722、および iLBC との間で使用できます。1 つの DSP（PVDM2-16）では、低複雑度コーデックと中複雑度コーデック間（G.711 と G.729a または G.722 など）のトランスコーディングに 8 セッション、または低複雑度コーデックと高複雑度コーデック間（G.711 と G.729 または iLBC など）のトランスコーディングに 6 セッションをサポートできます。

（注）　G.711 と G.722 との間にトランスコーディングが必要ない場合は、Cisco IOS の dspfarm profile 設定に G.722 を入れないことを推奨します。これは、Unified CM が、トランスコーディングを必要とするコールのコーデックとして G.722 を選択しないようにするためです。G.722 と他のコーデック間のトランスコーディングでは、ユニバーサル トランスコーダーとして設定された DSP リソースが必要です。

- Cisco Unified IP Phone は、G.729 コーデックの G.729a バリアントだけを使用します。新規 DSP ファーム プロファイルのデフォルトは、G.729a/G.729ab/G.711u/G.711a です。単一の DSP が同時に提供できる機能は 1 つだけなので、プロファイルで設定する最大セッション数は、リソースを無駄にしないように、8 の倍数で指定する必要があります。

Cisco ISR ゲートウェイの適切な DSP のサイジングを行うために、Cisco Unified Communications Sizing Tool（Unified CST）を使用できます。このツールはシスコの従業員および代理店が http://tools.cisco.com/cucst から入手できます。シスコ代理店でない場合は、http://www.cisco.com/go/dspcalculator から DSP Calculator を使用できます。旧来のシスコの非 ISR ゲートウェイ プラットフォーム（Cisco 1700、2600、3700、AS5000 シリーズなど）や Cisco IOS の 12.4 以前の主要なリリースについては、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl からレガシーの DSP Calculator にアクセスできます。

ハードウェア トランスコーダ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729b、または G.723 との間で使用できます。
- 1 つの ACT ごとに、個別に DSP プールに割り当て可能な 4 つの DSP があります。
- CCM-ACT は、DSP ごとに 16（ACT ごとに 64）のトランスコーディングされたコールをサポートします。ACT は、リソースをコールではなくストリームとしてレポートします。単一のトランスコーディングされたコールは、2 つのストリームで構成されます。

ハードウェア トランスコーダ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。

- NM-HDV は、4 つまでの PVDM-256K モジュールを使用できます。Cisco 1700 シリーズ ルータは、1 ～ 2 の PVDM-256K モジュールを使用できます。
- NM-HDV モジュールと NM-HDV2 モジュールは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。会議、MTP、またはトランスコーディングに対して同時にアクティブにできる DSP ファームのタイプは 1 つだけです（NM-HDV または HM-HDV2）。
- G.711 mu-law または a-law から G.729、G.729a、G.729b、または G.729ab コーデックへのトランスコーディングがサポートされます。
- 1 つの DSP で 2 つのトランスコーディング セッションを提供できます。
- Cisco 1751 のシャーシは 16 セッションに制限されています。Cisco 1760 のシャーシは 20 セッションに制限されています。

ハードウェア トランスコーダ（Cisco WS-X6608）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- DSP はポート レベルで機能に割り当てられます。1 つのポートで 24 のトランスコーディング セッションを提供できます。
- ブレードごとに 8 つのポートがあります。
- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729ab、G.729、または G.729b との間で使用できます。

トランスコーダは、Media Termination Point（MTP; メディア ターミネーション ポイント）と同じ機能も実行できます。トランスコーダ機能と MTP 機能の両方が必要な場合、トランスコーダがシステムによって割り当てられます。MTP 機能が必要な場合、Unified CM はトランスコーダまたは MTP をリソース プールから割り当てます。リソースの選択はメディア リソース グループによって決まります（「メディア リソース グループとメディア リソース グループ リスト」（P.17-38）の項を参照）。

ハードウェア トランスコーダ（PVDM3 DSP）

PVDM3 DSP は、Cisco 2900 シリーズおよび 3900 シリーズのサービス統合型ルータによってホストされており、任意のコーデックとのセキュアなトランスコーディングと非セキュア トランスコーディングの両方をサポートしています。音声インターフェイスおよび会議と同様に、各トランスコーディング セッションでは、各 PVDM3 DSP タイプの使用可能なクレジットが差し引かれます。使用可能なクレジットによって、DSP の合計キャパシティが決まります。

1 つの PVDM3-16 では、低複雑度コーデックと中複雑度コーデック間（G.711 と G.729a または G.722 など）のトランスコーディングに 12 セッション、または低複雑度コーデックと高複雑度コーデック間（G.711 と G.729 または iLBC など）のトランスコーディングに 10 セッションをサポートできます。

（注）　Cisco Unified CMBE 3000 では、デフォルト ゲートウェイ設定は、PVDM3-128 ごとに 10 のトランスコーディング セッションのみをサポートします。

Cisco ISR ゲートウェイの適切な DSP のサイジングを行うために、Cisco Unified Communications Sizing Tool（Unified CST）を使用できます。このツールはシスコの従業員および代理店が http://tools.cisco.com/cucst から入手できます。シスコ代理店でない場合は、http://www.cisco.com/go/dspcalculator から DSP Calculator を使用できます。旧来のシスコの非 ISR ゲートウェイ プラットフォーム（Cisco 1700、2600、3700、AS5000 シリーズなど）や Cisco IOS の 12.4 以前の主要なリリースについては、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl からレガシーの DSP Calculator にアクセスできます。

メディア ターミネーション ポイント（MTP）

Media Termination Point（MTP; メディア ターミネーション ポイント）は、2 つの全二重メディア ストリームを受け入れるエンティティです。MTP はこの 2 つのストリームをブリッジし、これらのストリームを個々にセットアップおよび終了できるようにします。ある接続の入力ストリームから受信されるストリーミング データは、他の接続の出力ストリームに渡され、逆も同様です。MTP には次のような多くの用途があります。

- 「ストリームの再パケット化」（P.17-16）
- 「DTMF 変換」（P.17-16）
- プロトコル固有の用途
  - 「SIP アーリー オファー」（P.17-18）
  - 「H.323 付加サービス」（P.17-20）
  - 「H.323 発信時の Fast Connect」（P.17-21）

ストリームの再パケット化

MTP は、G.711 a-law 音声パケットから G.711 mu-law パケット（およびその逆）にトランスコードしたり、パケット化周期が異なる（使用するサンプル サイズが異なる）2 つの接続をブリッジしたりできます。再パケット化するには、Cisco IOS MTP に DSP リソースが必要です。

DTMF 変換

コール中にメニュー システムのナビゲート、データの入力、またはその他の操作の目的で遠端のデバイスに信号を送信する際は、DTMF トーンが使用されます。これらは、呼制御の一部としてコール セットアップ中に送信される DTMF トーンとは異なる方法で処理されます。IP 上で DTMF を送信する方法はいくつかありますが、2 つの通信エンドポイントで共通の手順がサポートされていない場合があります。このような場合、Unified CM はメディア パスに動的に MTP を挿入して、DTMF 信号をエンドポイント間で変換できます。残念ながら、このようなコールには MTP リソースが 1 つずつ必要となるため、この方法は拡張性に欠けています。必要な MTP リソースの最適な量は、以降の項に従い、システム内のエンドポイント、トランク、およびゲートウェイの組み合せに基づいて判断してください。

MTP の挿入が必要であると判断された場合に使用可能な MTP リソースがないとき、Unified CM はサービス パラメータの「Fail call if MTP allocation fails」の設定に従って、そのコールを続行するかどうかを決定します。この設定のデフォルト値は False で、コールは続行されます。

Named Telephony Event（RFC 2833）

RFC 2833 で規定されている Named Telephony Event（NTE）は、コール メディアが確立された後で、あるエンドポイントから別のエンドポイントに DTMF を送信する方式です。トーンは、すでに確立されている RTP ストリームを使用して、パケット データとして送信されます。これらのトーンは、RTP ペイロード タイプ フィールドによってオーディオとは区別されます。たとえば、コールのオーディオをセッションで送信する際は、そのオーディオを G.711 データとして識別する RTP ペイロード タイプを使用できます。DTMF パケットの送信時には、そのパケットを NTE として識別する RTP ペイロード タイプが使用されます。ストリームの受信側は、G.711 パケットと NTE パケットを別々に利用します。

Key Press Markup Language（RFC 4730）

Key Press Markup Language（KPML）は RFC 4730 で規定されています。DTMF をインバンドで送信する NTE とは異なり、KPML はシグナリング チャネルを使用して（つまり、out-of-band（OOB; アウトオブバンド）で）、DTMF 番号を含む SIP メッセージを送信します。

KPML 手順では、DTMF 番号の登録に SIP SUBSCRIBE メッセージが使用されます。DTMF 番号自体は、XML で符号化された本体を含む NOTIFY メッセージで送信されます。

Unsolicited Notify（UN）

Unsolicited Notify 手順は、主に Cisco IOS SIP ゲートウェイにおいて、SIP NOTIFY メッセージを使用して DTMF 番号を転送するために使用されます。KPML とは異なり、これらの NOTIFY メッセージは非請求メッセージで、これらのメッセージを受信するために事前に SIP SUBSCRIBE メッセージで登録が行われることはありません。ただし、KPML と同様に、Unsolicited Notify メッセージもアウトオブバンドです。

また、KPML には XML で符号化されたメッセージ本体が含まれますが、Unsolicited Notify の NOTIFY メッセージの本体はそれとは異なり、DTMF イベントを表す 10 文字の符号化された数字、ボリューム、および継続時間です。

H.245 Signal、H.245 Alphanumeric

H.245 は、H.323 ネットワークで使用されるメディア制御プロトコルです。メディア特性のネゴシエートに使用されるほか、DTMF 転送用のチャネルも提供します。H.245 はシグナリング チャネルを利用するため、DTMF 番号はアウトオブバンド（OOB）で送信されます。Signal 方式は、Alphanumeric 方式よりも多くの DTMF イベント情報（DTMF イベントの実際の継続時間など）を伝送します。

シスコ独自の RTP

この方法は DTMF 番号をインバンドで（つまり、RTP パケットと同じストリームで）送信します。ただし、DTMF パケットはメディア パケットとは符号化方法が異なり、別のペイロード タイプが使用されます。この方法は Unified CM ではサポートされていませんが、Cisco IOS ゲートウェイではサポートされています。

Skinny Client Control Protocol（SCCP）

SCCP は、Unified CM により、Unified CM に登録されている SCCP ベースの各種デバイスを制御するために使用されます。SCCP は、Unified CM と制御デバイス間で DTMF 番号を転送するアウトオブバンド メッセージを定義します。

エンドポイント間の DTMF リレー

同じクラスタ内の Unified CM サーバに登録されたエンドポイントには、次の規則が適用されます。

- SIP 以外の 2 つのエンドポイント間のコールには、MTP は必要ありません。

  SIP 以外のすべての Cisco Unified Communications エンドポイントはさまざまなシグナリング パスによって DTMF を Unified CM に送信し、Unified CM は受け取った DTMF を異なるエンドポイント間で転送します。たとえば、IP Phone は Unified CM への SCCP メッセージを使用して DTMF を送信します。この DTMF は H.245 シグナリング イベントによって H.323 ゲートウェイに送信されます。Unified CM は、異なるシグナリング方式の間で DTMF を転送できます。

- 2 つの Cisco SIP エンドポイント間のコールには、MTP は必要ありません。

  Cisco SIP エンドポイントはすべて NTE をサポートしているため、DTMF はエンドポイント間で直接送信され、変換は不要です。すべてのエンドポイントが Cisco SIP デバイスの場合、DTMF を変換する MTP は必要ありません。

- SIP エンドポイントと SIP 以外のエンドポイントの組み合せの場合、MTP が必要になることがあります。

  ご使用のデバイスで NTE がサポートされるかどうかは、そのデバイスの製品マニュアルを参照してください。NTE のサポートは SIP に限定されていないため、その他の呼制御プロトコルを使用するデバイスでサポートされていることがあります。Unified CM は、エンドポイントのペアの機能に基づき、MTP をコール単位に動的に割り当てることができます。

SIP トランク

SIP トランク設定は、SIP ユーザ エージェント（別の Cisco Unified CM クラスタや SIP ゲートウェイなど）との通信をセットアップする際に使用されます。

SIP アーリー オファー

SIP は Session Description Protocol（SDP）によってメディア情報をネゴシエートします。これにより、一方が提示したメディア セットに他方が応答する形で、使用するメディアがある組み合せに決定します。SIP では、発信側が初期 INVITE メッセージ（アーリー オファー）によって初期オファーを送信するか、発信側がそうしなかった場合は着信側が最初の信頼性のある応答（ディレイド オファー）で初期オファーを送信できます。

デフォルトで、Unified CM SIP トランクは、初期オファー（ディレイド オファー）を伴わない INVITE を送信します。Unified CM には、SIP トランクが INVITE でオファー（アーリー オファー）を送信できるようにする 2 つの設定可能なオプションがあります。

- [Media Termination Point Required]

  SIP トランク上でこのオプションをオンにすると、すべての発信コールに対して 1 つの MTP が割り当てられます。静的に割り当てられるこの MTP は、G.711 コーデックまたは G.729 コーデックしかサポートしません。つまり、メディアが音声コールに限定されます。

- [Early Offer support for voice and video calls (insert MTP if needed)]

  SIP トランクに関連付けられた SIP プロファイル上でこのオプションをオンにすると、発信元のデバイスが Unified CM にアーリー オファーの作成に必要なメディア特性を提供できない場合（たとえば、Unified CM に対する着信コールがディレイド オファー SIP トランクまたは Slow Start H.323 トランク上で受信される場合）にのみ MTP が挿入されます。

通常、[Early Offer support for voice and video calls (insert MTP if needed)] 設定オプションは MTP の使用を抑えるため、このオプションの使用を推奨します。SIP アーリー オファー トランク経由で Unified CM に登録された旧式の SCCP 電話機からのコールでは、オファー SDP の作成に MTP が使用されます。このようなコールでは、音声、ビデオ、および暗号化がサポートされます。SIP アーリー オファー トランク経由で拡張された SIP アーリー オファー トランクまたは H.323 Slow Start トランクから Unified CM への着信コールでは、オファー SDP の作成に MTP が使用されます。ただし、このようなコールの初期コール セットアップでは音声しかサポートされませんが、着信側または発信側のデバイスがビデオ通話を呼び出した場合にそれをサポートするようにコールをエスカレーションできます。

また、INVITE メッセージに初期オファーが含まれているかどうかにかかわらず、着信 INVITE メッセージに MTP リソースは必須ではないことにも注意してください。

SIP トランク上の DTMF リレー

Unified CM で MTP が必要になるのは、2 つのエンドポイントの間で DTMF を送信する共通の方式がない場合、またはシステム設定で MTP を割り当てるように指定した場合です。

Unified CM によって MTP が割り当てられるかどうかは、両方の通信エンドポイントの機能と中間デバイスの設定（該当する場合）によって決まります。たとえば、SIP トランクでの DTMF 交換の処理について特定の方法（KPML を使用して DTMF を伝送する、NTE を使用するように通信エンドポイントに指示する、など）が設定されている場合があります。

SIP トランクの MTP に関する要件

デフォルトでは、SIP トランク パラメータの [Media Termination Point Required] と SIP プロファイル パラメータの [Early Offer support for voice and video calls (insert MTP if needed)] は選択されていません。

SIP トランクで MTP リソースが必要かどうかを判断するには、次の手順に従います。

1. この SIP トランクで定義されている対向の SIP デバイスが、SIP アーリー オファーを含まない着信コールを受け入れられるかどうかを確認します。

   そうでない場合は、このトランクに関連付けられた SIP プロファイル上で、[Early Offer support for voice and video calls (insert MTP if needed)] を有効にするボックスをオンにします。発信 SIP トランク コールでは、発信側デバイスが Unified CM にアーリー オファーの作成に必要なメディア特性を提供できない場合、または、DTMF 変換が必要な場合にのみ、MTP が挿入されます。

   そのとおりの場合は、[Early Offer support for voice and video calls (insert MTP if needed)] ボックスをオンにせず、ステップ 2. に進んで、MTP が DTMF 変換に対して動的に挿入されるかどうかを判断します。MTP による DTMF 変換は、どのコーデックを使用している場合でも実行できます。

   （注）「SIP アーリー オファー」（P.17-18）に記載されているように、アーリー オファーは、SIP トランク上で [Media Termination Point Required] オプションをオンにすることによっても有効にできます。ただし、このオプションでは、MTP が、必要に応じてではなく、すべての発信コールに対して割り当てられるため、MTP の使用が増大します。

2. トランクの DTMF Signaling Method を選択します。このパラメータは、そのトランクでの DTMF 選択の動作を制御します。すべてのコールについて、DTMF 方式を一致させるために、必要に応じて使用可能な MTP が割り当てられます。

   a. DTMF Signaling Method : No Preference

      このモードでは、Unified CM は、最も適切な DTMF シグナリング方式を選択することで、MTP の使用を最小限に抑えようとします。

      両方のエンドポイントが NTE をサポートしている場合は、MTP は必要ありません。

      両方のデバイスがいずれかのアウトオブバンド DTMF メカニズムをサポートしている場合、Unified CM は SIP トランク上で KPML を使用します。たとえば、上記のように設定された SIP トランク上で、SCCP を使用する Cisco Unified IP Phone 7936（SCCP メッセージングだけを使用して DTMF をサポートします）が、SIP を使用する Cisco Unified IP Phone 7970（NTE および KPML を使用して DTMF をサポートします）と通信する場合がこれに該当します。MTP が必要となる唯一のケースは、一方のエンドポイントがアウトオブバンドだけをサポートしていて、他方のエンドポイントが NTE だけをサポートしている場合です（たとえば、7936 SCCP 電話機と 7960 SIP 電話機が通信する場合）。

   b. DTMF Signaling Method : RFC 2833

      トランク全体の DTMF シグナリング方式を制限することにより、一方または両方のエンドポイントが NTE をサポートしていない場合に MTP を強制的に割り当てます。この設定では、MTP が割り当てられないのは、両方のエンドポイントが NTE をサポートしている場合だけです。

c. DTMF Signaling Method：OOB and RFC 2833

このモードでは、SIP トランクを通じて KPML と NTE ベースの両方の DTMF が送信されます。これは MTP の使用される可能性が最も高いモードです。MTP リソースが必要とされない唯一のケースは、両方のエンドポイントが NTE といずれかの OOB DTMF 方式（KPML または SCCP）の両方をサポートしている場合です。

（注）　Cisco IP Phone は、DTMF を SCCP 経由で受信した場合、エンド ユーザに対して DTMF を再生しますが、NTE で受信したトーンは再生しません。ただし、DTMF を別のエンド ユーザに送信する必要はありません。DTMF を必要とするエンドポイント（公衆網ゲートウェイ、アプリケーション サーバなど）と対応するコールを発信するエンドポイントについてのみ検討する必要があります。

SIP ゲートウェイおよび Cisco Unified Border Element での DTMF リレーの設定

Cisco SIP ゲートウェイは、その設定に応じて、DTMF メカニズムとして KPML、NTE、または Unsolicited Notify をサポートします。システムにはさまざまなエンドポイントが混在している場合があるため、複数の方式をゲートウェイに同時に設定することで、MTP の要件を最小限に抑えることができます。

Cisco SIP ゲートウェイでは、SIP ダイヤル ピアの DTMF リレー方式として、**sip-kpml** と **rtp-nte** の両方を設定します。このように設定すると、NTE だけをサポートするものや OOB 方式だけをサポートするものも含めて、すべてのタイプのエンドポイント間で MTP リソースなしに DTMF 交換を実現できます。この設定では、ゲートウェイは NTE と KPML の両方を Unified CM とネゴシエートします。Unified CM のエンドポイントで NTE がサポートされていない場合は、DTMF 交換に KPML が使用されます。両方の方式のネゴシエーションが成功した場合、ゲートウェイは NTE を使用して DTMF 番号を受信し、KPML へのサブスクライブは行いません。

Cisco SIP ゲートウェイでは、DTMF に独自の Unsolicited Notify（UN）方式を使用することもできます。UN 方式は、DTMF トーンを表すテキストをメッセージ本体に含む SIP Notify メッセージを送信します。この方式は Unified CM でもサポートされており、**sip-kpml** が有効でない場合に使用されます。DTMF リレー方式として **sip-notify** を設定します。この方式はシスコ独自のものである点に注意してください。

NTE だけをサポートする SIP ゲートウェイでは、NTE をサポートしないエンドポイントと通信する場合、MTP リソースの割り当てが必要となります。

H.323 トランクおよびゲートウェイ

H.323 プロトコルでは、次の 3 つの理由で MTP が呼び出されます。

- 「DTMF 変換」（P.17-16）
- 「H.323 付加サービス」（P.17-20）
- 「H.323 発信時の Fast Connect」（P.17-21）

H.323 付加サービス

MTP は、付加サービスに使用され、Empty Capabilities Set（ECS）機能を使用している H.323v2 の OpenLogicalChannel および CloseLogicalChannel 要求機能をサポートしていない H.323 エンドポイントの機能を拡張できます。この要件はあまり発生しません。すべての Cisco H.323 エンドポイント、およびほとんどのサードパーティのエンドポイントが ECS をサポートしています。必要に応じて、MTP

が割り当てられ、H.323 エンドポイントに代わってコールに接続されます。MTP が H.323 コールで要求され、使用できるものがない場合、コールは処理されますが、付加サービスを呼び出すことはできません。

H.323 発信時の Fast Connect

H.323 では、Fast Connect という手順が定義されています。これは、コール セットアップ時に交換されるパケット数を削減し、メディアを確立する時間を短縮します。この手順では、制御チャネルのシグナリングに Fast Start 要素を使用します。H.323 を利用する 2 つのデバイスのネットワーク遅延が高いときは、この遅延がメディアを確立する時間に影響を与えるため、この手順が役立ちます。
Unified CM は、コール セットアップの方向に基づき、着信 Fast Start と発信 Fast Start を区別します。MTP 要件が同じではないため、この区別は重要です。着信 Fast Start の場合、MTP は必要ありません。H.323 トランクの発信コールは、Fast Start が有効なとき、MTP を必要とします。多くの場合、問題になるのは、着信コールだけです。問題を解決するには、発信 Fast Start を有効にせずに着信 Fast Start を使用します。

H.323 トランク上の DTMF リレー

H.323 トランクは、H.245 アウトオブバンド方式による DTMF のシグナリングをサポートします。Unified CM 5.0 およびそれ以降のリリースの H.323 クラスタ間トランクは、NTE による DTMF もサポートします。H.323 トランクには DTMF 設定オプションはありません。DTMF 転送方式は Unified CM によって動的に選択されます。

異なるクラスタにある 2 つのエンドポイントが H.323 トランクを使用して接続する場合は、次のケースが起こり得ます。

- 両方のエンドポイントが SIP の場合は、NTE が使用されます。DTMF のために MTP は必要ありません。
- 一方のエンドポイントが SIP で、KPML と NTE の両方をサポートしていて、他方のエンドポイントが SIP でない場合は、SIP エンドポイントから Unified CM に KPML で DTMF が送信され、トランクでは H.245 が使用されます。DTMF のために MTP は必要ありません。
- 一方のエンドポイントが SIP で、NTE だけをサポートしていて、他方のエンドポイントが SIP でない場合は、トランクで H.245 が使用されます。この場合はコールに対して使用可能な MTP が割り当てられます。MTP は、SIP エンドポイントがある Unified CM クラスタで割り当てられます。

たとえば、SIP を使用する Cisco Unified IP Phone 7970 が、SCCP を使用する Cisco Unified IP Phone 7970 と通信する場合は、SIP トランク経由で接続されるときは NTE が使用され、H.323 トランク経由で（H.245 方式を使用するトランクを使用して）通信するときは OOB 方式が使用されます。

コールがある H.323 トランクから着信し、そのコールを別の H.323 トランクにルーティングする場合、両方のエンドポイントが SIP のときは、DTMF 用に NTE が使用されます。どちらか一方のエンドポイントが SIP でないときは、H.245 が使用されます。一方が NTE だけをサポートする SIP エンドポイントで、他方が SIP でない場合は、MTP が割り当てられます。

H.323 ゲートウェイおよび Cisco Unified Border Element での DTMF リレーの設定

H.323 ゲートウェイは、H.245 Alphanumeric、H.245 Signal、NTE、およびメディア ストリームのオーディオによる DTMF リレーをサポートします。現時点では、H.323 ゲートウェイ用の Unified CM において NTE オプションはサポートされていないため、使用できません。これに適したオプションは H.245 Signal です。他のエンドポイントに Unified CM と共通のシグナリング機能がない場合、H.323 ゲートウェイへのコールを確立するために、MTP が必要です。たとえば、SIP スタックを実行している Cisco Unified IP Phone 7960 は NTE だけをサポートするため、H.323 ゲートウェイを使用する場合は MTP が必要です。

CTI ルート ポイント

CTI ルート ポイントは、CTI イベントを使用して CTI アプリケーションと通信します。DTMF の観点では、CTI ルート ポイントは、すべての OOB 方式をサポートし、RFC 2833 はサポートしないエンドポイントと見なすことができます。そのようなエンドポイントで DTMF 変換に MTP が必要となるケースは、RFC 2833 だけをサポートする別のエンドポイントと通信する場合だけです。

電話コールのファーストパーティ制御を持つ CTI ルート ポイントは、コールのメディア ストリームに参加し、MTP の挿入を必要とします。CTI によるコールのサードパーティ制御が可能で、メディアが CTI で制御されているデバイスを通過する場合、MTP が必要かどうかは制御されるデバイスの機能によって異なります。

例 17-1　NTE 変換用に MTP を必要とするコール フロー

例として、ファーストパーティ制御（CTI ポートがメディアの終端）の CTI ルート ポイントがあり、IVR メニューをナビゲートするために DTMF を使用するシステムに統合されているシステムを考えます。システムのすべての電話機が SCCP を実行している場合、MTP は必要ありません。この場合、Unified CM が CTI ポートを制御し、IP Phone からの DTMF を SCCP 経由で受信します。Unified CM が、DTMF 変換を提供します。

ただし、SIP スタックを実行している電話機（NTE だけをサポートしていて、KPML をサポートしていない電話機）がある場合は、MTP が必要です。NTE はメディア ストリームの一部なので、Unified CM は受信しません。MTP がメディア ストリームの中に呼び出され、SCCP を使用する 1 つのコール レッグと NTE を使用する 2 番めのコール レッグを持ちます。MTP は Unified CM による SCCP の制御下にあり、Unified CM の制御下で NTE から SCCP への変換を実行します。KPML をサポートしている新しい電話機では、MTP は必要ありません。

カンファレンス ブリッジでの MTP の使用

MTP は、会議の参加者のデバイスの中に RFC 2833 を使用するデバイスがある場合に使用されます。会議機能が呼び出されると、Unified CM が、コールに含まれており、RFC 2833 だけをサポートするすべての会議参加者のデバイスに MTP リソースを割り当てます。これは、カンファレンス ブリッジの DTMF 機能が使用されているかどうかにかかわらず行われます。

MTP リソース

次のタイプのデバイスは、MTP として使用できます。

ソフトウェア MTP（Cisco IP Voice Media Streaming Application）

ソフトウェア MTP とは、サーバに Cisco IP Voice Media Streaming Application をインストールすることによって設定されるデバイスです。インストールされたアプリケーションが、MTP アプリケーションとして設定されると、そのアプリケーションは、Unified CM ノードに登録され、サポートする MTP リソース数を Unified CM に知らせます。ソフトウェア MTP デバイスは、G.711 ストリームだけをサポートします。IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ガイダンスではすべての機能を同時に考慮する必要があります（「Cisco IP Voice Media Streaming Application」（P.17-4）を参照）。

ソフトウェア MTP（Cisco IOS に基づく）

- ルータでソフトウェアベースの MTP を提供する機能は、Cisco 3800 シリーズ ルータでは Cisco IOS Release 12.3(11)T、Cisco 2900 シリーズおよび 3900 シリーズ ルータでは Release 15.0(1)M、ASR1002、1004、および 1006 ルータでは、Release IOS-XE、ASR1001 ルータでは、Release IOS-XE 3.2、その他のルータ モデルでは、Release 12.3(8)T4 から使用できるようになりました。
- この MTP によって、G.711 mu-law および a-law、G.729a、G.729、G.729ab、G.729b、およびパススルーのコーデックを設定できます。ただし、同時に設定できるコーデックは 1 つだけです。これらの内の一部のコーデックは、Unified CM では実装していません。
- ルータ設定では、最大 1,000 の個別ストリームが可能で、500 のトランスコーディングされたセッションをサポートします。この数の G.711 ストリームを使用すると、10 MB のトラフィックが生成されます。Cisco ISR G2 および ASR ルータでは、これよりもはるかに大きな数をサポートできます。

ハードウェア MTP（PVDM2、Cisco NM-HDV2 および NM-HD-1V/2V/2VE）

- このハードウェアは、PVDM-2 モジュールを使用して DSP を提供します。
- 各 DSP は、16 の G.711 mu-law または a-law MTP セッション、8 つの G.729a または G.722 MTP セッション、または 6 つの G.729 または G.729b MTP セッションを提供できます。

ハードウェア MTP（PVDM3 を搭載した Cisco 2900 および 3900 シリーズ ルータ）

- これらのルータでは、マザーボード上の PVDM3 DSP をネイティブに使用するか、またはマザーボード上やサービス モジュール上のアダプタによる PVDM2 を使用します。
- 各 DSP タイプのキャパシティの範囲は、16 G.711 a-law または mu-law セッション（PVDM3-16 の場合）から、256 G.711 セッション（PVDM3-256 の場合）までとなります。

ハードウェア MTP（Cisco WS-SVC-CMM-ACT）

- このモジュールには、個別に設定できる 4 つの DSP があります。
- 各 DSP は、128 の G.711 mu-law または a-law MTP セッションをサポートします。

ハードウェア MTP（Catalyst WS-X6608-T1 および WS-X6608-E1）

- サポートされるコーデックは、G.711 mu-law または a-law、G.729、または G.729b です。
- 設定はポート レベルで行います。モジュールごとに 8 つのポートを使用できます。
- MTP リソースとして設定されたポートごとに、24 のセッションが提供されます。

（注） Cisco IOS でハードウェア MTP リソースを設定している場合は、G.729 または G.729b コーデックは設定できません。ただし、他のすべての MTP リソースが使い果たされた場合、または使用できない場合には、Unified CM はハードウェア トランスコーディング リソースを MTP として使用できます。

Trusted Relay Point

Trusted Relay Point（TRP）はメディア ストリームに挿入可能なデバイスの一種で、そのストリームのコントロール ポイントとして機能します。TRP を使用すると、そのストリームにさらに処理を加えることができます。また、ストリームが任意の特定のパスを通るようにする手段として TRP を使用することも可能です。TRP 機能を使用するためには 2 つの要素が存在します。1 つは CUCM 上で論理的に TRP を設定すること。もう 1 つは実際に TRP として動作するコールのアンカーポイントとなるデバイスです。TRP 機能は MTP デバイスをアンカーポイントとして使用する際に使うことができます。

Unified CM の個々の電話機に関する設定に、その電話機へのコールまたはその電話機からのコールに対して TRP を呼び出すための設定パラメータが新しく追加されました。TRP リソースの管理には、メディア リソース プール メカニズムが利用されます。その電話機のメディア リソース プールには、TRP として呼び出し可能なデバイスが含まれている必要があります。

TRP を QoS 強制メカニズムとして使用する例については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。冗長ファイアウォールを備えた冗長なデータセンターでメディア ストリームのアンカー ポイントとして TRP を利用する例については、「Unified Communications のセキュリティ」（P.4-1）の章を参照してください。

Annunciator

Annunciator は Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種コール プログレス トーンをシステムからユーザに流すことができます。この機能は、複数の片方向 RTP ストリームを Cisco IP Phone やゲートウェイなどのデバイスに送信できます。さらに、SCCP メッセージを使用して、RTP ストリームを確立します。この機能を使用するには、デバイスが SCCP に対応している必要があります。トーンとアナウンスは、システムで事前に定義されています。アナウンスでは、ローカリゼーションがサポートされています。また、適切な .wav ファイルを置き換えて、アナウンスをカスタマイズすることもできます。Annunciator は、トランスコーディング リソースを使用しないで、G.711 a-law および mu-law、G.729、および Wideband コーデックをサポートできます。

次の機能には、Annunciator リソースが必要です。

- Cisco Multilevel Precedence Preemption（MLPP）

  この機能には、次のようなコール失敗の状態に応じて再生されるストリーミング メッセージが用意されています。

  - 優先順位の高い既存のコールが原因で、プリエンプション処理できない。
  - 優先順位アクセス制限に到達した。
  - 試行された優先順位レベルが許可されていない。
  - 着信番号が、プリエンプション処理またはコール ウェイティングに対応していない。

- SIP トランクを介した統合

  SIP エンドポイントには、トーンを生成し、RTP ストリームでインバンドで送信する機能があります。SCCP デバイスにはこの機能がないため、SIP エンドポイントと統合した場合、DTMF トーンの生成または受け入れ時には Annunciator と MTP が併用されます。次のタイプのトーンがサポートされます。

  - コール プログレス トーン（ビジー、アラート、およびリングバック）
  - DTMF トーン

- Cisco IOS ゲートウェイとクラスタ間トランク

  これらのデバイスには、コール プログレス トーン（リングバック トーン）のサポートが必要です。

- システム メッセージ

  次のようなコール失敗の状態では、システムはエンド ユーザにストリーミング メッセージを再生します。

  - ダイヤル番号をシステムが認識できない。
  - サービスが中断したためコールがルーティングされない。

  - 番号が通話中で、その番号がプリエンプション処理またはコール ウェイティング用に設定されていない。

- 会議

  電話会議の間、システムは、参加者がブリッジに参加、またはブリッジから退出したことをアナウンスするときに、割り込み音を再生します。

Cisco IP Voice Media Streaming Application をサーバ上でアクティブにすると、Annunciator がシステム内に自動的に作成されます。Media Streaming Application を非アクティブにすると、Annunciator も削除されます。単一の Annunciator インスタンスは、パフォーマンス要件を満たす場合は、Unified CM クラスタ全体にサービスを提供できます（「Annunciator のパフォーマンス」（P.17-25）を参照）。そうでない場合は、追加の Annunciator をクラスタ用に設定する必要があります。追加の Annunciator を設定するには、クラスタ内の他のサーバ上で Cisco IP Voice Media Streaming Application をアクティブにします。

Annunciator は、そのデバイス プールで定義されたとおり、一度に 1 つの Unified CM に登録されます。デバイス プールに対してセカンダリが設定されている場合、Annunciator は自動的にセカンダリ Unified CM にフェールオーバーします。障害発生時に再生されるアナウンスはいずれも保持されません。

Annunciator はメディア デバイスと見なされるため、メディア リソース グループ（MRG）に含めて、電話機およびゲートウェイで使用される Annunciator の選択を制御できます。

Annunciator のパフォーマンス

デフォルトでは、Annunciator は 48 のストリームを同時にサポートするように設定されています。この設定値は、Unified CM サービスが同一のサーバ（共存）上で動作する Annunciator に推奨される最大値です。サーバの接続性が 10 Mbps しかない場合は、設定を下げて同時ストリームを 24 にします。

Cisco CallManager Service を含まないスタンドアロン サーバでは、最大 255 のアナウンス ストリームを同時にサポートできます。デュアル CPU と高性能ディスク システムを持つ高性能サーバでは、最大 400 のストリームをサポートできます。複数のスタンドアロン サーバを追加して、必要な数のストリームをサポートできます。

Cisco RSVP Agent

トポロジ対応型のコール アドミッション制御を提供するために、Unified CM は 1 つまたは 2 つの RSVP Agent をコール セットアップ時に呼び出し、IP WAN で RSVP 予約を実行します。これらのエージェントは、RSVP 機能を提供するように設定された MTP またはトランスコーダ リソースです。RSVP リソースは、Unified CM による MTP またはトランスコーダ リソースの割り当てという観点から見て、通常の MTP またはトランスコーダと同様に処理されます。

Cisco RSVP Agent 機能は、Cisco IOS Release 12.4(6)T で最初に導入されました。RSVP および Cisco RSVP Agent の詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください。

保留音

Music On Hold（MoH; 保留音）機能を利用するには、各 MoH サーバが Unified CM クラスタに含まれている必要があります。すべての MoH サーバは、パブリッシャ サーバと設定を共有し、データベース複製スキーマに加わる必要があります。具体的には、MoH サーバはデータベースによって次の情報を共有する必要があります（これらの情報は Unified CM Administration で設定されます）。

- オーディオ ソース：設定されたすべての MoH オーディオ ソースの数と ID
- マルチキャストまたはユニキャスト：これらのソースそれぞれに設定されたトランスポートの種類
- マルチキャスト アドレス：マルチキャストとしてストリーミングするように設定されたソースのマルチキャスト ベース IP アドレス

MoH サーバは、Unified CM クラスタの一部になり、自動的にデータベースの複製に加わります。スタンドアロン MoH サーバを設定するには、標準の Unified CM インストールから開始し、次に、Cisco CallManager サービスを有効にせずに（スタンドアロン MoH サーバ上でだけ）、Cisco IP Voice Media Streaming Application を有効にします。

ユニキャストおよびマルチキャスト MoH

Unified CM は、次の 2 つのタイプの MoH トランスポート メカニズムをサポートします。

- ユニキャスト
- マルチキャスト

ユニキャスト MoH は、MoH サーバから MoH オーディオ ストリームを要求するエンドポイントに直接送信されるストリームで構成されます。ユニキャスト MoH ストリームは、サーバとエンドポイント デバイス間のポイントツーポイント片方向オーディオ Real-Time Transport Protocol（RTP）ストリームです。ユニキャスト MoH は、ユーザまたは接続ごとに別々のソース ストリームを使用します。ユーザまたはネットワーク イベントを介して保留になるエンドポイント デバイスが増えるにつれて、MoH ストリームの本数も増加します。したがって、20 台のデバイスが保留になっている場合、サーバとこれらのエンドポイント デバイス間のネットワーク上で、RTP トラフィックとしてストリームが 20 本生成されます。このような MoH ストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。しかし、ユニキャスト MoH が非常に役立つのは、マルチキャストが使用可能になっていないネットワークの場合や、デバイスがマルチキャスト対応になっていないネットワークの場合です。このようなときに、管理者はユニキャスト MoH を使用することで、MoH 機能を利用できます。

マルチキャスト MoH は、MoH サーバからマルチキャスト グループ IP アドレスに送信されるストリームで構成されます。MoH オーディオ ストリームを要求するエンドポイントは、必要に応じてこの IP アドレスに加わることができます。マルチキャスト MoH ストリームは、MoH サーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片方向オーディオ RTP ストリームです。マルチキャスト MoH では、複数のユーザが同じオーディオ ソース ストリームを使用して保留音を提供できるようにするので、システム リソースと帯域幅を節約できます。したがって、20 台のデバイスが保留中であっても、ネットワーク上で 1 つの RTP トラフィックのストリームだけしか生成されない場合もあります。このため、マルチキャストは、ソース デバイスに対する CPU の影響を大幅に削減し、共通パス上の伝送の帯域幅使用量も大幅に削減するので、MoH などのサービスの配置に非常に魅力的なトランスポート メカニズムです。しかし、ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、マルチキャスト MoH に問題が生じます。

MoH 操作は、通常の電話のコール フローに非常によく似ています。MoH サーバは、被保留側デバイスが必要に応じて接続または切断されるエンドポイント デバイスの役目をします。しかし、ユニキャストとマルチキャストの MoH コール フローの動作には、明らかな相違点があります。ユニキャスト

MoH コール フローは、Unified CM から MoH サーバへのメッセージによって初期化されます。このメッセージは、被保留側デバイスの IP アドレスにオーディオ ストリームを送信するように、MoH サーバに指示します。一方、マルチキャスト MoH コール フローは、Unified CM から被保留側デバイスへのメッセージによって初期化されます。このメッセージは、設定されたマルチキャスト MoH オーディオ ストリームのマルチキャスト グループ アドレスに加わるように、エンドポイント デバイスに指示します。

MoH コール フローの詳細については、「ユニキャストとマルチキャスト MoH コール フローの詳細」（P.17-54）の項を参照してください。

サポートされるユニキャストおよびマルチキャスト ゲートウェイ

次のゲートウェイは、ユニキャスト MoH とマルチキャスト MoH の両方をサポートします。

- Cisco IOS 15.0.1M 以降のリリースを搭載した Cisco 2900 シリーズおよび Cisco 3900/3900E シリーズ ISR G2 ルータ
- MGCP または H.323 を使用し、Cisco IOS 12.3.14T 以降のリリースを搭載した Cisco 2800 シリーズおよび 3800 シリーズ ルータ
- SIP を使用する Cisco 2800 シリーズおよび 3800 シリーズ ルータと、Cisco IOS 12.4(24)T 以降のリリース
- MGCP を使用し、Cisco IOS 12.3.14T 以降のリリースを搭載した Cisco VG224 Analog Voice Gateway
- MGCP または SCCP を使用する Cisco VG204 および VG202 Analog Voice Gateway と、Cisco IOS 12.4(22)T 以降のリリース
- Cisco VG248 Analog Phone Gateway
- Cisco ASR 1000 シリーズ Aggregation Services Router

（注）　Cisco 2800 シリーズ、3800 シリーズ、および VG248 ゲートウェイは、End of Sale（EoS; 販売終了）となっています。ユニキャスト MoH およびマルチキャスト MoH をサポートするレガシー ゲートウェイは他にもあります。

（注）　Cisco ASR 1000 シリーズ Aggregation Services Router 上の Cisco Unified Border Element は、Cisco Unified Communications Manager の Music on Hold（MoH; 保留音）機能による音楽またはアナウンスの一方向のストリーミングをサポートしていない場合があります。詳細については、ご使用のバージョンの Cisco Unified Communications Manager のリリース ノート（http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_release_notes_list.html で入手可能）を参照してください。

MoH 選択プロセス

この項では、Unified CM に実装するときの MoH 選択プロセスについて説明します。

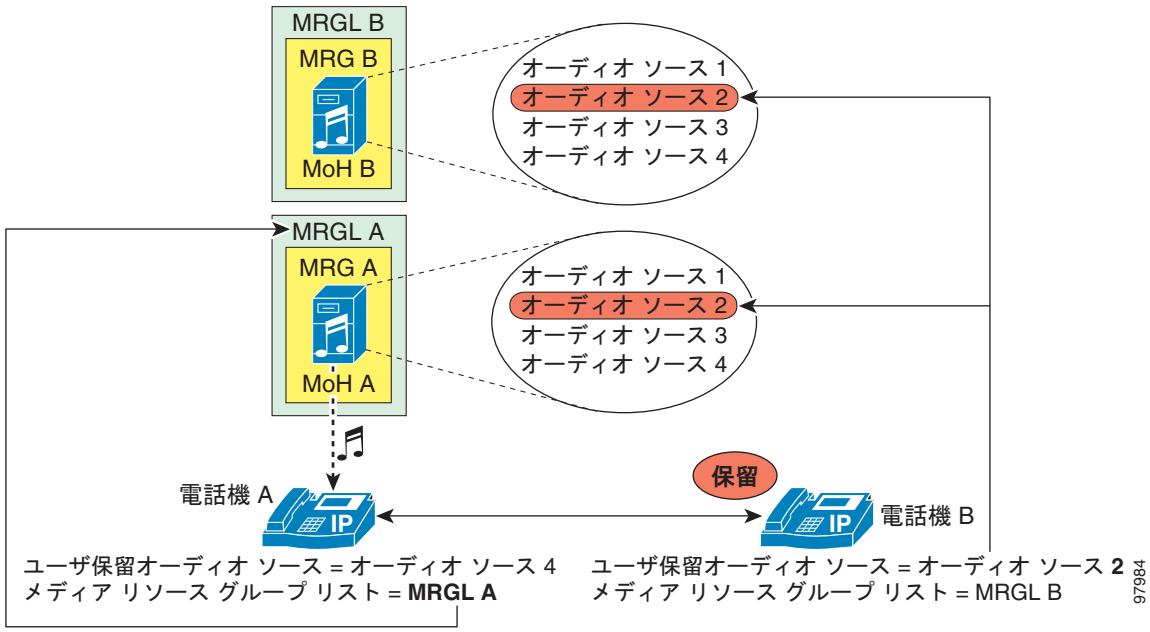
Cisco Unified Communication 環境における基本的な MoH の動作は、保留側と被保留側から構成されます。*保留側*とは、通話を保留にするエンドポイント ユーザまたはネットワーク アプリケーションです。一方、*被保留側*とは、保留にされたエンドポイント ユーザまたはデバイスです。

エンドポイントが受信する MoH ストリームは、エンドポイントを保留にするデバイス（保留側）のユーザ保留 MoH オーディオ ソースと、保留にされたエンドポイント（被保留側）に設定された Media Resource Group List（MRGL; メディア リソース グループ リスト）との組み合せによって決まります。

保留側に対して設定されたユーザ保留 MoH オーディオ ソースによって、保留側が通話を保留にしたときに流されるオーディオ ファイルが決まります。被保留側に設定された MRGL は、被保留側が MoH ストリームを受信する元のリソースまたはサーバを指定します。

簡単に言えば、保留側の設定により、再生されるオーディオ ファイルが決まり、被保留側の設定により、そのファイルを再生するリソースまたはサーバが決まります。図 17-3 の例に示すように、電話機 A および B が通話中であるときに、電話機 B（保留側）で電話機 A（被保留側）を保留にする場合、電話機 A には、電話機 B に対して設定された MoH オーディオ ソース（オーディオソース 2）が聞こえます。ただし、電話機 A はこの MoH オーディオ ストリームを、電話機 A に対して設定された MRGL（リソースまたはサーバ）（MRGL A）から受信します。

図 17-3　ユーザ保留オーディオ ソースとメディア リソース グループ リスト（MRGL）



設定した MRGL により、ユニキャスト専用デバイスが MoH ストリームを受信するサーバが決まるので、ユニキャスト専用デバイスを設定する場合は、ユニキャスト MoH リソースまたは Media Resource Group（MRG; メディア リソース グループ）を指定する MRGL を使用する必要があります。同様に、マルチキャスト機能を持つデバイスは、マルチキャスト用に設定された MoH サーバが含まれたマルチキャスト MRG を指定する MRGL を使用して設定する必要があります。

ユーザ保留とネットワーク保留

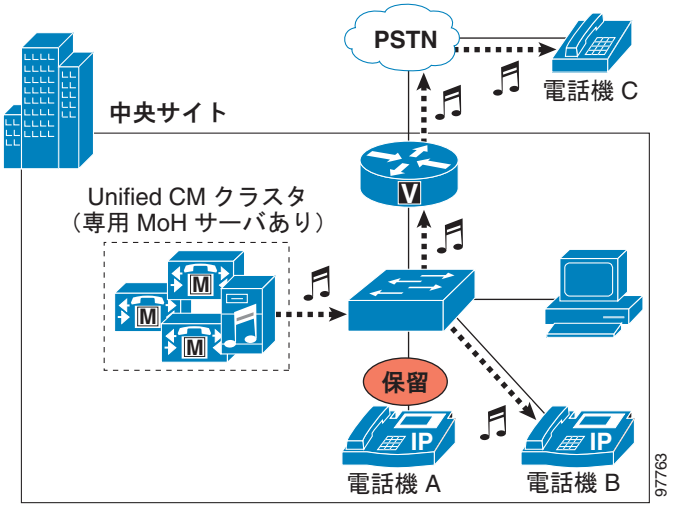
ユーザ保留には次のタイプがあります。

- IP Phone またはその他のエンドポイント デバイスでのユーザ保留
- MoH がゲートウェイにストリーミングされる公衆網でのユーザ保留

図 17-4 は、これらの 2 つのタイプのコール フローを示しています。電話機 A が電話機 B と通話中であるときに、電話機 A（保留側）で [Hold] ソフトキーを押すと、MoH サーバから電話機 B（被保留側）に音楽ストリームが送信されます。この音楽ストリームは、IP ネットワーク内の被保留側だけでなく、電話機 A が電話機 C を保留にする場合と同様に、公衆網上の被保留側にも送信できます。電話

機 C の場合、MoH ストリームは音声ゲートウェイ インターフェイスに送信され、公衆網電話機に適したフォーマットに変換されます。電話機 A が [Resume] ソフトキーを押すと、被保留側（電話機 B または C）は、音楽ストリームから切り離され、電話機 A に再び接続されます。

図 17-4　ユーザ保留の基本的な例

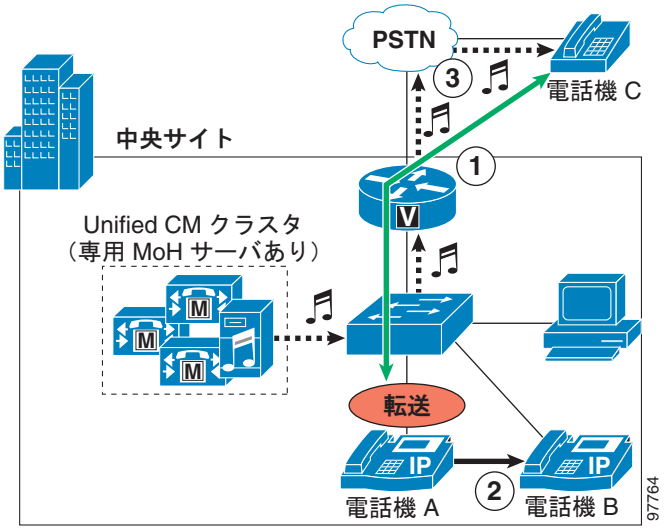


ネットワーク保留には次のタイプがあります。

- コール転送
- コール パーク
- 会議セットアップ
- アプリケーションベースの保留

図 17-5 は、コール転送のコール フローを示しています。電話機 A が公衆網電話機 C からコールを受信する（ステップ 1）と、電話機 A はそのコールに応答し、電話機 B に転送します（ステップ 2）。転送プロセス時に、電話機 C は、ゲートウェイを介して MoH サーバから MoH ストリームを受信します（ステップ 3）。電話機 A が転送アクションを完了したあと、電話機 C は音楽ストリームから切り離され、電話機 B（転送の宛先）に転送されます。このプロセスは、コール パークや会議セットアップなどの他のネットワーク保留操作の場合と同じです。

図 17-5　コール転送のネットワーク保留の基本的な例



MoH ソース

Unified CM MoH サーバでは、次の 2 つのタイプのソースから MoH ストリームを生成できます。

- Unified CM MoH サーバにアップロードされるオーディオ ファイル
- USB サウンド カード経由の固定（ライブ）音楽ソース

また、いずれのタイプのソースも、ユニキャストまたはマルチキャストとして送信できます。

オーディオ ファイル

MoH オーディオ ファイルは、[MoH Audio File Management] ページ（または [Music On Hold Audio Source Configuration] ページ）でファイル アップロード機能を使用して、.wav フォーマットのオーディオ ファイルを MoH サーバにアップロードすると、Unified CM によって自動的に生成されます。次に、Unified CM は、オーディオ ソース ファイルを指定されたコーデック タイプに適した MoH ソース ファイルにトランスコードし、フォーマットします。Unified CM では、MoH ストリーム用に次のコーデックをサポートしています。

- G.711 A-law または mu-law
- G.729 Annex A
- ワイドバンド

MoH イベントが発生すると、MoH サーバは、設定されたオーディオ ソース ファイルを保留中の要求側デバイスにストリーミングします。

（注）　MoH オーディオ ソースの設定前に、.wav フォーマットのオーディオ ソース ファイルをクラスタ内の各 MoH サーバにアップロードしておく必要があります。オーディオ ソース ファイルをアップロードするには、管理者がクラスタ内のすべての MoH サーバ上で Unified CM Administration インターフェイスに移動し、[MoH Audio File Management] ページでファイルのアップロード機能を使用する必要があります。管理者は、この手順をすべてのオーディオ ソース ファイルに対して実行する必要があります。最初にオーディオ ソース ファイルをクラスタ内の各 MoH サーバにアップロードし、次にその

オーディオ ファイルをパブリッシャ サーバ（MoH サーバでなくてもかまいません）にアップロードし、最後にそのパブリッシャ上の Unified CM Administration インターフェイスで MoH オーディオ ストリーム番号を割り当て、MoH オーディオ ソースを設定することを推奨します。

固定ソース

録音済みまたはライブ オーディオが必要である場合、固定ソースから MoH を生成できます。このタイプの MoH の場合、サウンド カードが必要です。固定オーディオ ソースは、ローカル サウンド カードのオーディオ入力に接続されます。

このメカニズムにより、ラジオ、CD プレーヤー、または互換性があるその他のサウンド ソースを使用できます。固定オーディオ ソースからのストリームは、リアルタイムで変換され、Unified CM Administration によって設定されたコーデックに対応します。固定オーディオ ソースは、G.711（A-law または mu-law）、G.729 Annex A、およびワイドバンドに変換することができる、リアルタイムで変換可能な唯一のオーディオ ソースです。

固定またはライブ オーディオ ソースを MoH サーバに接続するには、Cisco MoH USB オーディオ サウンド カード（MOH-USB-AUDIO=）を使用する必要があります。この USB サウンド カードは、Cisco Unified CM をサポートするすべての MCS プラットフォームと互換性があります。

（注）　保留音を送信するときに固定オーディオ ソースを使用する場合は、事前に、著作権のあるオーディオ素材の再ブロードキャストについて、その適法性および問題を検討しておく必要があります。起こりうる問題については、貴社の法務部門に相談してください。

MoH 構成の設定値の選択

MRGL、およびユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの設定値は、Unified CM Administration 内の複数の箇所で指定できます。それぞれの箇所で別々の設定値（優先順位あり）を設定できます。

個々のケースにユーザ オーディオ ソース設定値とネットワーク オーディオ ソース設定値のいずれかを適用するか決定するために、Unified CM は、次の優先順位で、*保留側*デバイスに対するこれらの設定値を使用します。

1. ディレクトリまたは回線設定（ゲートウェイなど、回線定義のないデバイスには、このレベルはありません）
2. デバイス設定値
3. 共通のデバイス設定
4. クラスタ全体のデフォルト設定

特定の保留側のオーディオ ソースを決定しようとする場合、Unified CM はまず、ディレクトリまたは回線レベルで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、保留側デバイスで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、保留側デバイスの共通プロファイルに設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Unified CM は、Unified CM システム パラメータで設定された、クラスタ全体のデフォルト オーディオ ソース ID を調べます（デフォルトでは、このオーディオ ソース ID は、ユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの両方に対して 1 に設定されています。これは、SampleAudioSource です）。

Unified CM は、*被保留側*デバイスの MRGL 設定値も、次の優先順位で使用します。

1. デバイス設定値
2. デバイス プールの設定値
3. システムのデフォルト MoH リソース

特定の被保留側の MRGL を決定しようとする場合、Unified CM は、デバイス レベルで設定された MRGL を調べます。このレベルが定義されていない場合、Unified CM は、被保留側デバイスのデバイス プールに対して設定された MRGL を調べます。このレベルが定義されていない場合、Unified CM は、システムのデフォルト MoH リソースを使用します。システムのデフォルト MoH リソースとは、MRG に割り当てられていないリソースであり、これらのリソースは常にユニキャストです。

メディア リソースのキャパシティ プランニング

この項では、DSP を含むネットワークモジュールおよびシャーシのキャパシティ、ネットワーク モジュールを含むシャーシのキャパシティ、およびハードウェアに対するソフトウェアの依存性に関するデータを提供します。すべての Cisco ISR G1 および G2 のキャパシティ プランニングには、http://www.cisco.com/go/dspcalculator で入手できる DSP Calculator を使用します。他のプラットフォーム（Cisco 1700、2600、および 3700 シリーズ ルータなど）については、http://www.cisco.com/cgi-bin/Support/DSP/cisco_dsp_calc.pl からレガシーの DSP Calculator を使用します。

表 17-2、表 17-3、および表 17-4 に、PVDM の 3 つのモデルまたは固定構成ネットワーク モジュールに配置できる DSP の数を示します。PVDM3 モジュールは、PVDM2 モジュールと PVDM-256K モジュールよりも新しく、これらの 3 つのタイプは互いに交換できません。

表 17-2　PVDM-256K モジュールあたりの DSP 数

モジュール	DSP 数
PVDM-256K-4	1 DSP
PVDM-256K-8	2 DSP
PVDM-256K-12	3 DSP
PVDM-256K-16HD	4 DSP
PVDM-256K-20HD	5 DSP

表 17-3　PVDM2 モジュールまたは固定構成ハードウェアあたりの DSP 数

ハードウェア モジュールまたはシャーシ	DSP 数
PVDM2-8	½ DSP
PVDM2-16	1 DSP
PVDM2-32	2 DSP
PVDM2-48	3 DSP
PVDM2-64	4 DSP
NM-HD-1V NM-HD-2V	1 DSP
NM-HD-2VE	3 DSP

表 17-4　PVDM3 モジュールあたりの DSP 数

ハードウェア モジュール	DSP テクノロジー
PVDM3-16	1 つの DSP、シングル コア
PVDM3-32	1 つの DSP、シングル コア
PVDM3-64	1 つの DSP、デュアル コア
PVDM3-128	1 つの DSP、3 コア
PVDM3-192	2 つの DSP : 一方にデュアル コア、もう一方に 3 コア
PVDM3-256	2 つの DSP、両方に 3 コア

PVDM3 DSP モジュールは、Cisco 2900 シリーズおよび 3900 シリーズ プラットフォームでサポートされており、Cisco IOS Release 15.0(1) M 以降が必要です。

表 17-5 に、PVDM2 モジュールの各ハードウェア プラットフォームでメディア リソース機能をサポートするために必要な、Cisco IOS ソフトウェアの最小バージョンを示します。

表 17-5　メディア サポートに必要な使用可能 PVDM2 スロット数と Cisco IOS のバージョン

シャーシまたはネットワーク モジュール	マザーボードの PVDM2 スロット数	メディア用 Cisco IOS 最小リリース
2801	2	12.3(11)T
2811	2	12.3(8)T4
2821 または 2851	3	12.3(8)T4
3825 または 3845	4	12.3(11)T
NM-HDV2	4	12.3.7T
2901 または 2911	2	15.0.1M
2921 または 2951	3	15.0.1M
3925 または 3945	4	15.0.1M
3925E または 3945E	3	15.1.1T

Cisco 2900 および 3900 シリーズ プラットフォーム

Cisco 2900 および 3900 シリーズ プラットフォームは、Integrated Services Router Generation 2（ISR G2; サービス統合型ルータ第 2 世代）とも呼ばれます。これらのルータでは、マザーボード上で使用可能な DSP スロットに直接挿入できる PVDM3 DSP モジュールをサポートしています。また、PVDM2 DSP モジュールも、アダプタ カードを使用することによって、マザーボード上に取り付けることができます。

ISR G2 では、アダプタ カードを使用することで、サービス モジュール スロットでの NM-HD カードと NM-HDV2 カードもサポートされます。

次のガイドラインおよび考慮事項は、これらのプラットフォームでホストされる DSP リソースに適用されます。

- Cisco 2900 および 3900 シリーズ ルータでは、オンボード（マザーボード）の DSP スロットに挿入された PVDM3 DSP だけがサポートされます。PVDM2 DSP は、アダプタ カードを使用することで、これらのスロットで使用できます。
- PVDM2 モジュールと PVDM3 モジュールは、同じマザーボード上で同時に使用することはできません。
- DSP は、同じ DSP タイプ間でだけ共有できます。たとえば、マザーボードに PVDM3 DSP が挿入されており、サービス モジュールに PVDM2 DSP が挿入されている場合、サービス モジュールの複数の DSP は相互に共有できますが、マザーボード上の DSP は、サービス モジュールの DSP とは共有できません。
- PVDM3 DSP では、Cisco FAX リレーを除き、PVDM2 DSP がサポートしているすべての機能がサポートされます。

PVDM2 とは異なり、PVDM3 DSP は、すべてのメディア機能の単一ソフトウェア イメージを提供します。

Cisco 2800 および 3800 シリーズ プラットフォーム

Cisco 2800 および 3800 シリーズ ルータはすべて、2 つの AIM スロットを備えていますが、AIM-VOICE-30 または AIM-ATM-VOICE-30 カードをサポートしません。これは、これらのカードの機能は、マザーボード上に取り付けられた PVDM2 モジュールによって代わりに提供されるためです。

ネットワーク モジュール

NM-HDV2、NM-HD-*xx*、および NM-HDV モジュールは、表 17-6 に示されている Cisco IOS プラットフォームに取り付けることができます。その場合の最大モジュール数は、表のとおりです。

表 17-17 内の 3 つのモジュール ファミリはすべて 1 つのシャーシに取り付けることができます。ただし、会議機能とトランスコーディング機能は、NM-HDV ファミリと、残りのファミリのどちらか（NM-HD-*xx* または NM-HDV2）との両方で同時に使用することはできません。また、NM-HDV（TI-549）、NM-HD-*xx*、および NM-HDV2（TI-5510）を、1 つのシャーシ内で同時に会議およびトランスコーディングに使用することはできません。

NM-HDV モジュールと NM-HDV-FARM モジュールは、同じシャーシに混在できます。すべてのシャーシがこれらのモジュールをフル装備できるわけではありません。表 17-16 では、各タイプのハードウェア プラットフォームがサポートする最大モジュール数を示しています。

表 17-6　プラットフォーム タイプごとのネットワーク モジュールまたはサービス モジュールのスロット数

Cisco IOS プラットフォーム	スロット数
2691、2811、2821、2851、2911、2921	1
3620[1]、3725、3825、2951、3925、3925E	2
3640、3745、3845、3945、3945E	4
3660	6

1. Cisco 3620 ルータは 2 つの NM スロットを備えていますが、サポートする NM-HDV モジュールは 1 つだけです。

表 17-7　プラットフォーム タイプでサポートされるモジュール

Cisco IOS プラットフォーム	プラットフォームでサポートされるモジュール		
	NM-HDV2	NM-HD-1V NM-HD-2V NM-HD-2VE	NM-HDV NM-HDV-FARM
VG200 2600 3620 3640	なし	なし	あり
3660	なし	あり	あり
2600XM、2691、 3725、3745 2811、2821、2851 3825、3845	あり	あり	あり
2901、2911、2921、2951、 3925、3945、3925E、 3945E	あり	あり	なし

（注）　Cisco VG200、2620、2621、および 3620 は、NM-HDV-FARM をサポートせず、さらに MTP、会議、およびトランスコーディングもサポートしません。Cisco 2801 には NM スロットがありません。

保留音のキャパシティ プランニング

MoH リソースも、他のすべてのメディア リソースと同じように、ハードウェアを配置し、設定した後、予想されたネットワークのコール量を確実にサポートするために、キャパシティ プランニングが非常に重要です。このため、MoH リソースのハードウェア キャパシティを認識し、このキャパシティとの関連からマルチキャストとユニキャストの MoH の役割を考慮することが重要です。

共存 MoH サーバとスタンドアロン MoH

MoH 機能を利用するには、Unified CM クラスタに含まれているサーバを使用する必要があります。MoH サーバは、次のいずれかの方法で設定できます。

- 共存配置

  共存配置では、MoH 機能は Unified CM ソフトウェアも実行している、クラスタ内の任意のサーバ（パブリッシャまたはサブスクライバ）で実行されます。

  （注）　「*共存*」という用語は、同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態を指します。

- スタンドアロン配置

  スタンドアロン配置では、MoH 機能は Unified CM クラスタ内の専用サーバに置かれます。つまり、Cisco IP Voice Media Streaming Application サービスが、そのサーバ上で使用できる唯一のサービスとなります。この専用サーバの機能は、MoH ストリームをネットワーク内のデバイスに送信することだけです。

サーバ プラットフォームの最大同時セッション数

表 17-8 は、サーバ プラットフォームと、そのプラットフォームがサポートできる最大同時 MoH セッション数をリストしています。MoH セッションがこの最大同時セッション数を超えてから、さらに負荷が増えると、MoH 品質の低下、不規則な MoH 動作、または MoH 機能の喪失までも発生するおそれがあるので、ネットワークのコール量が最大同時セッション数を超えないようにしてください。

表 17-8　サーバ プラットフォーム タイプごとの最大 MoH セッション数

サーバ プラットフォーム	サポートされるコーデック	サポートされる MoH セッション数
MCS 7816 MCS 7825 MCS 7828	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロンサーバ： 250 MoH セッション[1]
MCS 7835 MCS 7845	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロンサーバ： 500 MoH セッション

1. Unified CM クラスタごとに最大 51 の固有オーディオ ソースを設定できます。

次の MoH サーバー設定パラメータは、MoH サーバのキャパシティに影響を与えます。

- **Maximum Half Duplex Streams**

  このパラメータにより、ユニキャスト MoH に配置できるデバイスの数が決まります。デフォルトでは、この値は 250 に設定されています。

  Maximum Half Duplex Streams パラメータは、次の公式から得られた値に設定する必要があります。

  （サーバーおよび配置キャパシティ）–（[マルチキャスト MoH ソースの数] * [有効な MoH コーデックの数]）

  次の例を参考にしてください。

MCS-7835 スタンドアロン MoH サーバ	マルチキャスト MoH オーディオ ソース	有効な MoH コーデック（G.711 mu-law と G.729）	**Maximum Half Duplex Streams**
500	- (12	* 2)	= **476**

  したがって、この例では、Maximum Half Duplex Streams パラメータは 476 未満の値で設定されます。

  このパラメータには、プラットフォームや配置タイプ（共存またはスタンドアロン）に基づいて、表 17-8 に示すキャパシティよりも大きい値を絶対に設定しないでください。

- **Maximum Multicast Connections**

  このパラメータにより、マルチキャスト MoH に配置できるデバイスの数が決まります。

  Maximum Multicast Connections パラメータは、必要に応じてすべてのデバイスを確実にマルチキャスト MoH に配置できるような数に設定する必要があります。MoH サーバが生成できるマルチキャスト ストリームは、有限ですが（最大 204）、多数の保留デバイスを各マルチキャスト ストリームに加えることができます。このパラメータは、同時にマルチキャスト MoH に配置される可能性のあるデバイスの数、またはそれよりも大きい数に設定する必要があります。一般的なマルチキャスト トラフィックは、生成されるストリームの数に基づいて決まりますが、Unified CM では、マルチキャスト MoH に実際に配置されたデバイスの数または各マルチキャスト MoH ストリームに結合されたデバイスの数が保持されます。この方式は、マルチキャスト トラフィックが通常トラッキングされる方法と異なりますが、このパラメータを適切に設定することが重要です。

  （注）　Unified CM クラスタごとに設定できる固有オーディオ ソースの上限は 51 で、MoH ストリームに使用可能なコーデックの上限は 4 つであるため、MoH サーバごとのマルチキャスト ストリームの最大数は 204 です。

これらのパラメータを適切に設定しないと、MoH サーバ リソースが十分に使用されない、またはサーバがネットワーク負荷を処理できないといった問題が発生する可能性があります。

（注）　表 17-8 にリストされている最大セッションの上限は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時セッションに適用されます。この上限は、トランスポート メカニズムに関係なく、プラットフォームがサポートできる推奨最大セッション数を示しています。

リソースのプロビジョニング

共存またはスタンドアロンの MoH サーバ設定のプロビジョニングを行う場合、ネットワーク管理者は、MoH オーディオ ストリームに使用されるトランスポート メカニズムのタイプを考慮する必要があります。ユニキャスト MoH を使用する場合、保留される各デバイスには、別々の MoH ストリームが必要です。しかし、マルチキャスト MoH と単一のオーディオ ソースのみを使用する場合、保留にするタイプのデバイス数に関係なく、設定されているコーデック タイプごとに必要な MoH ストリームは 1 つだけです。

たとえば、30,000 台の電話機のあるクラスタがあり、保留率が 2% である（すべてのエンドポイント デバイスの 2% だけが、常に保留になる）場合、600 の MoH ストリームまたはセッションが必要です。ユニキャスト専用の MoH 環境の場合、次の計算で示されているように、この負荷を処理するには、2 つの共存（またはスタンドアロン）MoH サーバが必要です。

[（MCS 7835 または 7845 共存サーバごとに 500 セッション）*（共存サーバ 1 台）] + [（MCS 7816、7825、または 7828 共存サーバごとに 250 セッション）*（共存サーバ 1 台）] > 600 セッション

一方、たとえば、36 の固有 MoH オーディオ ストリームがあるマルチキャスト専用 MoH 環境には、次の計算で示されているように、1 つの共存 MoH サーバ（MCS 7816、7825、または 7828）だけが必要です。

（MCS 7816、7825、または 7828 共存サーバごとに 250 セッション）*（共存サーバ 1 台）> 36 セッション

36 の固有マルチキャスト ストリームは、次のいずれかの方法でプロビジョニングできます。

- 単一のコーデックを使用して 36 の固有オーディオ ソースをストリーミングする。
- 2 つのコーデックだけを使用して 18 の固有オーディオ ソースをストリーミングする。

- 3 つのコーデックだけを使用して 12 の固有オーディオ ソースをストリーミングする。
- 4 つのコーデックすべてを使用して 9 つの固有オーディオ ソースをストリーミングする。

上記の例で示されているように、マルチキャスト MoH は、ユニキャスト MoH よりも、サーバ リソースを大幅に節約できます。

上記の例では、2% の保留率は、30,000 台の電話機に基づくものであり、保留になる可能性があるネットワーク内のゲートウェイまたはその他のエンドポイント デバイスを考慮していません。こうしたその他のデバイスは、電話機と同じように保留になる可能性があるので、保留率を計算するときは、これらのデバイスも考慮する必要があります。

上記の計算では、MoH サーバの冗長性を見込んでいません。MoH サーバに障害が発生する場合、またはユーザの 2% 以上が同時に保留になる場合、このシナリオでは、オーバーフローが発生したり負荷が増えたときに処理するための MoH リソースがありません。MoH リソースの計算には、冗長性に配慮して十分に余裕のあるキャパシティを含める必要があります。

メディア リソースのハイ アベイラビリティ

Unified CM のメディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）のコンストラクトは、この章で説明されているリソースの編成とアクセスの方法を制御するために使用されます。この項では、これらのコンストラクトを効率的に利用する方法について説明します。

メディア リソース グループとメディア リソース グループ リスト

メディア リソース グループとメディア リソース グループ リストは、リソースの割り当て方法を制御する方式を提供するもので、リソースに対するアクセス権、リソースの場所、特定のアプリケーションのリソース タイプなどが含まれます。この項では、読者がメディア リソース グループを理解しているものとして、次の設計上の考慮事項について詳しく説明します。

- システムは、ユーザ インターフェイスに表示されず、すべてのリソースが作成時にメンバーとなるデフォルト メディア リソース グループを定義します。メディア リソースの使用側は、まず、設定で指定されている任意のメディア リソース グループ（MRG）またはメディア リソース グループ リスト（MRGL）のリソースを使用します。必要なリソースが使用できない場合、デフォルト MRG でリソースが検索されます。単純な配置では、デフォルトの MRG だけを使用することがあります。
- MRG を使用してリソースへのアクセスを制御する場合は、リソースを明示的に別のグループに設定することによって、デフォルト MRG の外に移動する必要があります。すべてのコールに対する最後の手段としてのみリソースを使用できるようにする場合は、そのリソースをデフォルト グループに残しておくことができます。また、リソースの制御が必要ない場合も、デフォルト グループに残しておくことができます。
- MRG には、複数のタイプのリソースが含まれていることがあります。必要な機能に基づいて、適切なリソースがグループから割り当てられます。MTP とトランスコーダは、特別な例です。トランスコーダは MTP としても使用できます。
- MRG の用途の 1 つは、類似したタイプのリソースのグループ化です。カンファレンス ブリッジ リソースがサポートする参加者の数は異なります。MRG を使用して、カンファレンス ブリッジのサイズ別に会議リソースをグループ化できます。
- Media Resource Group（MRG; メディア リソース グループ）と Media Resource Group List（MRGL; メディア リソース グループ リスト）を使用して、複数の Unified CM 間でリソースを共有します。MRG と MRGL を使用しない場合、リソースは、1 つの Unified CM からしか使用できません。

- また、MRG と MRGL を使用すると、地理的なロケーションに基づいてリソースを分離できます。その結果、WAN 帯域幅を節約できる場合もあります。
- MRGL は、設定にリストされている順序で MRG を使用します。ある MRG に必要なリソースがない場合、次の MRG が検索されます。すべての MRG が検索され、リソースが見つからない場合、検索は終了します。
- MRG から類似のリソースを割り当てるアルゴリズムでは、類似したリソース間での負荷分散が試みられます。リソースが使用されると、その MRG のポインタは次のデバイスにインクリメントされます。1 つのデバイスが複数の MRG に存在することがあります。この場合、このデバイスがメンバーであるすべてのグループのポインタに影響を与えます。MTP が必要で、トランスコーダが同じグループに存在する場合、すべての MTP が使用されるまで、MTP が常に割り当てられます。すべての MTP が使用されると、トランスコーダが MTP として使用されます。同じグループにキャパシティの異なるリソースがある場合、ロード シェアリングはキャパシティに基づいてリソースを割り当てようとします。システムはリソース間で負荷を分散しますが、上記の要素により、動作がラウンドロビンになることはあまりありません。
- Unified CM Administration には MRG のデバイスがアルファベット順に表示されますが、割り当てられる順序は設定データベースの順序に基づきます。この順序は変更できません。メディア リソースを特定の順序で割り当てるには、リソースごとに別の MRG を作成し、MRGL を使用して割り当て順序を指定します。
- メディア リソース自身には、別のメディア リソースを呼び出さない設定が必要です。たとえば、MTP がコールに挿入され、この MTP で設定されているコーデックが、このコールに対して Unified CM が必要とするコーデックと異なる場合、トランスコーダも呼び出されます。よくある間違いは、Unified CM が G.729a を必要とする場合に、MTP を G.729 または G.729b に設定することです。

Cisco IOS ベースのメディア リソースの冗長性とフェールオーバーに関する考慮事項

メディア リソースに関するハイ アベイラビリティ設計には、冗長なメディア リソースを含める必要があります。これらのリソースが Cisco IOS ベースのリソースである場合は、単一プラットフォームの障害を防ぐために各リソースを複数の Cisco IOS プラットフォームに分散できます。また、各リソースを異なるプライマリ Unified CM サーバに登録することも可能です。

Cisco IOS は、フェールオーバー機能のモードとして「グレースフル」と「即時」の 2 種類をサポートしています。デフォルトのフェールオーバー方法はグレースフルで、この場合はすべてのメディア アクティビティが停止して初めてリソースがバックアップ Unified CM サーバに登録されます。それに対して即時フェールオーバーでは、プライマリの障害が検出されるとすぐにリソースがバックアップ Unified CM サーバに登録されます。冗長性のない 1 組のメディア リソースしかない状況では、即時フェールオーバーを使用することを推奨します。

保留音のハイ アベイラビリティ

完全な冗長性のある MoH 動作を確保するために複数の MoH サーバを設定し、配置することを推奨します。最初の MoH サーバに障害が発生したり、要求を処理するために必要なリソースがなくなったために使用不能になると、2 番めのサーバが自動的に MoH 機能を引き継ぎ、要求に応答します。適切な冗長構成のために、クラスタ内の 2 つ以上の MoH サーバから各 MRG にリソースを割り当ててください。

マルチキャストとユニキャストの両方の MoH が必要な環境では、ネットワーク内のすべてのエンドポイントの MoH 冗長性が確保されるように、必ず両方のトランスポート タイプに冗長性をもたせてください。

メディア リソースの設計に関する留意点

この項では、さまざまな Unified CM 展開モデルと一緒に使用するメディア リソースの設計に関する留意点について検討します。また、Unified CM 実装でのメディア リソース割り当てに関する堅牢なソリューションの設計に役立つ、設定上の留意点とベスト プラクティスについても取り上げます。

配置モデル

ここでは、MTP リソースとトランスコーディング リソースが、どこで、いつ使用されるかを説明します。具体的には、次の 3 つの企業 IP テレフォニー配置のモデルと、4 つめのアプリケーション シナリオで示します。

- 「単一サイト配置」（P.17-40）は、1 つのサイト内の 1 つ以上のコール処理エージェントから構成され、音声トラフィックは IP WAN を介して伝送されません。
- 「集中型コール処理を使用するマルチサイト WAN 配置」（P.17-40）は、IP WAN を通じて接続された複数のサイトにサービスを提供する、単一のコール処理エージェントから構成されます。
- 「分散型コール処理を使用するマルチサイト WAN 配置」（P.17-41）は、IP WAN を通じて接続される複数のリモート サイトのそれぞれに置かれている、コール処理エージェントから構成されます。

単一サイト配置

単一サイト配置では、低ビット レート（LBR）コーデックを使用する根拠となっている低速リンクが不要のため、トランスコーディングの必要はありません。H.323v2 に準拠していない相当数のデバイス（旧バージョンの Microsoft NetMeeting や特定のビデオ デバイスなど）が存在する場合、何らかの MTP リソースが必要なことがあります。SIP エンドポイントがある場合は、DTMF 変換用に MTP リソースが必要になることがあります（「Named Telephony Event（RFC 2833）」（P.17-16）を参照）。

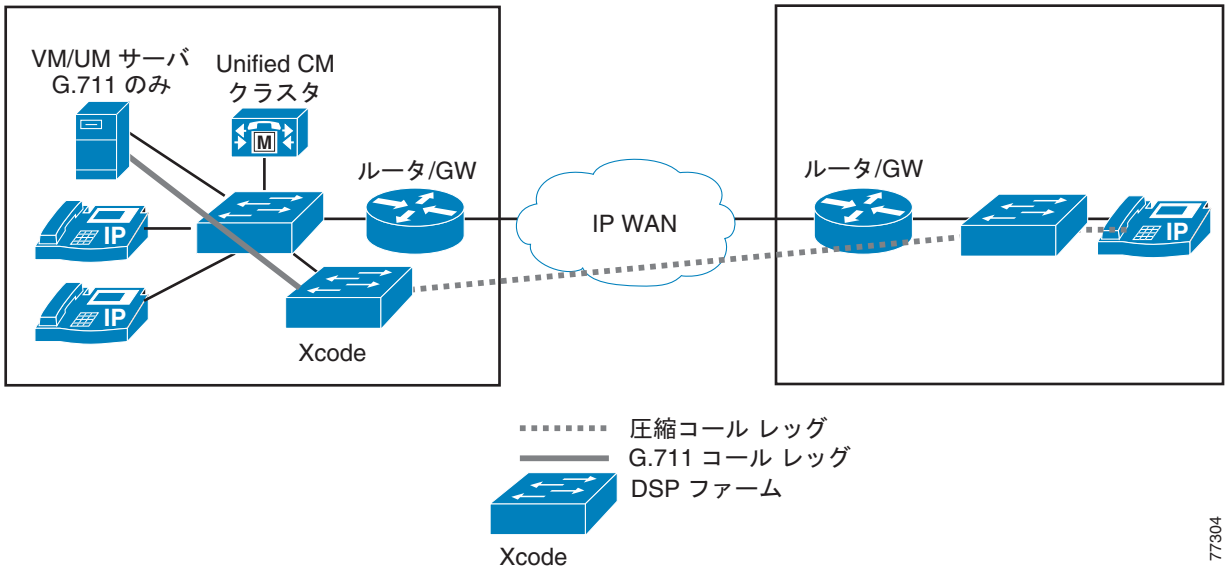
集中型コール処理を使用するマルチサイト WAN 配置

集中型コール処理配置では、Unified CM クラスタとアプリケーション（たとえば、ボイスメールや IVR）は、中央サイトに置かれ、複数のリモート サイトが IP WAN を介して接続されます。リモート サイトでは、コール処理に中央の Unified CM を使用します。

WAN 帯域幅は一般に制限されるので、WAN を通過するときは、G.729 などの低ビット レート コーデックを使用するようにコールが設定されます（図 17-6 を参照）。

IP Phone 間の音声圧縮は、Unified CM の *リージョン*と *ロケーション*を使用して簡単に設定されます。リージョンは、そのリージョン内のデバイスが使用する圧縮のタイプ（たとえば、G.711 または G.729）を指定します。ロケーションは、そのロケーションのデバイスに出入りするコールに使用可能な、合計帯域幅量を指定します。

図 17-6　　集中型コール処理を使用する WAN のトランスコーディング



Unified CM は、MRG（メディア リソース グループ）を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、異なるリージョンを通過するコールに LBR コーデック（たとえば、G.729a）を使用する場合、トランスコーディング リソースが使用されるのは、エンドポイントの一方（または両方）が、LBR コーデックを使用できない場合だけです。

図 17-6 では、Unified CM がトランスコーダが必要であることを認識し、高帯域幅コーデックを使用するデバイスの MRGL または MRG に基づいてトランスコーダを割り当てます。この場合、VM/UM サーバが、使用するトランスコーダ デバイスを決定します。この Unified CM の動作は、トランスコーダ リソースが高帯域幅デバイスの近くに正しく配置されていることを前提としています。VM/UM サーバ用のトランスコーダがリモート サイトに配置されるようにこのシステムが設計されていた場合、G.711 は WAN を経由して送信されるため、設計の意図が失われます。結果として、G.711 のみのデバイスを使用する複数のサイトがある場合に WAN で LBR が実行されていると、これらの各サイトがトランスコーダ リソースを必要とします。

その他のリソースの配置も重要です。たとえば、リモート サイトの 3 つの電話機で会議が発生し、会議リソースが中央（コール処理）サイトにある場合、3 つのメディア ストリームが WAN で伝送されます。会議リソースがローカルにあれば、コールは WAN を経由しません。WAN の帯域幅とコール アドミッション制御を設計するときは、この要素を考慮する必要があります。

分散型コール処理を使用するマルチサイト WAN 配置

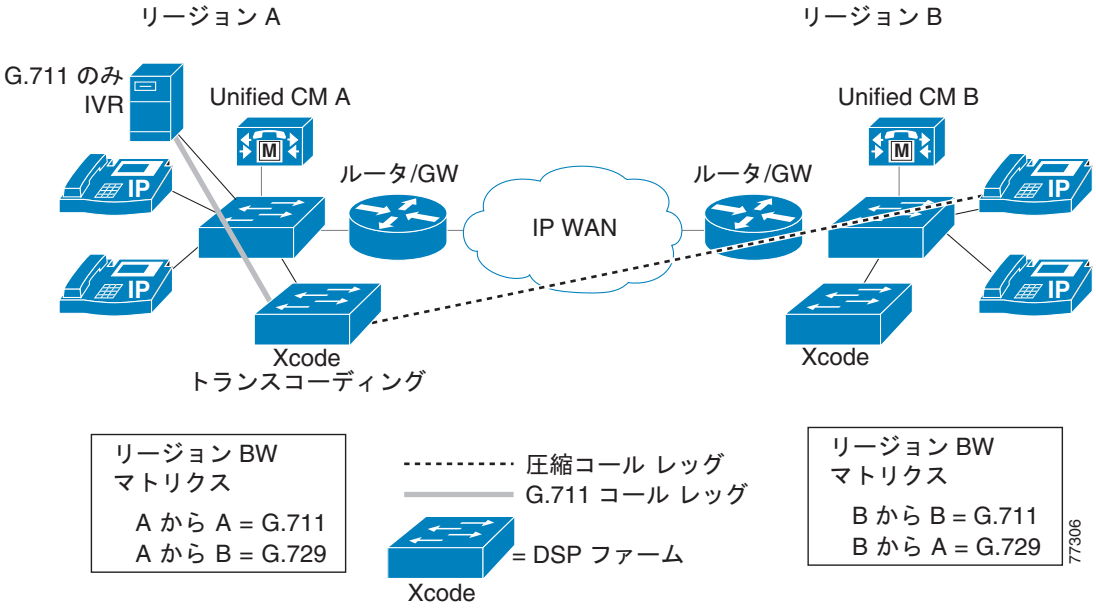
分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには Unified CM クラスタが含まれ、単一サイト モデルか、集中型コール処理モデルになります。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

WAN 帯域幅は一般に制限されているので、WAN を通過するときは、LBR コーデック（たとえば、G.729a）を使用するように、サイト間のコールが設定されていることがあります。H.323v2 クラスタ間トランクは、Unified CM クラスタの接続に使用されます。Unified CM は、ハードウェア MTP が使用される場合、MTP サービスを通じた圧縮音声コール接続もサポートします（図 17-7 を参照）。

次の状況では、分散型コール処理配置に、トランスコーディング サービスと MTP サービスが必要になる場合があります。

- 現行バージョンの Cisco アプリケーションを使用する場合は、トランスコーディング リソースの使用を回避できるため、回避することを推奨します。特別な例として、特定のデバイスの G.711 を回避できないことがあります。
- 一部のエンドポイント（たとえば、映像エンドポイント）が、H.323v2 機能をサポートしません。

図 17-7　トランスコーディングを使用したクラスタ間コール フロー



Unified CM は、MRG（メディア リソース グループ）を使用して、クラスタ内の Unified CM サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、クラスタ間トランクを介したコールの場合、MTP リソースとトランスコーディング リソースは、必要な場合だけ使用されます。したがって、LBR コーデックをサポートしないアプリケーションに対して MTP サービスを設定する必要がなくなります。

次の特性が、分散型コール処理配置に適用されます。

- トランスコーディングを必要とするクラスタ間コールだけが、MTP サービスを使用します。たとえば、コールの両方のエンドポイントが G.729 コーデックを使用できる場合、トランスコーディング リソースは使用されません。
- クラスタ内のサーバ間で MTP リソースを共有すると、リソースの使用効率が向上します。

メディアの機能と音声品質

メディアを操作するいずれのプロセスも、メディアの品質を低下させる可能性があります。たとえば、ネットワーク（IP または TDM）上で送信するための音声ストリームのエンコーディングと、相手側でのデコーディングは情報の損失を招き、結果として音声ストリームは元の音声を正確に再生しません。同じ音声ストリームの複数のエンコーディングおよびデコーディングの手順を含む、ネットワーク経由のメディア通過パスが存在する場合、エンコーディングおよびデコーディングの操作が繰り返されるたびに音声品質は低下していきます。通常、このようなパスは回避する必要があります。このことは特に、G.729 などの Low-bandwidth Codecs（LBC; 低帯域幅コーデック）に当てはまります。G.729 にはすでに低い Mean Opinion Score（MOS; 平均オピニオン評点、音声品質の主観的評価）が付いているので、エンコーディングとデコーディングの操作の繰り返しによってこの評点はただちに、許容できない品質まで低下します（詳細については、http://www.cisco.com で「Mean Opinion Score」を参照してください）。

このようなパスが回避できない場合には、G.711 または G.722 コーデックなどの帯域幅が比較的高く、低圧縮のコーデックを使用することによって通常、音声品質を向上させることができます。このようなパスが予想される場合には、これらのコーデックの使用を推奨します。このようなシナリオで、低帯域幅で高圧縮のコーデックを使用することは推奨できません。

保留音の設計に関する留意点

ここでは、堅牢な MoH ソリューションの設計に役立つ、MoH 設定上の考慮事項とベスト プラクティスについて説明します。

コーデックの選択

MoH 配置に複数のコーデックが必要な場合、CM Service Parameters Configuration の IP Voice Streaming Media App サービス パラメータでコーデックを設定します。Clusterwide Parameters の下の Supported MoH Codecs リストの中から、MoH ストリームに許可する、必要なコーデック タイプをすべて選択してください。デフォルトでは、G.711 mu-law のみが選択されています。別のコーデック タイプを選択するには、リストをスクロールさせて該当するコーデックをクリックしてください。複数選択する場合は、CTRL キーを押したまま、マウスを使用して、リストをスクロールさせて複数のコーデックを選択します。選択終了後、Update ボタンをクリックしてください。

MoH イベントに使用される実際のコーデックは、MoH サーバおよび保留にされるデバイス（IP Phone、ゲートウェイなど）のリージョン設定によって決まります。したがって、適切なリージョン設定（デバイス プール設定の下にあります）を MoH サーバに割り当て、必要なリージョンの関係を設定して、MoH インタラクションのコーデック選択を制御します。

（注）　MoH オーディオ ストリームに G.729 コーデックを使用する場合、このコーデックは会話用に最適化されているので、音楽用としては最低限のオーディオ品質であることに注意してください。

マルチキャスト アドレッシング

マルチキャスト MoH を設定するには、適切な IP アドレッシングが重要です。IP マルチキャストのアドレス範囲は 224.0.1.0 ～ 239.255.255.255 です。しかし、IANA（Internet Assigned Numbers Authority）は、公衆マルチキャスト アプリケーション用に 224.0.1.0 ～ 238.255.255.255 の範囲のアドレスを割り当てています。公衆マルチキャスト アドレスを MoH に使用しないことを強く推奨します。

代わりに、プライベート ネットワーク上の管理制御アプリケーション用に予約されている、239.1.1.1 ～ 239.255.255.255 の範囲内の IP アドレスを使用するように、マルチキャスト MoH オーディオ ソースを設定することを推奨します。

さらに、次の理由で、ポート番号ではなく、IP アドレスでインクリメントするように、マルチキャスト オーディオ ソースを設定することも必要です。

- 保留にされた IP Phone は、ポート番号ではなく、マルチキャスト IP アドレスに加わる。

  Cisco IP Phone には、マルチキャスト ポート番号という概念はありません。したがって、特定のオーディオ ストリームに対して設定されているすべてのコーデックが、同じマルチキャスト IP アドレス（別々のポート番号であっても）に送信される場合、1 本のストリームしか必要ない場合であっても、すべてのストリームが IP Phone に送信されます。IP Phone は 1 本の MoH ストリームしか受信できないので、不必要なトラフィックでネットワークが飽和状態になる可能性があります。

- IP ネットワーク ルータは、ポート番号ではなく、IP アドレスに基づいて、マルチキャストをルーティングする。

  ルータには、マルチキャスト ポート番号という概念はありません。したがって、同じマルチキャスト グループ アドレス（別々のポート番号であっても）に送信される複数のストリームを検出すると、ルータは、そのマルチキャスト グループのすべてのストリームを転送します。必要なストリームは 1 本だけなので、ネットワーク帯域幅が過剰に利用され、その結果、ネットワークの輻輳が発生する可能性があります。

MoH オーディオ ソース

オーディオ ソースは、Unified CM クラスタ内のすべての MoH サーバ間で共有されるため、各オーディオ ソース ファイルはクラスタ内の各 MoH サーバにアップロードしておく必要があります。クラスタごとに最大 51 の固有オーディオ ソースを設定できます（50 のオーディオ ファイル ソースと、サウンド カードを介した 1 つの固定/ライブ ソース）。追加のソースを提供する方法については、「複数の固定またはライブ オーディオ ソースの使用」（P.17-44）および「支社ルータからのマルチキャスト MoH」（P.17-49）の項を参照してください。

マルチキャストストリームに使用する、これらのオーディオ ソースには、[Allow Multicasting] と [Play continuously (repeat)] を必ず有効にしてください。オーディオ ソースの連続再生を指定していない場合、MoH オーディオ ソースは、最初の保留にされた通話者のみが受け取り、追加された通話者は受け取りません。

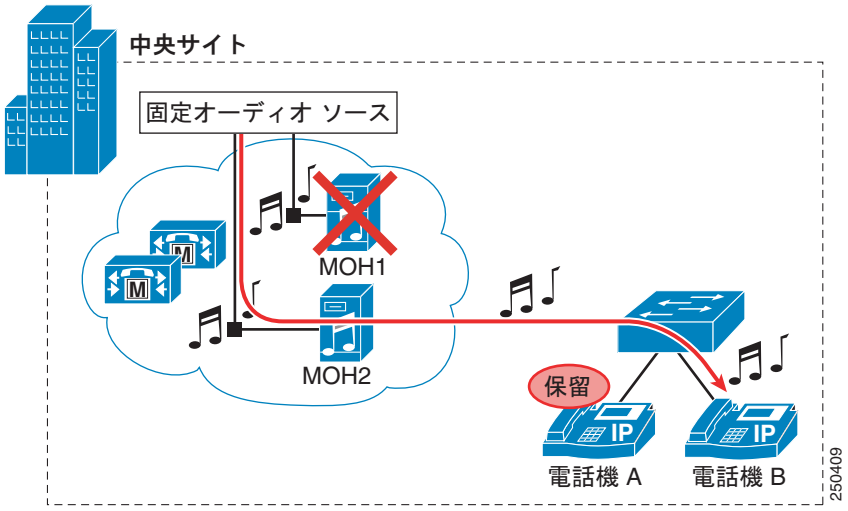
複数の固定またはライブ オーディオ ソースの使用

Unified CM では、1 つのオーディオ ソースのみ設定できることに留意することが重要です。ただし、Unified CM クラスタ内の各 MoH サーバは、Cisco MoH USB オーディオ サウンド カード（MOH-USB-AUDIO）を使用して、1 つの固定オーディオ ソースをストリーミングできます。複数の固定オーディオ ソースが必要な場合、追加の MoH サーバを追加して、これら複数のソースを提供できます。各 MoH サーバのサウンド カードには、同じ、または別のオーディオを提供できます。管理者は、MRG および MRGL の選択に基づいて、どの MoH サーバを選択するかを決定できます。複数のオーディオ ソースがこの方式で設定された場合、保留側の [User/Network Hold MoH Audio Source] は、固定オーディオ ソース（Unified CM に設定された 1 つの固定オーディオ ソース）に設定する必要があります。次に、被保留側の MRGL がその固定オーディオ ソースをデバイスにストリームする MoH サーバを決定します。

オーディオ ソースが同じ場合、この方式は固定オーディオ ソースの冗長性にも備えています。たとえば、図 17-8 には、2 つの MoH サーバがあり、それぞれは、ラジオ局のライブ フィードからのオーディオをストリームするオーディオ ソースに接続された MOH-USB-AUDIO サウンド カードを備えています。電話機 B の MRGL には、まず MOH1 サーバを含む MRG が、次に MOH2 サーバを含む

MRG が含まれます。電話機 A のユーザ/ネットワーク保留オーディオ ソースが固定オーディオ ソースに設定されているときに、コールが電話機 A と電話機 B の間で確立され、電話機 B が電話機 A によって保留にされた場合、電話機 B は、MOH1 サーバからライブ フィード オーディオ ソースを受信します。MOH1 サーバがダウンしている（または利用可能なキャパシティがない）ときに、電話機 A が電話機 B を保留にすると、電話機 B は MOH2 サーバからライブ フィード オーディオ ソースを受信します。

図 17-8　　固定オーディオ ソース冗長性の例



（注）　マルチキャスト オーディオ ソースとしてラジオのライブ ブロードキャストを使用すると、法律上の問題が発生するおそれがあります。起こりうる問題については、貴社の法務部門に相談してください。

同一 Unified CM クラスタ内のユニキャストとマルチキャスト

管理者は、1 つの Unified CM クラスタでユニキャストとマルチキャスト両方の MoH ストリームを処理するように設定できます。この設定が必要なのは、マルチキャストをサポートしないデバイス、またはエンドポイントがテレフォニー ネットワークに含まれている場合、あるいはネットワークの一部でマルチキャストが使用可能になっていない場合です。

クラスタがユニキャストとマルチキャストの両方の MoH オーディオ ストリームをサポートできるようにするには、次のいずれかの方法を使用してください。

- 別々の MoH サーバを配置します。一方のサーバをユニキャスト MoH サーバとして設定し、もう一方のサーバをマルチキャスト MoH サーバとして設定します。
- 2 つのメディア リソース グループ（MRG）を備えた 1 台の MoH サーバを配置します。各グループには同じ MoH サーバが含まれますが、1 つの MRG はオーディオストリームはマルチキャスト用に設定し、もう 1 つはユニキャスト用に設定します。

どちらの場合も、少なくとも 2 つの MRG、および少なくとも 2 つのメディア リソース グループ リスト（MRGL）を設定する必要があります。ユニキャスト MoH を必要とするエンドポイントには、1 つのユニキャスト MRG と 1 つのユニキャスト MRGL を設定します。同様に、マルチキャスト MoH を必要とするエンドポイントには、1 つのマルチキャスト MRG と 1 つのマルチキャスト MRGL を設定します。

別々の MoH サーバを配置する場合、一方のサーバをマルチキャスト無効（ユニキャスト専用）に設定し、もう一方の MoH サーバをマルチキャスト有効に設定してください。ユニキャスト専用 MoH メディア リソースとマルチキャスト使用可能 MoH メディア リソースを、ユニキャスト MRG とマルチキャスト MRG にそれぞれ割り当てます。マルチキャスト MRG には [Use Multicast for MoH Audio] ボックスにチェックマークが付き、ユニキャスト MRG にはチェックマークが付いていないことを確認してください。また、これらのユニキャスト MRG とマルチキャスト MRG をそれぞれの MRGL に割り当てます。この場合、MRG がマルチキャストを使用するように設定されているかどうか、また MoH ストリームを流す元のサーバに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

単一の MoH サーバをユニキャスト MoH とマルチキャスト MoH の両方に対して配置する場合は、サーバをマルチキャスト用に設定します。同じオーディオ ソースをユニキャスト MRG とマルチキャスト MRG の両方に割り当て、マルチキャスト MRG に対して [Use Multicast for MoH Audio] ボックスにチェックマークを付けます。この場合は、MRG がマルチキャストを使用するように設定されているかどうかだけで、MoH ストリームがユニキャストかマルチキャストかが決まります。

（注）　ユニキャスト MRG を設定する場合は、混乱しないようにしてください。これは、MoH メディア リソースをユニキャスト MRG に追加する場合であっても、リソース名の最後に、[Multicast] が追加されるからです。このラベルは、リソースがマルチキャスト対応であるという単なる表示です。リソースがユニキャストとして送信されるか、マルチキャストとして送信されるかを決定するのは、[Use Multicast for MoH Audio] ボックスのチェックの有無です。

さらに、適切な MRGL を使用するように、個々のデバイスまたはデバイス プールを設定する必要があります。1 つまたは複数のデバイス プールにすべてのユニキャスト デバイスを含め、ユニキャスト MRGL を使用するようにこれらのデバイス プールを設定できます。あるいは、1 つまたは複数のデバイス プールにすべてのマルチキャスト デバイスを含め、マルチキャスト MRGL を使用するようにこれらのデバイス プールを設定することもできます。オプションとして、該当するユニキャスト MRGL またはマルチキャスト MRGL を使用するように、個々のデバイスを設定できます。最後に、個々のデバイス、または（電話デバイスの場合）個々の回線かディレクトリ番号ごとに、ユーザ保留オーディオ ソースおよびネットワーク保留オーディオ ソースを設定して、適切なオーディオ ソースを割当ます。

マルチキャスト MoH とユニキャスト MoH の両方を同じクラスタに配置する方法を選択する場合は、必要なサーバの数を考慮することが重要です。単一の MoH サーバをユニキャストとマルチキャストの両方に使用すると、クラスタ全体に必要な MoH サーバの数が減ります。マルチキャスト MoH サーバとユニキャスト MoH サーバを別々に配置すると、クラスタ内に必要なサーバの数が明らかに増えます。

Quality of Service（QoS）

時間に依存する重要なリアルタイム アプリケーション（音声など）に遅延または損失がないように、1 つのネットワーク上のデータと音声のコンバージェンスには、適切な QoS が必要です。音声トラフィック用の適切な QoS を確保するには、ストリームがネットワークに入り、通過するときに、ストリームのマーク付け、分類、およびキューイングを行って、音声ストリームを重要度の低いトラフィックよりも優先的に処理する必要があります。MoH サーバは、DSCP（Differentiated Services Code Point）値 46 または PHB（Per Hop Behavior）値 EF（ToS 値 0xB8 に相当）を使用して、オーディオ ストリーム トラフィックに、音声ベアラトラフィックと同じマークを自動的に付けます。したがって、ネットワーク上で QoS が適切に設定されている限り、MoH ストリームは、音声 RTP メディア トラフィックとして分類され、プライオリティ キューイングとして扱われます。

MoH サーバと Unified CM サーバ間のコール シグナリング トラフィックは、デフォルトで DSCP 値 24 または PHB 値 CS3（ToS of 0x60 に相当）を使用して自動的にマーキングされます。したがって、ネットワーク上で、QoS が適切に設定されている限り、他のすべてのコール シグナリングと同様、ネットワーク内で、このコール シグナリング トラフィックは、適切に分類されキューに入れられます。

コール アドミッション制御と MoH

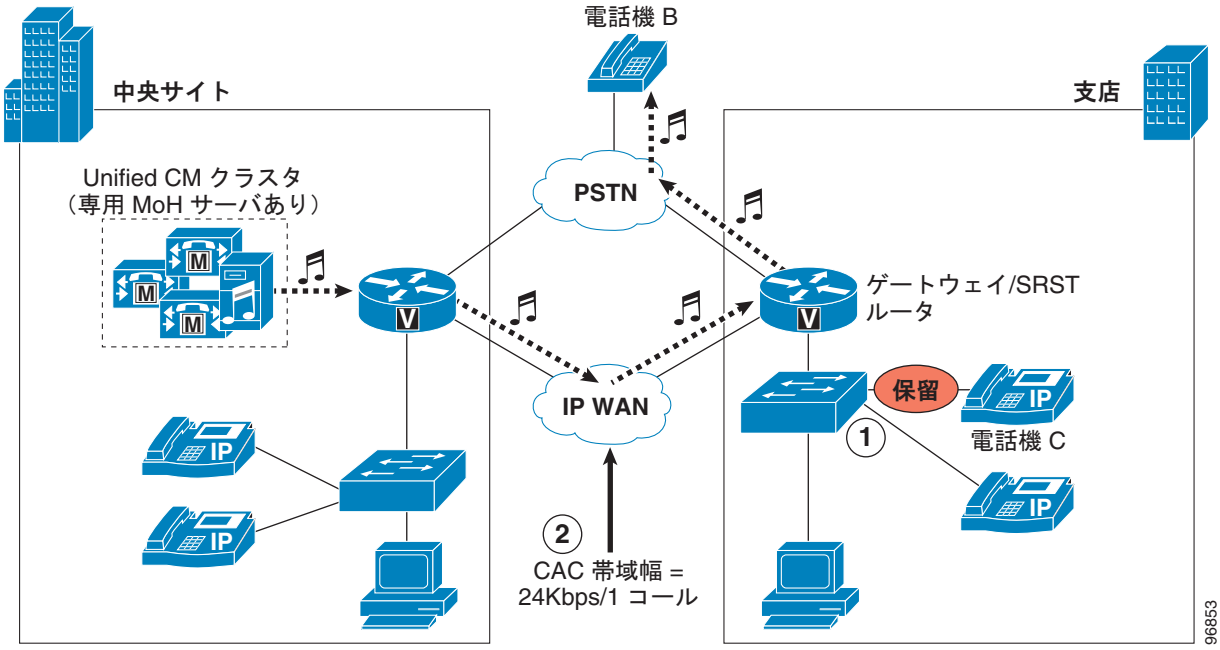
IP テレフォニー トラフィックが WAN リンク上を流れる場合は、コール アドミッション制御（CAC）が必要です。このようなリンク上では使用可能な帯域幅が制限されているので、適切なコール アドミッション制御がないと、音声メディア トラフィックの遅延または損失が起きる可能性が高くなります。詳細については、「コール アドミッション制御」（P.11-1）を参照してください。

Unified CM の（静的ロケーションまたは RSVP 対応ロケーションのいずれかに基づく）コール アドミッション制御は、WAN を通過するユニキャスト MoH ストリームをトラッキングできますが、マルチキャスト MoH ストリームはトラッキングできません。したがって、WAN 帯域幅が完全にサブスクライブされた場合であっても、マルチキャスト MoH ストリームは、コール アドミッション制御によって WAN へのアクセスを拒否されません。ストリームは WAN を介して送信され、その結果、オーディオ ストリームの品質が低下し、WAN を通過するその他のすべてのコールの品質も低下する可能性があります。マルチキャスト MoH ストリームがこのオーバーサブスクリプション状態にならないようにするには、帯域幅を追加して Low-Latency Queuing（LLQ）音声プライオリティ キューを設定することによって、すべてのダウンストリーム WAN インターフェイス上で QoS 設定を余分にプロビジョニングする必要があります。MoH ストリームは単方向であるため、ダウンストリーム インターフェイス（中央サイトからリモート サイトへ）の音声プライオリティ キューのみを余分にプロビジョニングする必要があります。WAN リンクを通過する可能性があるすべての固有マルチキャスト MoH ストリームに対して、十分な帯域幅を追加してください。たとえば、4 つの固有マルチキャスト オーディオ ストリームが WAN を通過する可能性がある場合、音声プライオリティ キューに 96 Kbps を追加します（4 * 24 Kbps（G.729 オーディオ ストリームごと）= 96 Kbps）。

図 17-9 は、集中型マルチサイト配置におけるコール アドミッション制御と MoH の例を示しています。この例の場合、IP Phone C が公衆網電話機（電話機 B）とコール中であると想定します。この時点では、WAN 上で帯域幅は消費されていません。電話機 C で [Hold] ソフトキーを押すと（ステップ 1）、電話機 B は、WAN を介して中央サイトの MoH サーバから MoH ストリームを受信するので、リンク上の帯域幅を消費します。コール アドミッション制御でこの帯域幅を考慮すべきかどうかは、MoH ストリームのタイプに応じて決まります。マルチキャスト MoH が流れる場合、コール アドミッション制御は、24 Kbps が消費されているとは見なしません（したがって、ダウンストリーム WAN インターフェイス上の QoS はそれに応じてプロビジョニングされなければなりません）。しかし、ユニキャスト MoH が流れる場合、コール アドミッション制御は、使用可能な WAN 帯域幅から 24 Kbps を差し引きます（ステップ 2）。

（注）　上記の例では、ユニキャスト MoH を WAN 上で流すことを示唆しているように見えますが、これは、MoH とのロケーションベースのコール アドミッション制御をわかりやすく示すための例に過ぎません。また、この設定の推奨または保証を意味するものではありません。前述のように、WAN を介した MoH オーディオ ストリームの送信用のトランスポート メカニズムには、マルチキャスト MoH を推奨します。

図 17-9　ロケーションベースのコール アドミッション制御と MoH



保留音の配置モデル

各種 Unified Communications コール処理配置モデルにより、MoH の構成設計にはさらに考慮事項が発生します。配置モデルの選択が、MoH のトランスポート メカニズム（ユニキャストまたはマルチキャスト）、リソースのプロビジョニング、およびコーデックの決定に影響を与える場合があります。ここでは、各種配置モデルに関連した問題について説明します。

配置モデルの詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

単一サイト キャンパス（すべての配置に関連）

単一サイト キャンパス配置は、通常、LAN インフラストラクチャに基づくものであり、大量のトラフィックに対して十分な帯域幅が用意されています。LAN インフラストラクチャでは一般に帯域幅が制限されないので、単一サイト配置内のすべての MoH オーディオ ストリームには、G.711（A-law または mu-law）コーデックの使用を推奨します。G.711 は、IP テレフォニー環境に、最適な音声と音楽のストリーミング品質を提供します。

MoH サーバの冗長性も考慮する必要があります。MoH サーバが過負荷になるか、使用不能になった場合でも、複数の MoH サーバを設定し、それらのサーバを優先順に MRG に割り当てておくと、別のサーバが制御を引き継いで、MoH ストリームを流すことができます。

ネットワーク テクノロジーの多様性が増すにつれて、大規模な単一サイト キャンパスでは、一部のエンドポイント デバイスまたはネットワーク領域がマルチキャストをサポートできなくなる可能性があります。このため、ユニキャストとマルチキャストの両方の MoH リソースを配置する必要があります。詳細については、「同一 Unified CM クラスタ内のユニキャストとマルチキャスト」（P.17-45）の項を参照してください。

オフネット コールとアプリケーション処理コールが、保留時に期待された MoH ストリームを受け取るには、適切な MRGL とオーディオ ソースを使用してすべてのゲートウェイとその他のデバイスを設定するか、それらを適切なデバイス プールに割り当ててください。

集中型マルチサイト配置

集中型コール処理を使用するマルチサイト IP テレフォニー配置には、一般的に、中央以外の複数のサイトとの WAN 接続が含まれます。これらの WAN リンクは、通常、帯域幅とスループットの障害になります。これらのリンク上での帯域幅使用量を最小限にするには、WAN を通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することを推奨します。G.729 コーデックは、音楽アプリケーションではなく、音声用に最適化されています。したがって、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN 上でのみ、G.729 を使用してください。さらに、マルチキャスト トラフィックにより、帯域幅を大幅に節約できるので、WAN を介してエンドポイントにオーディオを流す場合は、常にマルチキャスト MoH を使用する必要があります。

WAN を介して G.729 を使用するときに MoH ストリームの音声品質が問題になる場合は、WAN を介した MoH オーディオ ストリームに G.711 コーデックを使用し、音声コールには引き続き G.729 を使用します。WAN を介した MoH ストリームの送信に G.711 コーデックを使用し、WAN を介した音声コールの送信に G.729 コーデックを使用するには、Unified CM リージョンにすべての MoH サーバだけを配置し、そのリージョンが他のリージョンとの間で G.711 を使用するように設定します。この設定により、WAN の一方の側にある 2 つの電話機間でコールを発信するときは、それぞれのリージョンの間で G.729 コーデックが使用されます。ただし、一方の通話者がコールを保留にした場合、MoH オーディオ ストリームは G.711 を使用して符号化されます。これは、G.711 が、MoH サーバのリージョンと、保留にされた電話機のリージョンとの間で使用するコーデックとして設定されているためです。

支社ルータからのマルチキャスト MoH

Cisco Unified Survivable Remote Site Telephony（SRST）機能を使用して配置された支社ルータは、支社の SRST ルータのフラッシュ、またはアナログ ポートに接続されているライブ フィードからの MoH ストリーミングを使用して、リモート サイトや支社サイトでマルチキャスト MoH を提供できます。これらの 2 つの方式によって支社のルータから MoH をマルチキャストすると、Cisco Unified Communications MoH の機能が次のシナリオの両方において向上します。

- 非フォールバック モード

  WAN が稼動中で、電話機が Unified CM で制御されている場合、この設定では、ローカルに発信される MoH を提供し、WAN を介してリモート支社サイトに MoH を転送する必要がなくなります。

- フォールバック モード

  SRST がアクティブで、支社のデバイスが中央サイトの Unified CM との接続を失った場合、支社のルータが継続して MoH をマルチキャストします。

いずれかのシナリオでライブ フィード オプションを使用している場合、ライブ フィードの入力をモニタすることにより、SRST ルータでは冗長性が確保され、ライブ フィードの接続が切断されても、フラッシュ内のファイルから MoH をストリームするようになります。マルチキャスト MoH を流す際に使用できるマルチキャスト アドレスとポート番号は、SRST ルータごとに 1 つのみです。このため SRST ルータではライブフィードとフラッシュ ファイルの両方からのストリーミングを同時に実行することはできません。また、SRST ルータでは、フラッシュから流すことのできるオーディオ ファイルは 1 つのみです。

（注）　SRST 機能が実際に使用されるかどうかに関係なく、SRST ライセンスが必要です。ライセンスが必要なのは、支社ルータのフラッシュから MoH を流すための設定が SRST コンフィギュレーション モードで行われるため、および SRST 機能が使用されない場合でも少なくとも 1 つの **max-ephones** と 1 つの **max-dn** を設定する必要があるためです。

非フォールバック モード

非フォールバック モード中（WAN が稼動していて、SRST がアクティブでない場合）、支社の SRST ルータは、マルチキャスト MoH をすべてのローカル Cisco Unified Communications デバイスに流すことができます。これを実現するには、支社ルータ上で設定された内容と同じマルチキャスト IP アドレスとポート番号をもつオーディオ ソースを使用して、Unified CM MoH サーバを設定する必要があります。このシナリオでは、マルチキャスト MoH オーディオ ストリームが、常に SRST ルータから発信されるので、中央サイトの MoH サーバのオーディオ ソースが WAN を通過する必要はありません。

中央サイトのオーディオ ストリームが WAN を通過しないようにするには、次のいずれかの方法を使用してください。

- 最大のホップ カウントを設定する

  中央サイトの MoH オーディオ ソースが、中央サイトの LAN より先に流れないように、最大ホップ カウントまたは TTL を十分に小さく設定します。

- WAN インターフェイス上で Access Control List（ACL; アクセス コントロール リスト）を設定する

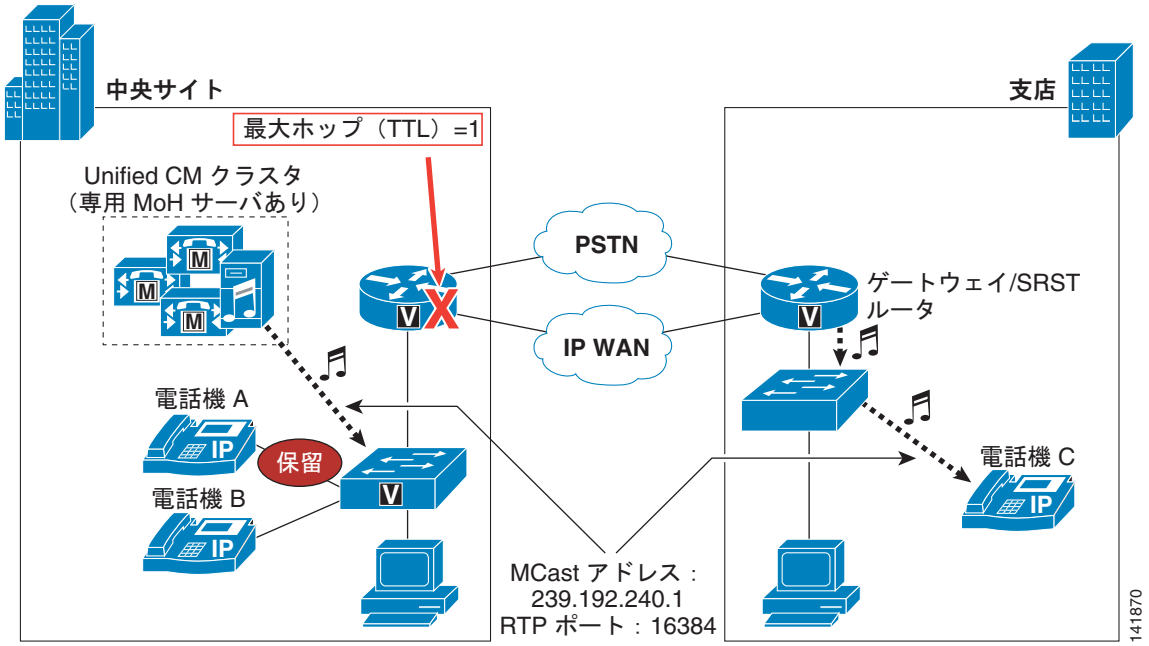
  中央サイトの WAN インターフェイス上で ACL を設定して、マルチキャスト グループ アドレス宛のパケットがインターフェイスから発信されないようにします。

- WAN インターフェイス上でマルチキャスト ルーティングを無効にする

  WAN インターフェイス上ではマルチキャスト ルーティングを設定しないでください。設定しなければ、マルチキャスト ストリームが WAN に転送されないことが保証されます。

図 17-10 は、フォールバック モードでないときに支社のルータからマルチキャスト MoH を流す仕組みを示しています。電話機 A で電話機 C を保留にすると、電話機 C は、ローカル SRST ルータからマルチキャスト MoH を受信します。この図では、MoH サーバは、（RTP ポート 16384 上で）239.192.240.1 にマルチキャスト オーディオ ソースを流します。しかし、最大ホップ数が 1 に制限されているので、このストリームは、ローカル MoH サーバのサブネットから WAN を通過して外に出ないことが保証されています。同時に、支社の SRST ルータまたはゲートウェイは、フラッシュまたはライブ フィードからオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.192.240.1 を使用し、RTP ポート番号として 16384 を使用します。電話機 A で [Hold] ソフトキーを押すと、電話機 C は、SRST ルータから発信された MoH オーディオ ストリームを受信します。

図 17-10　支社ルータのフラッシュからのマルチキャスト MoH



この方法を使用してマルチキャスト MoH を配信する場合は、Unified CM クラスタ内のすべてのデバイスが、同じユーザ保留およびネットワーク保留オーディオ ソースを使用するように設定し、すべての支社ルータに同じマルチキャスト グループ アドレスとポート番号を設定します。保留側のユーザまたはネットワーク保留オーディオ ソースは、オーディオ ソースを特定するときに使用されるため、クラスタ内に複数のユーザまたはネットワーク保留オーディオ ソースを設定する場合、リモートの被保留側が常にローカルの MoH ストリームを受信することを保証する手段はありません。たとえば、中央サイトの電話機に設定されているオーディオ ソースが、そのユーザおよびネットワーク保留オーディオ ソースとして、グループ アドレス 239.192.254.1 を使用するものとします。この電話機がリモート デバイスを保留にすると、ローカル ルータのフラッシュの MoH ストリームがマルチキャスト グループ アドレス 239.192.240.1 に送信される場合でも、リモート デバイスは 239.192.254.1 に加わろうとします。代わりに、ネットワーク内のすべてのデバイスがマルチキャスト グループ アドレス 239.192.240.1 でユーザ/ネットワーク保留オーディオ ソースを使用するように設定し、すべての支社ルータが 239.192.240.1 でフラッシュからマルチキャストするように設定すると、リモート デバイスはすべて、そのローカル ルータから MoH を受信します。

マルチキャスト MoH を流すように設定された複数の支社ルータを含むネットワークでは、Unified CM クラスタ内に 51 を超える固有 MoH オーディオ ソースを含めることができます。支社サイトの各ルータは、固有オーディオ ソースをマルチキャストできます。ただし、すべてのルータが同じマルチキャスト グループ アドレス上でこのオーディオをマルチキャストする必要があります。また、中央サイトの MoH サーバは、この同じマルチキャスト グループ アドレス上で MoH ストリームをマルチキャストできます。したがって、100 の支社サイトそれぞれがオーディオをマルチキャストする場合、クラスタには 実際には 101 の固有 MoH オーディオ ソース（100 の支社ストリームと 1 つの中央サイト ストリーム）が含まれることになります。中央サイトで 51 を超える固有オーディオ ストリームが必要な場合は、「複数の固定またはライブ オーディオ ソースの使用」（P.17-44）で説明されている方法を参照してください。

フォールバック モード

フォールバック モード中（WAN がダウンしていて SRST がアクティブな場合）、支社の SRST ルータはシャーシ内のすべてのアナログ ポートとデジタル ポートに、マルチキャスト MoH を流すことができます。これによりアナログ電話機および公衆網電話機に MoH を流すことができます。

支社のルータに対して、フォールバック モードのマルチキャスト MoH を設定する方法は、通常の設定方法と同じです。ただし、ルータに対して設定するマルチキャスト アドレスは、目的の動作によって異なります。支社のルータから、デバイスにマルチキャスト MoH をフォールバック モードでのみ流す必要がある場合（たとえば、リモート デバイスで受信する MoH が非フォールバック モード中に中央サイトの MoH サーバから発信される場合）、SRST ルータに設定したマルチキャスト アドレスとポート番号が、中央サイトの MoH サーバのいずれのオーディオ ソースと重複しないようにする必要があります。重複していると、リモート デバイスは、設定されているユーザ/ネットワーク保留オーディオ ソースに応じて、ローカル ルータのフラッシュから MoH を継続的に受信することがあります。

支社の SRST/ゲートウェイ ルータに、マルチキャスト MoH を設定すると、ルータはフォールバック モードでないときにも、MoH ストリームのマルチキャストを継続することに注意してください。

フォールバック モードを設定して、Cisco Unified Communications Manager Express（Unified CME）を SRST モードで使用することもできます。フォールバック モードの動作は同じですが、コンフィギュレーション コマンドが多少異なります。SRST コマンドは、Cisco IOS **call-manager-fallback** コンストラクトで入力しますが、SRST モードの Unified CME では、コマンドは **telephony-service** で入力します。

SRST を介して MoH をマルチキャストする方法は 4 つあります。

- 支社ルータのフラッシュからの SRST マルチキャスト MoH
- ライブ フィードからの SRST マルチキャスト MoH
- SRST モードの Unified CME での支社ルータ フラッシュからのマルチキャスト MoH
- SRST モードの Unified CME でのライブ フィードからのマルチキャスト MoH

Cisco Unified SRST と Unified CME の設定方法については、次のマニュアルを参照してください。

- 次のサイトで入手可能な『*Cisco Unified SRST System Administrator Guide*』

  http://www.cisco.com/en/US/products/sw/voicesw/ps2169/products_installation_and_configuration_guides_list.html

- 次の Web サイトで入手可能な『*Cisco Unified Communications Manager Express System Administrator Guide*』

  http://www.cisco.com/en/US/products/sw/voicesw/ps4625/products_installation_and_configuration_guides_list.html

分散型マルチサイト配置

分散型コール処理を使用するマルチサイト IP テレフォニー配置には、通常、サイト間の WAN または MAN 接続が含まれます。これらの低速リンクは、通常、帯域幅とスループットの障害になります。リンク上での帯域幅使用量を最小限にするには、リンクを通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することを推奨します。ただし G.729 コーデックは、音楽用ではなく、音声用に最適化されているので、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN/MAN 上でのみ、G.729 を使用してください。

集中型マルチサイト配置の場合とは異なり、WAN を介して流れる MoH オーディオ ストリーム用に G.711 が必要になる可能性がある状況では、分散型マルチサイト環境で MoH オーディオ ストリームが G.711 を使用するように強制することはできません。MoH サーバが別の Unified CM リージョンに配置されている状況で、このリージョンとクラスタ間トランクまたは SIP トランクのリージョンとの間で G.711 コーデックが設定されている場合でも、2 つのクラスタ間のコールが一方の電話機によって保留

にされたときは、元の音声コールのコーデックが保持されます。これらのクラスタ間コールは、一般に、帯域幅の節約のために G.729 を使用して符号化されるため、一方のクラスタからの MoH ストリームも G.729 を使用して符号化されます。

もう 1 つのオプションでは、マルチキャスト MoH を Intercluster Trunk（ICT; クラスタ間トランク）または SIP トランク経由でクラスタ間コールにプロビジョニングします。これにより、1 つの Unified CM クラスタ内のエンドポイントで別の Unified CM クラスタからストリーミングされたマルチキャスト MoH を聞くことができるようになるとともに、クラスタ間帯域幅をより効率的に使用できるようになります。この機能を活かすには、適切に設計された IP マルチキャスト環境が必要です。IP マルチキャストの詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Unified CM の初期のリリースでは、クラスタ間コールで利用できるのはユニキャスト MoH だけであり、ICT または SIP トランクで MoH が必要である場合に、各 Unified CM クラスタに少なくとも 1 つのユニキャスト MoH リソースを設定する必要があります。

分散型クラスタ間環境では、適切なマルチキャスト アドレス管理も、設計上の重要な考慮事項です。分散型ネットワーク全体で流れるリソースの重複を防止するために、いかなる MoH オーディオ ソース マルチキャスト アドレスも、配置内のすべての Unified CM クラスタに対して一意でなければなりません。

WAN を介したクラスタリング

その名前が示すように、クラスタオーバー WAN 配置には、他のマルチサイト配置と同様、低速 WAN リンクを含みます。したがって、これらの配置にも、G.729 コーデック、マルチキャスト トランスポート メカニズム、および低速 WAN リンクを介した MoH トラフィックに対して欠かせない安定した QoS の、3 つの要件が必要です。

さらに、このタイプの設定では、WAN の各端部に MoH サーバ リソースを配置することも必要です。WAN に障害が発生した場合には、WAN の各端部のデバイスは、ローカルに配置された MoH サーバから、引き続き MoH オーディオ ストリームを受信できます。さらに、適切な MoH 冗長設定がきわめて重要です。WAN の各端部のデバイスには、MRGL を指定する必要があります。この MRGL の MRG には、少なくとも 1 つのローカル リソースが最優先になった MoH リソースの優先順位リストが必要です。プライマリ サーバが使用不能になるか、要求を処理できない場合に備えて、この MRG に対して、MoH リソースを追加設定しておく必要があります。WAN のローカル側のリソースは使用不能になった場合に備えて、リスト内で他に少なくとも 1 つの MoH リソースは、リモート側の MoH リソースを指定しておく必要があります。

ユニキャストとマルチキャスト MoH コール フローの詳細

次の各項では、SCCP および SIP エンドポイントの両方について、ユニキャストとマルチキャスト MoH コール フローの詳細な図と説明を示します。

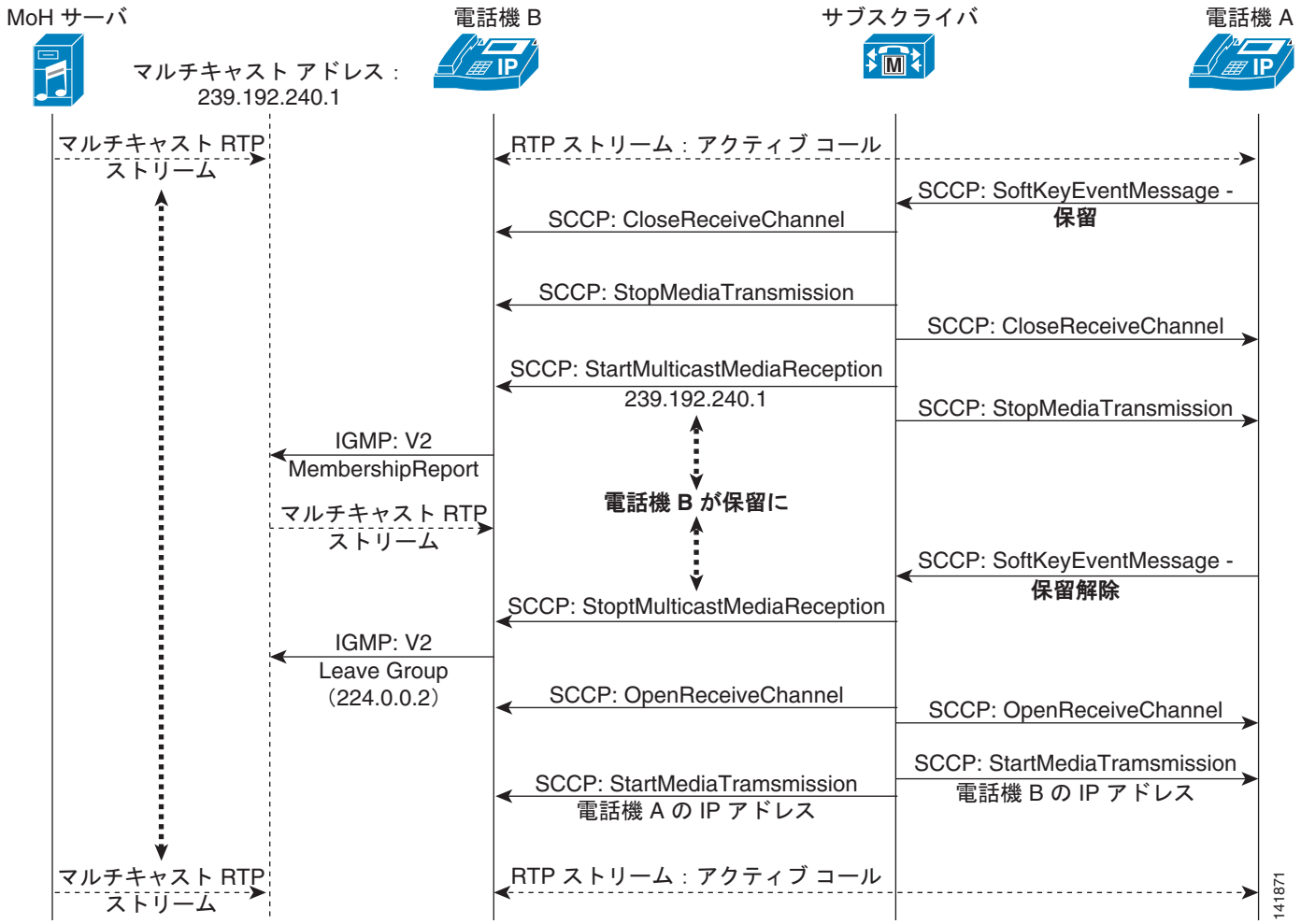
SCCP コール フロー

ここでは、Skinny Client Control Protocol（SCCP）エンドポイントでの保留音のコール フローについて説明します。

SCCP マルチキャスト コール フロー

図 17-11 は、標準的な SCCP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。次に、Unified CM は、マルチキャスト グループ アドレス 239.192.240.1 から、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を電話機 B（被保留側）に指示します。その後、電話機 B は Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）V2 の Membership Report メッセージを発行して、電話機 B がこのグループに加わることを示します。

図 17-11　SCCP マルチキャスト MoH コール フローの詳細



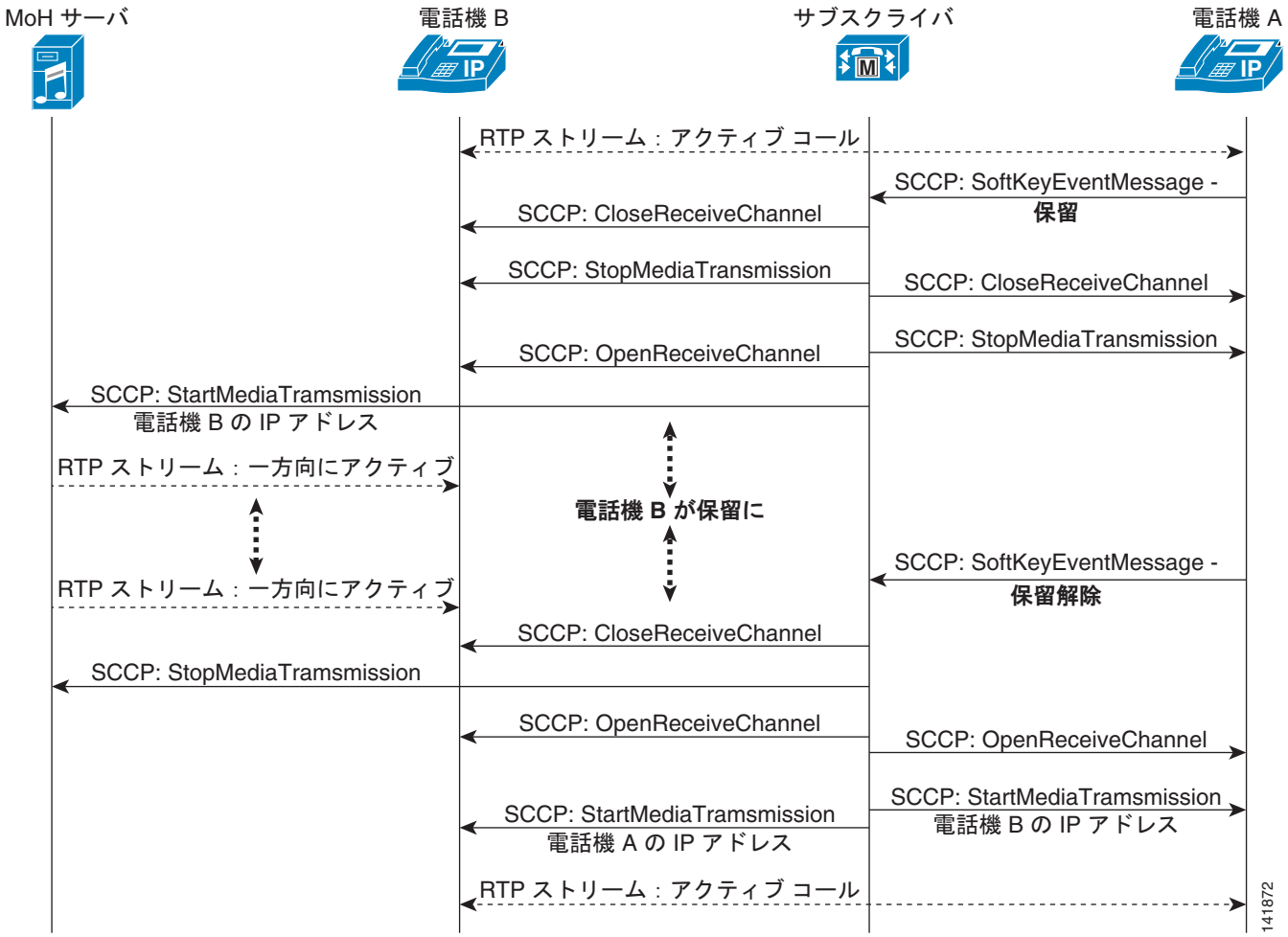
一方、MoH サーバがこのマルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、MoH ストリームの受信を開始します。電話機 A で [Resume] ソフトキーが押されると、Unified CM は、電話機 B に Stop Multicast Media Reception（マルチキャスト メディア受信の停止）を指示します。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。これにより、実質的に MoH セッションが終了します。次に、Unified CM は、電話機 A と電話機 B 間の通話の開始時に送信するように、両方の電話機に一連の Open Receive Channel（受信チャネルのオープン）メッセージを送信します。その後すぐに、Unified CM は、互いの IP アドレスへの Start Media Transmission（メディア送信の開始）を両方の電話機に指示します。電話機は、RTP 双方向オーディオ ストリームによって再び接続されます。

（注）　図 17-11 と図 17-12 のコール フロー図では、双方向 RTP オーディオ ストリームにより、初期化コールが電話機 A と電話機 B の間で存在することを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、確認応答、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される [Hold] ソフトキー アクションです。

SCCP ユニキャスト コール フロー

図 17-12 は、SCCP ユニキャスト MoH コール フローを示しています。このコール フロー図では、電話機 A で [Hold] ソフトキーが押されると、Unified CM は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。この時点まで、ユニキャストとマルチキャストの MoH コール フローは、まったく同じように動作します。

図 17-12　SCCP ユニキャスト MoH コール フローの詳細



次に、Unified CM は、Open Receive Channel（受信チャネルのオープン）を電話機 B（被保留側）に指示します。これは、マルチキャストの場合とまったく異なっています。マルチキャストでは、Unified CM は、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を被保留側に指示します。次に、Unified CM は、MoH サーバに、電話機 B の IP アドレスへの Start Media Transmission（メディア送信の開始）を指示します。これも、マルチキャスト MoH コール フローとはまったく異なる動作です。マルチキャストの場合、マルチキャスト グループ アドレスに加わるように、電話機に指示します。この時点で、MoH サーバは、片方向ユニキャスト RTP 音楽ストリームを電話機 B に送信します。電話機 A で [Resume] ソフトキーが押されると、Unified CM は、Stop Media Transmission（メディア送信の停止）を MoH サーバに指示し、Close Receive Channel（受信チャネルのクローズ）を電話機 B に指示して、実質的に MoH セッションを終了させます。マルチキャスト シ

ナリオの場合と同じように、Unified CM は、一連の Open Receive Channel（受信チャネルのオープン）メッセージおよび Start Media Transmissions（メディア送信の開始）メッセージを電話機 A と電話機 B に相互の IP アドレスを使用して送信します。電話機は、RTP 双方向オーディオ ストリームによって再び接続されます。

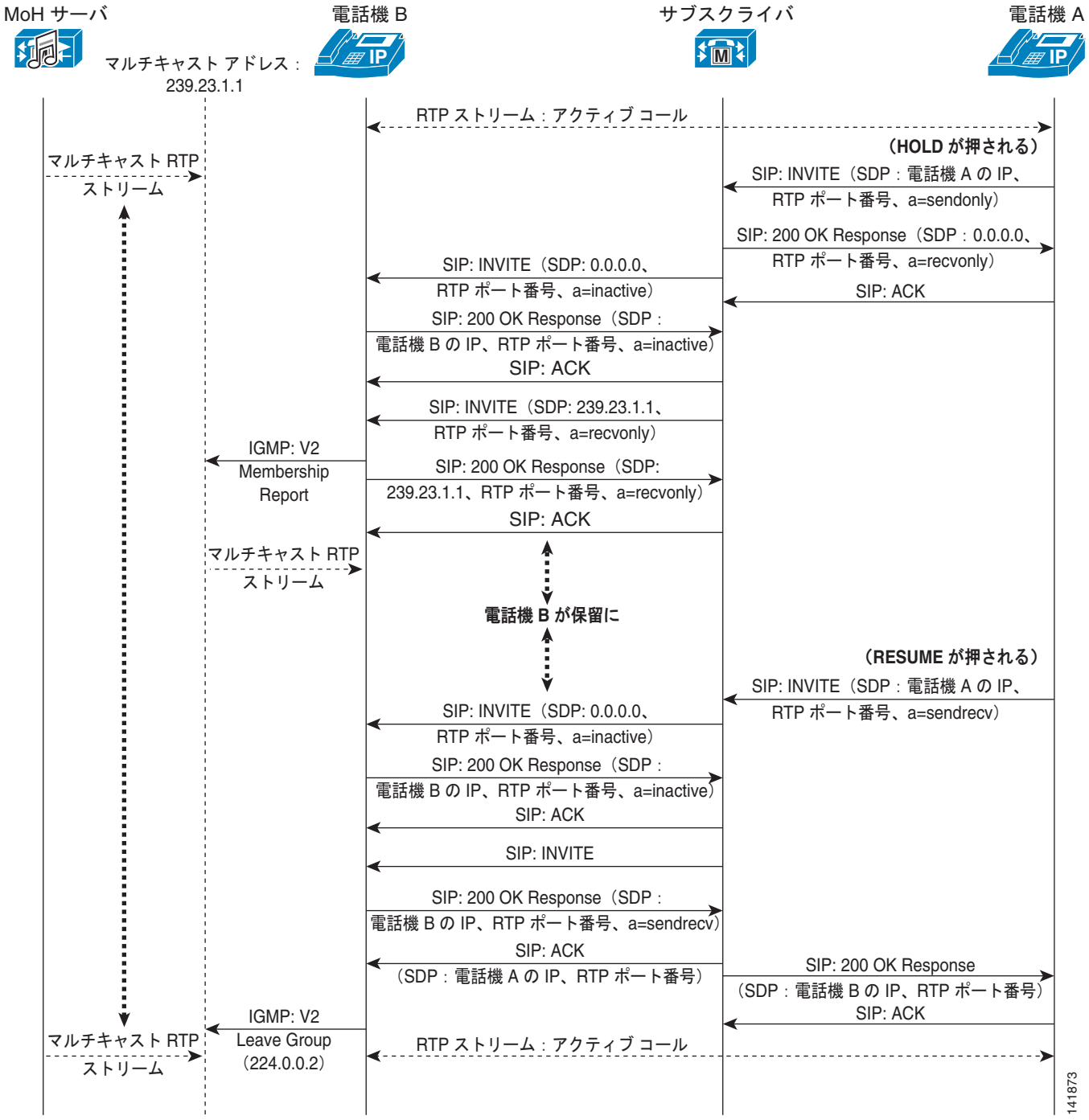
SIP コール フロー

ここでは、Session Initiation Protocol（SIP）エンドポイントでの保留音のコール フローについて説明します。

SIP マルチキャスト コール フロー

図 17-13 は、標準的な SIP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの Session Description Protocol（SDP）接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response によって、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE によって RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されると、Unified CM は SIP INVITE を電話機 B に送信します。このときの SDP 接続情報は MoH マルチキャスト グループ アドレス（この場合は 239.23.1.1）を示し、メディア属性は recvonly です。

図 17-13　SIP マルチキャスト MoH コール フローの詳細



次に、図 17-13 の電話機 B は IGMP V2 の Membership Report メッセージを発行して、電話機 B がこのマルチキャスト グループに加わることを示します。さらに、電話機 B は、前の SIP INVITE に応答して、SDP メディア属性が sendonly を示す SIP 200 OK Response を Unified CM に返します。一方、MoH サーバがこの MoH マルチキャスト グループ アドレスに RTP オーディオを送信しているので、電話機 B はそのマルチキャスト グループに加わった後、一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが [Resume] ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE によって、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。

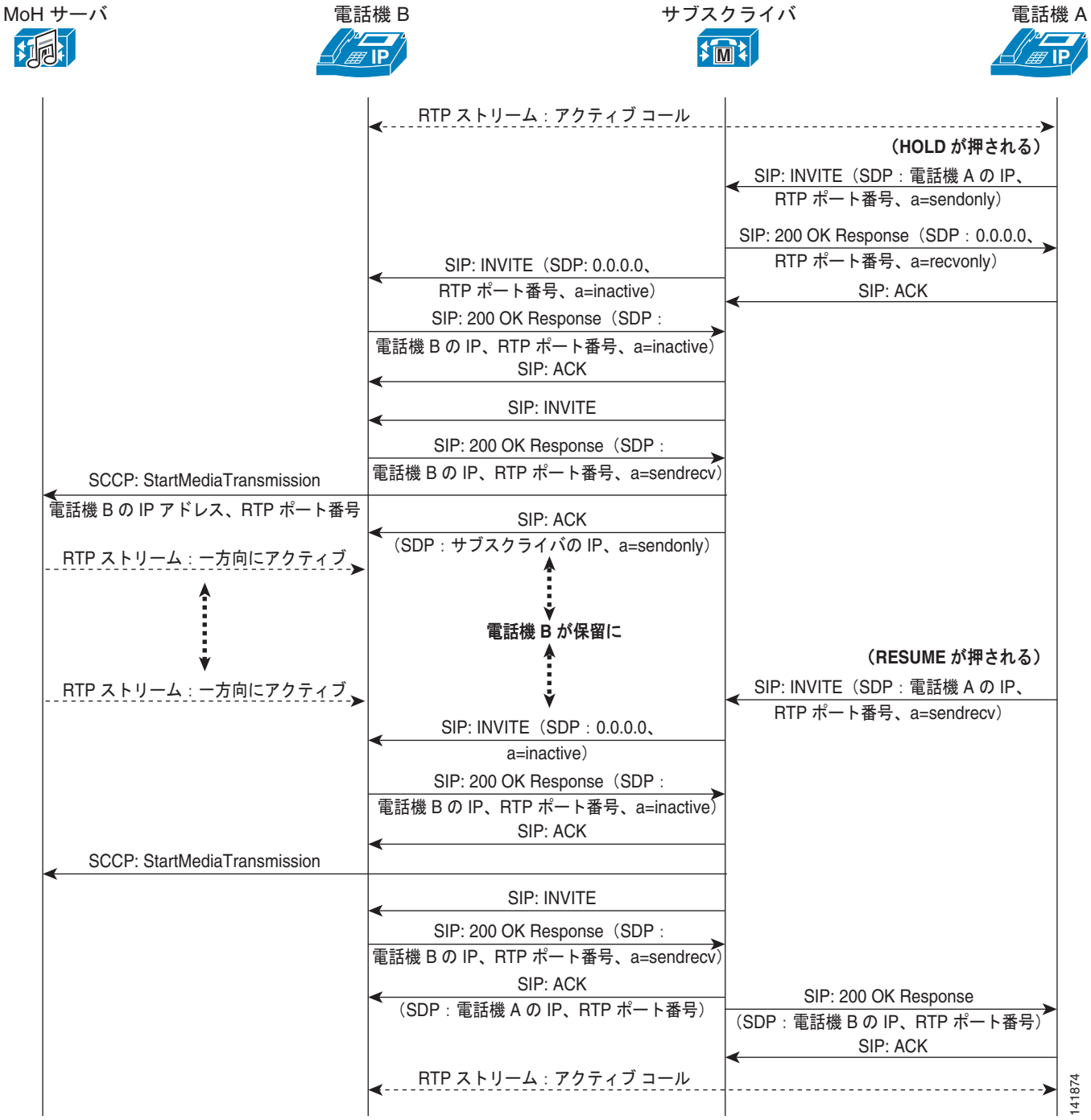
次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号です。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

（注）　図 17-13 と図 17-14 のコール フロー図では、双方向 RTP オーディオ ストリームを使用して、初期化コールが電話機 A と電話機 B の間で行われることを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、一部の確認応答、進行状況表示、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される [Hold] ソフトキー アクションです。

SIP ユニキャスト コール フロー

図 17-14 は、SIP ユニキャスト MoH コール フローを示しています。この図に示されているように、電話機 A で [Hold] ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response によって、RTP ストリームを切断するよう電話機 A に指示します。電話機 B は、Unified CM からの SIP INVITE によって RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。この時点まで、ユニキャストとマルチキャストの MoH コール フローはまったく同じです。

図 17-14　SIP ユニキャスト MoH コール フローの詳細



Unified CM は電話機 B に SIP INVITE を送信し、電話機 B は、それに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号および sendrecv を示す SIP 200 OK Response で応答します。Unified CM は、SCCP の StartMediaTransmission メッセージを MoH サーバに送信して、電話機 B のアドレスおよび受信 RTP ポート番号を伝えます。この後、

Unified CM から電話機 B への SIP ACK が続き、このときの SDP 接続情報には Unified CM の IP アドレス、メディア属性には sendonly が示されます。一方、MoH サーバが RTP オーディオを送信しているので、電話機 B は一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが [Resume] ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Unified CM は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE によって、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Unified CM に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。その後、Unified CM は、SCCP の StopMediaTransmission メッセージを MoH サーバに送信します。これによって、MoH サーバは電話機 B への MoH ストリームの転送を停止します。

次に、Unified CM は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Unified CM はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Unified CM は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートです。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

CHAPTER 18

Unified Communications エンドポイント

Cisco Unified Communications の配置では、さまざまなエンドポイントを使用できます。これらのエンドポイントは、IP 環境内の通常のアナログ電話機をサポートするゲートウェイから、さまざまな機能を提供するネイティブ IP Phone の拡張的なセットに至るまで、多岐にわたります。

エンドポイントを配置する際は、設定、認証、アップグレード、シグナリング プロトコル、QoS などのいくつかの要素を考慮する必要があります。Unified Communications システムは、これらの要素に対応するように適切に設計する必要があります。

この章では、さまざまなタイプの Unified Communications エンドポイントとその機能、および QoS 推奨事項について要約します。これらのエンドポイントは、次の主要なタイプに分類できます。

上記の各項では、それぞれのエンドポイント タイプについて詳細情報を示します。加えて、「QoS の推奨事項」（P.18-36）の項では QoS 設定のリストを示し、「エンドポイント機能の要約」（P.18-53）の項ではエンドポイントの全機能のリストを示します。

この章を参照して、使用可能なエンドポイント オプションの範囲と、その配置に伴う設計上の考慮事項を理解してください。

この章の新規情報

表 18-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 18-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco E20 Video Phone	「Cisco E20 Video Phone」（P.18-33） 「H.323 と SIP のビデオ エンドポイント」（P.18-49） 表 18-6 表 18-14 表 18-16	2010 年 11 月 15 日
Cisco Unified Wireless IP Phones 7925G-EX および 7926G	「ワイヤレス エンドポイント」（P.18-22） 表 18-14	2010 年 11 月 15 日
Cisco Unified IP Phone 6900 シリーズでサポートされる機能	「エンドポイント機能の要約」（P.18-53）	2010 年 11 月 15 日
Cisco Unified IP Phone 6900 シリーズでサポートされる機能	表 18-8 表 18-10 表 18-12	2010 年 7 月 23 日
Cisco Unified Client Services Framework（CSF）のビデオ設計に関する考慮事項	「ビデオ設計上の考慮事項」（P.18-21）	2010 年 4 月 2 日
Cisco Unified IP Phone 9951 および 9971 のビデオ サポート	「Cisco Unified IP Phone 9971 および 9951」（P.18-32） 表 18-16	2010 年 4 月 2 日

Unified Communications エンドポイント アーキテクチャ

Cisco Unified Communications Manager（Unified CM）のコール シグナリングでは、回線側シグナリングとトランク側シグナリングが区別されます。トランク側シグナリングは、Unified CM クラスタ全体を他のサーバおよびゲートウェイに接続するために使用されます。一方、回線側シグナリングは、エンド ユーザ デバイスをクラスタに接続するために使用されます。この 2 つのインターフェイスはそれぞれ、提供するサービスが異なります。回線側は、ユーザ指向の豊富な機能セットを提供します。

Unified CM でサポートされる 2 つの主要な回線側シグナリング プロトコルは、Session Initiation Protocol（SIP; セッション開始プロトコル）と Skinny Client Control Protocol（SCCP）です。すべての Cisco エンドポイントは、このうち一方または両方のプロトコルをサポートしています。どちらのプロトコルでも、サポートされる機能セットはおおよそ同じであるため、いずれのプロトコルの使用を選択するかは、基本的には配置における個人的な好みによります。表 18-7 ～表 18-15 では、さまざまなエンドポイントでサポートされるプロトコルおよび機能を比較しています。

Cisco エンドポイントを使用してコールの発信や受信、またはアプリケーションの実行を行うには、いくつかの操作パラメータを使用して Cisco エンドポイントを設定しておく必要があります。Unified CM で、事前にこの設定を実行しておく必要があります。設定の完了後は、Unified CM によって使用するエンドポイントの設定ファイルが生成され、TFTP サーバ内にそのファイルが格納されます。エンドポイント自体は、電源が投入されると、ブートアップ シーケンスを通過します。エンド

ポイントは、この設定ファイルを取得した後、適切なサーバに登録されます。これにより、エンドポイントは使用できる状態になります。エンドポイントは、ブートアップ シーケンスの一部として次のステップを実行します。

1. エンドポイントが電源に差し込まれていない場合、アクセス スイッチに接続されていれば、スイッチからの電力の獲得を試行します（Power over Ethernet）。
2. 電力の獲得後は、デバイス セキュリティが有効になっていれば、エンドポイントはセキュリティ サーバにクレデンシャルを提示します。
3. エンドポイントは、ネットワークを使用できる場合、エンドポイント内の静的プロビジョニングによって、または DHCP によって、ネットワーク パラメータ（IP アドレス、DNS サーバ、ゲートウェイ アドレスなど）を取得します。
4. また、エンドポイントは、エンドポイント内の静的プロビジョニングによって、または DHCP オプションによって、TFTP サーバ アドレスも取得します。
5. 続いて、エンドポイントは、TFTP サーバ アドレスを使用して、その設定ファイルを取得します。このファイルには、そのエンドポイントに関連付けられている Unified CM クラスタ内のサーバや、そのエンドポイントでサポートする必要のあるディレクトリ番号などが、他のパラメータとともに説明されています。
6. エンドポイントがサーバに登録され、使用できる状態になります。

アナログ ゲートウェイ

アナログ ゲートウェイには、ルータ ベースのアナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco コミュニケーション メディア モジュール（CMM）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG202、Cisco VG204、Cisco VG224、Cisco VG248、および Cisco Analog Telephone Adapter（ATA）186、188 が内蔵されています。アナログ ゲートウェイは通常、FAX マシン、モデム、TDD/TTY、およびアナログ電話機などのアナログ デバイスを VoIP ネットワークに接続するために使用します。これにより、アナログ信号を IP ネットワーク上でパケット化して送信できるようになります。

アナログ インターフェイス モジュール

ルータベースの Cisco アナログ インターフェイス モジュールには、低密度インターフェイス モジュール（NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1）と高密度インターフェイス モジュール（NM-HDA-4FXS および EVM-HD-8FXS/DID）があります。Cisco アナログ インターフェイス モジュールは、公衆網やその他の従来の電話機器（PBX、アナログ電話機、FAX、キー システムなど）を、Cisco マルチサービス アクセス ルータに接続するためのものです。Cisco アナログ インターフェイス モジュールは、低密度から高密度までのアナログ デバイスを、コール機能に制限がある IP ネットワークに接続する場合に最適です。

低密度アナログ インターフェイス モジュール

低密度アナログ インターフェイス モジュールには、NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 があります。NM-1V と NM-2V には、1 つまたは 2 つの音声インターフェイス カード（VIC）があります。このインターフェイス カードには、2 ポート FXS VIC（VIC-2FXS）、2 ポート FXO VIC（VIC-2FXO、VIC-2FXO-M1/M2/M3、および VIC-2FXO-EU）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2

ポート E&M VIC（VIC-2E/M）、2 ポート CAME（Centralized Automated Message Accounting）VIC（VIC-2CAMA）、および 2 ポート BRI VIC（VIC-2BRI-S/T-TE および VIC-2BRI-NT/TE）があります。NM-1V および NM-2V は、それぞれ最大で 2 個および 4 個の FXS 接続を処理できます。

（注）　NM-1V と NM-2V は、Cisco 2800 および 3800 シリーズのプラットフォームではサポートされていません。Cisco 2800 および 3800 シリーズのプラットフォームでは、VIC-2DID、VIC4-FXS/DID、VIC2-2FXO、VIC-2-4FXO、VIC2-2FXS、VIC2-2E/M、および VIC2-2BRI-NT/TE を含む音声インターフェイス カードは、オンボードの高速 WIC スロットでサポートされています。

NM-HD-1V と NM-HD-2V には、それぞれ 1 つおよび 2 つの VIC があります。NM-HD-2VE には、2 つの VIC または 2 つの音声 /WAN インターフェイス カード（VWIC）、または 1 つの VIC と 1 つの VWIC の組み合せが含まれます。NM-HD-1V、NM-HD-2V、および NM-HD-2VE は、それぞれ最大で 4 個、8 個、および 8 個の FXS 接続または FXO 接続を処理できます。NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 は、最大 4 個の FXS 接続または FXO 接続を処理するデジタル T1/E1 またはアナログ /BRI インターフェイス カードのいずれかに対応させることができます。これら 3 つのインターフェイス モジュールの相違点は、NM-HDV2-1T1/E1 には 1 つの組み込み T1/E1 ポートがあるのに対し、NM-HDV2-2T1/E1 には 2 つの組み込み T1/E1 ポートがあることです。

音声インターフェイス カードには、2 ポートおよび 4 ポート FXS VIC（VIC2-2FXS および VIC-4FXS/DID）、2 ポートおよび 4 ポート FXO VIC（VIC2-2FXO および VIC2-4FXO）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2 ポート E&M VIC（VIC2-2E/M）、および 2 ポート BRI VIC（VIC2-2BRI-NT/TE）があります。音声 /WAN インターフェイス カードには、音声および WAN 接続両用の 1 ポートおよび 2 ポート RJ-48 マルチフレックス トランク（MFT）T1/E1 VWIC（VWIC-1MFT-T1、VWIC-2MFT-T1、VWIC-2MFT-T1-DI、VWIC-1MFT-E1、VWIC-2MFT-E1、VWIC-2MFT-E1-DI、VWIC-1MFT-G703、VWIC-2MFT-G703、VWIC2-1MFT-T1/E1、VWIC2-2MFT-T1/E1、VWIC2-1MFT-G703、および VWIC2-2MFT-G703）があります。G.703 インターフェイス カードは主としてデータ接続用ですが、場合によっては音声アプリケーションをサポートするように設定できます。

高密度アナログ インターフェイス モジュール

高密度アナログ インターフェイス モジュールには NM-HDA-4FXS と EVM-HD-8FXS/DID があります。NM-HDA-4FXS には 4 つのオンボード FXS ポートがあり、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード
- EM-HDA-4FXO/EM2-HDA-4FXO：4 ポート FXO インターフェイス カード

NM-HDA-4FXS は、4 つの組み込み FXS ポートと 2 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 12 アナログ ポート（4 FXS および 8 FXO）の構成になるか、または 4 つの組み込み FXS ポートと 1 つの EM-HDA-8FXS 拡張モジュールおよび 1 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 16 アナログ ポート（12 FXS および 4 FXO）の構成になります。2 つの 8 ポート FXS 拡張モジュールを使用する構成はサポートされていません。NM-HDA には、追加の DSP リソースを提供するドーター モジュール（DSP-HDA-16）用のコネクタもあり、8 つの高複雑度コールまたは 16 の中複雑度コールを追加処理できます。

（注）　EM2-HDA-4FXO は、EM-HDA-FXO と同じ密度と機能をサポートしますが、最大 15,000 フィートのループ長のサポートや、グラウンドスタート シグナリング モードで使用して回線状態が悪い場合のパフォーマンス向上などの拡張機能があります。

EVM-HD-8FXS/DID は、基本ボード モジュール上に 8 つの独立したポートがあり、FXS または DID シグナリング用に構成可能です。また、EVM-HD-8FXS/DID には、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード
- EM-HDA-6FXO：6 ポート FXO インターフェイス カード
- EM-HDA-3FXS/4FXO：3 ポート FXS および 4 ポート FXO インターフェイス カード
- EM-4BRI-NT/TE：4 ポート BRI インターフェイス カード

これらの拡張モジュールは任意の組み合せで使用でき、EVM-HD-8FXS/DID あたり最大 24 FXS ポートの構成になります。

アナログ インターフェイス モジュールでサポートされているプラットフォームおよび Cisco IOS 要件

Cisco アナログ インターフェイス モジュールにサポートされるプラットフォームは、Cisco 2600、2800、3600、3700、および 3800 シリーズです。表 18-2 は、1 プラットフォームあたりにサポートされるインターフェイス モジュールの最大数を示し、表 18-3 は、Cisco IOS ソフトウェアの最低限必要なバージョンを示しています。

表 18-2　各プラットフォームでサポートされるアナログ インターフェイス モジュールの最大数

	サポートされているインターフェイス モジュールの最大数				
プラットフォーム	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	1	1	なし	1	1
Cisco 2691	1	1	なし	1	1
Cisco 3640	3	3	なし	3	なし
Cisco 3660	6	6	なし	6	なし
Cisco 3725	2	2	なし	2	2
Cisco 3745	4	4	なし	4	4
Cisco 2811	なし	1	1	1	1
Cisco 2821	なし	1	1	1	1
Cisco 2851	なし	1	1	1	1
Cisco 3825	なし	2	1	2	2
Cisco 3845	なし	4	2	4	4

表 18-3　アナログ インターフェイス モジュールの Cisco IOS 最小要件

	必要な Cisco IOS ソフトウェア対応リリース				
プラットフォーム	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 2691	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T

表 18-3　アナログ インターフェイス モジュールの Cisco IOS 最小要件（続き）

プラットフォーム	必要な Cisco IOS ソフトウェア対応リリース				
	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco 3640	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3660	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3725	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 3745	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 2811	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2821	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2851	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 3825	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T
Cisco 3845	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T

Cisco コミュニケーション メディア モジュール（CMM）

Cisco CMM は、Catalyst 6000 および Cisco 7600 シリーズ スイッチに、高密度アナログ、T1、および E1 ゲートウェイ接続を提供するライン カードです。Cisco CMM は、最大 72 個の FXS 接続を処理できます。CMM は MGCP または H.323 ゲートウェイとして動作し、最大 480 個の IP Phone に Survivable Remote Site Telephony（SRST）サービスを提供します。

Cisco CMM に含まれるインターフェイス ポート アダプタは、24 ポート FXS アナログ ポート アダプタ（WS-SVC-CMM-24FXS）、6 ポート T1 インターフェイス ポート アダプタ（WS-SVC-CMM-6T1）、6 ポート E1 インターフェイス ポート アダプタ（WS-SVC-CMM-6E1）、および会議 / トランスコーディング ポート アダプタ（WS-SVC-CMM-ACT）です。表 18-4 は、互換性があるポート アダプタの最低限のソフトウェア要件を示しています。

表 18-4　CMM ポート アダプタのソフトウェア要件

	WS-SVC-CMM-24FXS	WS-SVC-CMM-6T1	WS-SVC-CMM-6E1	WS-SVC-CMM-ACT
Cisco IOS リリース	12.3(8)XY	12.3(8)XY	12.3(8)XY	12.3(8)XY
CatOS リリース	7.3(1)	7.3(1)	7.3(1)	7.6.8
Native IOS リリース	12.1(15)E	12.1(14)E	12.1(13)E	12.1(13)E
CMM ごとの最大ポート アダプタ数	3	3	3	4

WS-X6624-FXS アナログ インターフェイス モジュール

Cisco WS-X6624-FXS アナログ インターフェイス モジュールは、高密度アナログ デバイスを IP テレフォニー ネットワークに接続するための MGCP ベースのデバイスで、24 個のアナログ ポートを提供します。

（注）　WS-X6624 FXS アナログ インターフェイスは販売終了になりました。

Cisco VG202 および VG204 ゲートウェイ

Cisco VG202 および VG204 アナログ ゲートウェイは、Cisco IOS ベースで低密度の 2 ポートおよび 4 ポート ゲートウェイであり、アナログ電話、FAX マシン、モデム、およびその他のアナログ デバイスを会社の音声システムに接続できます。これらのゲートウェイは、Skinny Client Control Protocol（SCCP）または Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）ゲートウェイのいずれかとして、Unified CM に直接統合できます。これらのゲートウェイが MGCP モードで動作している場合に Unified CM クラスタとの接続が失われると、H.323 を介した Survivable Remote Site Telephony（SRST）へのフェールオーバーを実行します。

また、これらのゲートウェイは SIP プロトコルをサポートしており、Unified CM に SIP トランクを介して接続できます。ただし、このモードでは、Unified CM との SCCP または MGCP 統合で利用可能ないくつかの機能を利用できません。

Cisco VG224 ゲートウェイ

Cisco VG224 アナログ ゲートウェイは、アナログ デバイスを IP テレフォニー ネットワークに接続するための、Cisco IOS の 24 ポート高密度ゲートウェイです。Cisco IOS Release 12.4(2)T 以降では、Cisco VG224 は、Skinny Client Control Protocol（SCCP）または Cisco Unified Communications Manager（Unified CM）を搭載したメディア ゲートウェイ コントロール プロトコル（MGCP）エンドポイントとして機能することができ、フェールオーバーのシナリオでは Survivable Remote Site Telephone（SRST）ルータに復帰できます。また、Cisco VG224 は、モデム パススルー、モデム リレー、FAX パススルー、および FAX リレーもサポートしています。さらに、Cisco VG224 は、Cisco Unified Communications Manager Express（Unified CME）および Cisco Unified Survivable Remote Site Telephone（SRST）上で SCCP サポートの アナログ電話を接続するために使用できます。

Cisco VG248 ゲートウェイ

Cisco VG248 は、アナログ電話機、FAX マシン、モデム、スピーカーフォンのようなアナログ デバイスを企業の Cisco Unified CM および音声ネットワークに接続するための、48 ポートの高密度 Skinny Client Control Protocol（SCCP）ゲートウェイです。また、Cisco VG248 は、Simplified Message Desk Interface（SMDI）、NEC Message Center Interface（MCI）、または Ericsson のボイスメール プロトコルと互換性があるレガシー ボイスメール システムおよび PBX との Unified CM の統合もサポートしています。Cisco VG248 は、Survivable Remote Site Telephone（SRST）へのフェールオーバーをサポートしています。

Cisco ATA 186 および 188

Cisco Analog Telephone Adaptor（ATA）186 または 188 は、IP テレフォニー ネットワークに 2 つのアナログ デバイスを接続でき、低密度アナログ デバイスを IP ネットワークに接続する場合に最適です。

Cisco ATA 186 と 188 の相違点は、前者には 10 Base-T イーサネット接続が 1 つしかないのに対し、後者には、自らの接続用と、共存する PC または他のイーサネットベース デバイスの接続用の 2 つの 10/100 Base-T イーサネット接続を提供する統合イーサネット スイッチがあることです。Cisco ATA 186 および 188 は、次のいずれかの方法で設定できます。

- Cisco ATA Web 設定ページ
- Cisco ATA 音声設定メニュー
- TFTP サーバからダウンロードした設定ファイル

SCCP ベースの ATA は、SCCP IP Phone のように動作します。別のエンドポイントから電話をかけられるように、Cisco ATA 186 または 188 を、SIP プロキシ サーバに登録された SIP クライアントとして設定できます。Cisco ATA 186 または 188 は、SIP 要求を開始するときは User Agent Client（UAC; ユーザ エージェント クライアント）として、要求に応答するときは User Agent Server（UAS; ユーザ エージェント サーバ）として動作できます。

Cisco Unified IP Phone

Cisco IP Phone 製品には、ベーシック IP Phone、ビジネス IP Phone、マネージャ IP Phone、およびエグゼクティブ IP Phone があります。

Cisco ベーシック IP Phone

Cisco ベーシック IP Phone は、コール機能に制限があり、予算上の要求がある、トラフィック量の少ないユーザに最適です。ベーシック IP Phone には、Cisco Unified SIP Phone 3911、および Cisco Unified IP Phone 6901、6911、7902G、7905G、7906G、7910G、7910G+SW、7911G、7912G が内蔵されています。

Cisco Unified SIP Phone 3911

Cisco Unified SIP Phone 3911 は単一回線をサポートし、電話機の背面に 1 つの 10/100 Base-T イーサネット ポートを備えています。Cisco Unified SIP Phone 3911 は、2 行の液晶ディスプレイ（LCD）画面と半二重のスピーカーフォンを備えています。電源は、IEEE 802.3af、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。この電話機は SIP だけをサポートします。

Cisco Unified IP Phone 6901

Cisco Unified IP Phone 6901 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6901 は、1 つの 10/100 Base-T イーサネット接続を持つ基本的な単一回線電話で、ロビーや玄関、エレベータ、および音声通信が必要になる場合があるその他のエリアでの使用に理想的です。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 6911

Cisco Unified IP Phone 6911 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6911 は、1 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続および全二重スピーカーフォンを装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7902G

Cisco Unified IP Phone 7902G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。Cisco Unified IP Phone 7902G に液晶（LCD）画面はありません。Cisco Unified IP Phone 7902G は SCCP をサポートしていますが、SIP をサポートしていません。

Cisco Unified IP Phone 7905G

Cisco Unified IP Phone 7905G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでだけ動作します。
Cisco Unified IP Phone 7905G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

Cisco Unified IP Phone 7906G

Cisco Unified IP Phone 7906G は単一回線をサポートし、電話機の背面に 1 つの 10/100 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでだけ動作します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。Cisco Unified IP Phone 7906G は SCCP と SIP をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンド ユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

Cisco Unified IP Phone 7910G、7910G+SW

Cisco Unified IP Phone 7910G は単一回線だけをサポートし、スピーカーは、一方向のリッスン モードでだけ動作します。Cisco Unified IP Phone 7910G には、カスタマイズされた電話機ボタン テンプレート中で管理者が設定できる 6 つの機能アクセス キーもあり、エンド ユーザにさまざまなコール機能を提供します。この電話機モデルには機能アクセス キーが 6 つしかないため、1 つの電話機ボタン テンプレートは、エンド ユーザにすべてのコール機能を提供することができません。Cisco Unified IP Phone 7910G と 7910+SW の両方とも SCCP をサポートしていますが、SIP はサポートしていません。
Cisco Unified IP Phone 7910G と 7910G+SW の唯一の相違点は、前者には 10 Base-T イーサネット ポートが 1 つあるのに対し、後者には 10/100 Base-T イーサネット ポートが 2 つあることです。

Cisco Unified IP Phone 7911G

Cisco Unified IP Phone 7911G は単一回線だけをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでだけ動作します。
Cisco Unified IP Phone 7911G は SCCP と SIP をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンド ユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

Cisco Unified IP Phone 7912G

Cisco Unified IP Phone 7912G は単一回線だけをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでだけ動作します。Cisco Unified IP Phone 7912G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

（注）　Cisco Unified IP Phone 7902G、7905G、7910G、7910G+SW、および 7912G は販売終了になりましたが、Cisco Unified Communications Manager によりサポートされることに変わりありません。

Cisco ビジネス IP Phone

Cisco ビジネス IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度のトランザクション タイプの社員に最適です。ビジネス IP Phone には、Cisco Unified IP Phone 6921、6961、7931G、7940G、7941G、7941G-GE、7942G、および 7945G があります。

Cisco Unified IP Phone 6921

Cisco Unified IP Phone 6921 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6921 は、最大 2 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続および全二重スピーカーフォンを装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 6961

Cisco Unified IP Phone 6961 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6961 は、最大 12 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続を装備しています。また、全二重スピーカーフォンも装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7931G

Cisco Unified IP Phone 7931G は、24 の点灯ライン キーに割り当てることができる最大 24 のディレクトリ番号をサポートし、小売業、営業、および製造業のユーザに最も適しています。Cisco Unified IP Phone 7931G は 2 つの 10/100 Base-T イーサネットを持ち、SIP および SCCP の両方をサポートしています。他の Cisco Unified IP Phone で使用可能なプログラマブル ソフトキー のサポートに加えて、Cisco Unified IP Phone 7931G には、保留、リダイヤル、および転送の各機能に対応する 3 つの専用キーがあります。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7940G

Cisco Unified IP Phone 7940G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7940G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7940G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7940G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7940G にはビデオ サポートがありません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7941G

Cisco Unified IP Phone 7941G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7941G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンド ユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7941G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7941G は保留トーンをサポートしているのに対し、SIP はサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7941G-GE

Cisco Unified IP Phone 7941G-GE は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7941G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco Unified IP Phone 7942G

Cisco Unified IP Phone 7942G は、7941G と同様に、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。7941G の他の機能およびプロトコル サポートに加えて、7942G では G.722 ワイドバンド コーデック のサポートもあり、また、高忠実度の音声通信用のスピーカー、マイク、受話器が更新されています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7945G

Cisco Unified IP Phone 7945G は、7942G の機能を拡張しています。7942G と同様に 7945G は、最大 2 つのディレクトリ番号を持つことができますが、7942G と異なり 7945G は、2 つの 10/100/1000 Base-T イーサネット接続、および 5 方向のナビゲーション ボタン セットも備えています。G.722 ワイドバンド コーデック、および高忠実度のスピーカー、マイク、受話器のサポートに加えて、7945G はバックライト TFT カラー ディスプレイを備えており、通信情報、時間節約アプリケーション、および機能使用状況に簡単にアクセスできます。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco マネージャ IP Phone

Cisco マネージャ IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度から大量の、マネージャおよびアシスタントに最適です。ビジネス IP Phone には、Cisco Unified IP Phone 6941、7960G、7961G、7961G-GE、7962G、7965G、8961 があります。

Cisco Unified IP Phone 6941

Cisco Unified IP Phone 6941 は、そのハードウェアの特性と工業設計を Cisco Unified IP Phone 6900 シリーズの他のモデルと共有しています。

Cisco Unified IP Phone 6941 は、最大 4 つのディレクトリ番号をサポートし、2 つの 10/100 Base-T イーサネット接続を装備しています。また、全二重スピーカーフォンも装備しています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7960G

Cisco Unified IP Phone 7960G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7960G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7960G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7960G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7960G にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7960G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7961G

Cisco Unified IP Phone 7961G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7961G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンド ユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7961G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7961G は保留トーンをサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7961G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7961G-GE

Cisco Unified IP Phone 7961G-GE は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7961G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco Unified IP Phone 7962G

Cisco Unified IP Phone 7962G は、7961G と同様に、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。7961G の他の機能およびプロトコル サポートに加えて、7962G では G.722 ワイドバンド コーデック のサポートもあり、また、高忠実度の音声通信用のスピーカー、マイク、および 受話器が更新されています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7965G

Cisco Unified IP Phone 7965G は、7962G の機能を拡張しています。7962G と同様に 7965G は、最大 6 つのディレクトリ番号を持つことができますが、7962G と異なり 7965G は、2 つの 10/100/1000 Base-T イーサネット接続、および 5 方向のナビゲーション ボタン セットも備えています。G.722 ワイドバンド コーデック、および高忠実度のスピーカー、マイク、受話器に加えて、7965G はバックライト TFT カラー ディスプレイを備えており、通信情報、時間節約アプリケーション、および機能使用状況に簡単にアクセスできます。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 8961

Cisco Unified IP Phone 8961 は、Cisco IP Phone 製品の中では高度な機能を提供します。8961 は、最大 5 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、8961 は、5 つのセッション キー、ヘッドセット用の 1 つの USB ポート、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、8961 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco エグゼクティブ IP Phone

Cisco エグゼクティブ IP Phone は、拡張コール機能を使用する、トラフィック量の多い経営幹部ユーザに最適です。エグゼクティブ IP Phone には、Cisco Unified IP Phone 7970G、7971G-GE、7975G、9951、および 9971 があります。

Cisco Unified IP Phone 7970G

Cisco Unified IP Phone 7970G は、最大 8 つのディレクトリ番号の設定が可能で、高解像度のカラー タッチ スクリーンを備え、他の Cisco Unified IP Phone よりも多くのアクセス キーがあります。Cisco Unified IP Phone 7970G は SCCP と SIP の両方をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコ

ルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンド ユーザの操作性は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7970G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7970G は保留トーンをサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7970G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 7971G-GE

Cisco Unified IP Phone 7971G-GE は、最大 8 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7970G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

（注）　Cisco Unified IP Phone は、アクセス スイッチからのインライン パワー、またはローカルの壁面コンセントからの電源供給に加えて、Cisco Unified IP Phone パワー インジェクタによる電源供給も可能です。Cisco Unified IP Phone パワー インジェクタを使用すると、インライン パワーをサポートしない Cisco スイッチまたは Cisco 以外のスイッチに、Cisco Unified IP Phone を接続できます。Cisco Unified IP Phone パワー インジェクタは、すべての Cisco Unified IP Phone と互換性があり、Cisco PoE と IEEE 802.3af PoE の両方をサポートしています。2 つの 10/100/1000 Base-T イーサネット接続を備え、一方をスイッチのアクセス ポートに接続し、もう一方を Cisco Unified IP Phone に接続します。

Cisco Unified IP Phone 7975G

Cisco Unified IP Phone 7975G は、7971G-GE と同様に、最大 8 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えています。ただし、7971G-GE と異なり、7975G には、G.722 ワイドバンド コーデックおよび高忠実度のスピーカー、マイク、および受話器が追加されています。7975G には、タッチ スクリーン カラー ディスプレイも備わっています。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco Unified IP Phone 9951

Cisco Unified IP Phone 9951 は、Cisco IP Phone 製品の中では高度な機能を提供します。9951 は、最大 5 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、9951 は、5 つのセッション キー、1 つの USB ポート、Bluetooth ヘッドセットのサポート、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、9951 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

9951 は、ビデオ メディア ストリームを受信する機能を備えています。ポイントツーポイント ビデオ コールを行うために、特別に設計されたオプションの USB カメラを 9951 に接続できます。ビデオに関連する設計上の考慮事項については、「ビデオ エンドポイント」（P.18-29）の項を参照してください。

Cisco Unified IP Phone 9971

Cisco Unified IP Phone 9971 は、Cisco IP Phone 製品の中では高度な機能を提供します。9971 は、最大 6 つのディレクトリ番号、2 つの 10/100/1000 Base-T イーサネット接続、および 1 つの 5 方向のナビゲーション ボタン セットをサポートします。また、9971 は、6 つのセッション キー、2 つの USB ポート、Bluetooth ヘッドセットのサポート、タッチ スクリーン、802.11a/b/g 無線インターフェイス、ユーザ エクスペリエンスを向上させるための、固定ハード ボタンに割り当てられた最も一般的なコール機能（保留、転送、会議）を備えています。さらに、9971 は、ワイドバンド オーディオ ヘッドセット、スピーカー、ハンドセットを備え、MIDlet および XML アプリケーションをサポートします。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

9971 は、ビデオ メディア ストリームを受信する機能を備えています。ポイントツーポイント ビデオ コールを行うために、特別に設計されたオプションの USB カメラを 9971 に接続できます。ビデオに関連する設計上の考慮事項については、「ビデオ エンドポイント」（P.18-29）の項を参照してください。

Cisco Unified IP Phone 拡張モジュール 7914、7915、7916

Cisco Unified IP Phone 拡張モジュール 7914、7915、7916 は、いくつかの回線の状態が電話機の現在の回線容量を超えていることを判断する必要があるアシスタントなどに適しています。

Cisco Unified IP Phone 拡張モジュール 7914、7915、および 7916 は、追加のボタンと LCD によって、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G、7970G、7971G-GE、または 7975G の機能を拡張します。Cisco Unified IP Phone 拡張モジュール 7914 ではモジュールあたり 14 のボタンが提供され、Cisco Unified IP Phone 拡張モジュール 7915 および 7916 ではモジュールあたり 24 のボタンが提供されます。Cisco Unified IP Phones 796*x*G および 797*x*G は、最大 2 つの Cisco Unified IP Phone 拡張モジュールをサポートできます。IP Phone で Cisco インライン パワーまたは IEEE802.3af PoE を使用している場合には、Cisco Unified IP Phone 拡張モジュール 7914、7915、7916 に外部電源アダプタ（CP-PWR-CUBE-3）を使用する必要があります。

（注）　1 台の電話機で 2 つの拡張モジュールを使用する場合、2 番めのモジュールを 1 番めのモジュールと同じモデルにする必要があります。

Cisco Unified IP Phone 6921、6941、および 6961 シリーズの配置に関する考慮事項

これらの IP 電話は、統一的な工業設計、1 回線 1 コール、最も一般的に使用されるユーザ機能（保留、転送、会議など）のハード キーなどの一般的な特性を共有しています。

このモデルの電話はすべて回線ごとに 1 つのコールをサポートします。すでにアクティブ コールのある回線への着信コールは、ビジーとして処理されます。つまり、設定によってボイスメールまたは別のディレクトリ名に転送されるか、（転送が設定されていない場合）コールは完了せず、ビジー トーンが発信者に返されます。転送する代わりに第 2 のコールが電話機に表示されるようにするには、プライマリと同じディレクトリ番号に別の回線を設定する必要があります。この第 2 の回線はプライマリと別のパーティションにある必要があり、プライマリ回線はコールを第 2 の回線に転送するように設定する必要があります。パーティションの設定の詳細については、「ダイヤル プラン」（P.9-1）を参照してください。

Cisco Unified IP Phones 6921、6941、および 6961 シリーズには、Direct Transfer や Direct Transfer Across Lines などのコール機能が導入され、Join や Join Across Lines 機能も提供されています。これらの機能は、複数の回線をまたがるコールに対して動作でき、これらの動作は電話機上のプライマリ回線だけをモニタする Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）アプリケーションに対して不透明にできます。したがって、これらのアプリケーションを適切に動作させ、電話機能を制御できるようにするには、これらのコール機能を無効にする必要があります。これらの機能は、優先順位の高い順に特定の電話機設定、プロファイルを共有する電話機グループに適用できる [Common Device Profile] 設定、企業全体の電話機設定のいずれかで無効にできます。

Cisco Unified IP Phone 8900 および 9900 シリーズの配置に関する考慮事項

Cisco Unified IP Phone 8961、9951、および 9971 は、共通のハードウェアおよびソフトウェア プラットフォーム、強化されたアクセサリのサポート、ユニークなユーザ エクスペリエンスを共有する IP Phone ファミリに属します。ユーザ エクスペリエンスには、保留、転送、会議などの一般的なコール機能用の専用ハード キー、（複数の同時コールをより直感的な処理を容易にする）回線とは別の一連のセッション ボタン、ワイドバンド アコースティック対応ハンドセット、マイク、スピーカーが含まれます。モデルに応じて、この IP Phone ファミリは、タッチ スクリーン、USB および Bluetooth ヘッドセット、SDIO、IEEE 802.11a/b/g 無線インターフェイスなどのさまざまなユーザ アクセサリとハードウェア機能をサポートします。

これらの電話機は SIP シグナリング プロトコルだけを実行し、XSI および Java MIDlet アプリケーションをサポートします。

Cisco Unified IP Phone 8961、9951、および 9971 は、Cisco Unified IP Phone 3900、6900、および 7900 シリーズよりも高度な機能を備えています。これらの電話機を配置するには、次に説明する複数の事項について考慮する必要があります。

ファームウェアのアップグレード

通常、デフォルトでは IP 電話機は、UDP ベースのプロトコルである Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）を使用して 1 つまたは複数の Unified CM サブスクライバ サーバに統合された TFTP サーバからそのイメージをアップグレードします。このようにして、すべての電話機はこれらの TFTP サーバからそのイメージを直接取得します。この方法は、電話機の数が比較的少ない場合や、すべての電話機が実質的に帯域幅の制限がない LAN 環境を持つ単一のキャンパス領域に存在する場合に効果的です。

集中型コール処理を使用する大規模な配置の場合は、低速 WAN リンクで中央データ センターに接続された支社の電話機をアップグレードするのに WAN を介した大量のデータ トラフィックが必要になることがあります。それぞれの電話機に対して同じファイル セットが WAN を複数回通過することになります。このような大量のデータを転送することは WAN 帯域幅を浪費するだけでなく、各データ転送がお互いに帯域幅を求めて競合するため長時間かかることがあります。また、TFTP プロトコルの特性により、一部の電話機でアップグレードが強制的に中止され、既存のバージョンのコードに戻る場合があります。

（注）　7900 シリーズの電話機と異なり、Cisco Unified IP Phone 9900 および 8900 シリーズはアップグレード中にも使用できます。9900 および 8900 シリーズの電話機は、アクティブな状態を保持しつつ、メモリに新しいファームウェアをダウンロードおよび格納します。これらの電話機はダウンロードが正常に行われた後に新しいファームウェアでリブートされます。

WAN を介して電話機をアップグレードすることが必要なため生じた問題を緩和するのに 2 つの方法が存在します。1 つの方法はアップグレードのためだけにローカル TFTP サーバを使用することです。管理者は TFTP サーバを支社（特に大量の電話機が存在する支社あるいは WAN リンクが高速または堅牢でない支社）に設置し、支社の電話機がその特定の TFTP サーバを新しいファームウェアのためだけに使用するように設定できます。この変更により、電話機が新しいファームウェアをローカルに取得します。このアップグレード方法では、管理者が支社の TFTP サーバに電話機のファームウェアを事前にロードし、関連する電話機の設定の「load server」パラメータの TFTP サーバ アドレスを手動で設定する必要があります。支店のルータを TFTP サーバとして使用できることに注意してください。

WAN リソースを大量に使用せずに電話機をアップグレードする 2 つめの方法は、Peer File Sharing（PFS; ピア ファイル共有）機能を使用することです。この機能では、支社の各モデルの 1 つの電話機だけが中央 TFTP サーバからそれぞれの新しいファームウェア ファイルをダウンロードします。電話機がファームウェア ファイルをダウンロードしたら、この電話機はそのファイルを支社の他のすべての電話に配布します。支社に 1 種類の電話機しかない場合は、ファームウェアが WAN 全体で 1 度だけ転送されます。この方法では、load server の方法で必要な手動によるロードと設定を回避できます。

PFS 機能は、同じ支社のサブネット内の電話機が階層形式（チェーン形式）で配置されている場合にアップグレードが要求されると動作します。これは、電話機間でメッセージを交換し、実際にダウンロードを実行する「ルート」電話機を選択することによって行われます。ルート電話機は TCP 接続を使用してチェーンの 2 つめの電話機にファームウェア ファイルを送信し､2 つめの電話機はチェーンの 3 つめの電話機にファームウェア ファイルを送信し、というようにチェーンのすべての電話機がアップグレードされるまでこの作業が繰り返されます。ルート電話機は完全な電話ファームウェアを構成するファイルに応じて異なる場合があることに注意してください。

アップグレード プロセスが完了したら、システム管理者は Unified CM 管理ページ（[Device] -> [Device Settings] -> [Firmware Load Information]）にアクセスして、すべての電話が正常にアップグレードされているかどうかを確認できます。ここでは、デフォルトのイメージ レベルでないすべての電話にフラグが付けられます。

無線インターフェイスを介したネットワーク接続

Cisco Unified IP Phone 9971 には IEEE 802.11a/b/g 無線インターフェイスが搭載されています。この機能により、電話機を配置するうえでの柔軟性が提供されます。ただし、無線アクセス可能によってなこれらの電話機を配置する前に次の点を考慮してください。

- ユーザはネットワーク アクセスのために PC を電話機の PC ポートに接続できない。
- 無線インターフェイスが動作するように電話機背面のネットワーク ポートは未接続のままにしておく。電話機が有線ネットワークを利用可能であることを検出した場合、電話機は無線インターフェイスの接続を解除し、有線接続を使用します。
- 電話機は外部電源により電力供給する必要がある。
- 2.4 GHz 無線と Bluetooth との間には干渉に関する既知の問題が存在する。Bluetooth ヘッドセットと 802.11b/g の共存は可能ですが、コール機能が制限されることがあります。この共存モードではマルチキャスト Music On Hold（MoH; 保留音）がサポートされないことに注意してください。この共存モードが 2.4 GHz IEEE 802.11g で使用される場合、12 Mbps 以上のデータレートで無線インターフェイスを使用することを推奨します。Bluetooth が有効な場合の干渉の問題を避けるためには、5.0 GHz IEEE 802.11a 無線接続を使用することを推奨します。
- 無線アクセス密度を考慮する必要がある。
- 有線モードではファームウェアのダウンロードが低速になることがある。
- 電話機に 2 つの異なる Media Access Control（MAC; メディア アクセス コントロール）アドレスを設定する必要はない。無線と有線の両方の設定には、設定メニューで示された MAC アドレスを使用する必要があります。

- Cisco Emergency Responder は、有線 IP 電話機の場合とは異なりスイッチ ポートではなく IP アドレスだけによってワイヤレス IP 電話機を追跡する。したがって、無線で接続された電話機の場所情報は有線電話機の場合ほど正確ではありません。

Power over Ethernet（PoE）

Cisco Unified IP Phone 9971 および 9951 は、PoE の旧 IEEE 802.3af と新しく策定された 802.3at 標準の両方をサポートします。新しい標準は最大 30 W の電力に対応しています。これらの電話機自体はこの値よりも少ない電力（12.95 W）を消費するため 802.3af 電力標準で対応できます。ただし、Key Extension Module（各 5 W）や USB デバイスなどの電力を消費する他の機器が存在する場合は、IEEE 802.3at 標準が提供できるよりも多くの電力が必要になることがあります。この場合は、コンセントを使用して電話機に電力を供給してください。電話機には、必要な電力が使用できない場合にユーザに警告する電力管理機能があります。

IEEE 802.3at 標準は非常に新しいため、電力を電話機に供給する既存のスイッチをこの新しい標準にアップグレードしなければならないことがあります。

アプリケーション

Cisco Unified IP Phone 8961、9951、および 9971 には CTI を通じて電話機をモニタするアプリケーションによる処理が必要な JTAPI イベントを生成するコール機能が導入されています。これらのコール機能により、ユーザは処理中の転送や会議を中止したり、同じ回線または異なる回線でコールの参加や直接転送を実行したりできます。モニタリング アプリケーションがこれらのイベントを適切に処理するバージョンにアップグレードされていない場合は、アプリケーションが電話のビューやコール状態を電話機自体と同期しなくなるなどの、予期しないアプリケーション動作が発生することがあります。したがって、デフォルトではすべてのアプリケーションはこれらの電話機のモニタまたは制御が制限されています。

これらの新しいイベントを適切に処理するようアップグレードされたアプリケーションやアプリケーションがこれらのイベントの影響を受けないことが確認されたアプリケーションの場合は、管理者がアプリケーションに関連付けられたアプリケーションまたはエンド ユーザ設定で **Standard CTI Allow Control of Phones supporting Connected Xfer and conf** という新しく定義されたロールを有効にできます。このロールが有効にならないと、アプリケーションはこれらの電話機をモニタまたは制御できません。

SRST、Unified CME、および Unified CME as SRST のサポート

Cisco Unified IP Phone 8961、9951、および 9971 は、Unified CM クラスタとの WAN 接続が失われた場合に Survivable Remote Site Telephony（SRST）にフェールオーバーすることがあります。ただし SRST モードで利用可能な機能セットは、電話機が Unified CM に登録されている場合よりもかなり少なくなります。

Cisco Unified Communications Manager Express（Unified CME）または Unified CME as SRST では、現在これらの電話機はサポートされていません。

ビデオのサポート

Cisco Unified IP Phone 9951 および 9971 はビデオ機能を備えているため、ビデオの受信や、（USB がマウントされたカメラを追加して）ビデオの送信を実行できます。これらの電話機のビデオ機能は、Unified CM の各設定ページから、必要に応じて有効化、無効化、または調整できます。9951 および 9971 電話機の設定ページには、USB ポート、ビデオ、および Cisco Camera を有効または無効にするためのコントロール設定があります。電話機にはビデオ ミュート、全画面、ピクチャ イン ピクチャ、

明度、コントラストなどのコントロールがありますが、解像度とフレーム レートは、2 つの電話機に関連付けられたデバイス プールのリージョン間設定によって決まります。目的の解像度およびフレーム レートを達成するには、次の表のビット レート値を使用してください。

表 18-5　Cisco Unified IP Phone 9951 および 9971 の解像度とフレーム レートの設定

解決策	フレーム レート	リージョン間設定のビデオ ビット レート
QCIF	10 fps	60 ～ 79.9 kbps
QCIF	15 fps	80 ～ 99.9 kbps
QCIF	30 fps	100 ～ 249.9 kbps
CIF	15 fps	250 ～ 299.9 kbps
CIF	30 fps	300 ～ 499.9 kbps
VGA	15 fps	500 ～ 799.9 kbps
VGA	24 fps	800 ～ 999.9 kbps

デフォルトでは、ビデオ ビット レート設定は Common Intermediate Format（CIF）で 30 fps（384 kbps）です。ビデオ コールの解像度をこれより高くするには、それに応じてリージョン間帯域幅を調整してください。

同様に、ロケーションベースのコール アドミッション制御は、ビデオ コールの帯域幅を増やす可能性を考慮して設定する必要があります。さらに、カメラが装備されていない Cisco Unified IP Phone 9971 または 9951 に対してビデオ コールを発信した場合、ビデオ送信は一方向だけになりますが、コール アドミッション制御の目的で双方向ビデオ コールとしてカウントされることに注意してください。

ソフトウェアベースのエンドポイント

ソフトウェアベースのエンドポイントには、Cisco Unified Personal Communicator および Cisco IP Communicator があります。ソフトウェアベースのエンドポイントは、クライアント PC にインストールされたアプリケーションであり、登録と管理は Unified CM で行います。

Cisco Unified Personal Communicator

Cisco Unified Personal Communicator は、Microsoft Windows または Macintosh 上で動作するソフトウェア アプリケーションです。Cisco Unified Personal Communicator は、幅広い通信のアプリケーションおよびサービスを 1 つのデスクトップ アプリケーションに統合し、人々が効率的にコミュニケーションできるようにします。Cisco Unified Personal Communicator を使用すると、音声、ビデオ、コール管理、在籍情報、および Web 会議などのさまざまの強力なコミュニケーション ツールにアクセスできます。統合アプリケーションには、Cisco Unified Communications Manager（Unified CM）、Cisco Unified Presence、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、Cisco Unified MeetingPlace Express、Cisco Unified Videoconferencing and MeetingPlace Express VT、および Lightweight Directory Access Protocol（LDAP）バージョン 3（v3）サーバがあります。Cisco Unified Personal Communicator の詳細については、「Cisco Unified Presence」（P.23-1）の章を参照してください。

サーバごとに許可されるデバイスの制限とは関係なく、Unified CM で設定できる最大 CTI デバイス数に制限があります。Cisco Unified Personal Communicator に適用される CTI デバイスの制限は、次のとおりです。

- Cisco Media Convergence Server（MCS）7825 または 7835 の場合、1 台あたり最大 800 台の Cisco Unified Personal Communicator。MCS 7825 または 7835 サーバの場合、1 クラスタあたり最大 3,200 台の Cisco Unified Personal Communicator。
- Cisco Media Convergence Server（MCS）7845 の場合、1 台あたり最大 2,500 台の Cisco Unified Personal Communicator。MCS 7845 サーバの場合、1 クラスタあたり 最大 10,000 台の Cisco Unified Personal Communicator。

上記の Cisco Unified Personal Communicator の最大限度には、次の前提が適用されます。

- 各 Cisco Unified Personal Communicator は、見積もりで 6 コール以下の Busy Hour Call Attempt（BHCA）を処理します。
- CTI デバイスを必要とする他の CTI アプリケーションが、その Unified CM クラスタで設定されていません。

Cisco IP Communicator

Cisco IP Communicator は、コンピュータに IP Phone 機能を与える Microsoft Windows ベースのアプリケーションです。このアプリケーションを使用すると、出張中やオフィス内など、企業ネットワークにユーザがどの場所からアクセスする場合でも高品質の音声コールが可能になります。リモート ユーザと在宅勤務者にとって最適なソリューションです。Cisco IP Communicator は配置が簡単で、現在 IP コミュニケーションで利用可能な最新テクノロジーや先端機能のいくつかが採用されています。

Cisco IP Communicator は SCCP および SIP をサポートするスタンドアロン デバイスであるため、さまざまな IP テレフォニー配置モデルに含まれる IP Phone の設計に関するガイドラインは、Cisco IP Communicator にも当てはまります。詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

サポートされる機能に関するエンド ユーザ環境は、SCCP または SIP のいずれの呼制御シグナリングを使用している場合でも同じです。SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco IP Communicator は、ビデオ コールの発信に関して CiscoUnified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。さらに、SCCP を使用した Cisco IP Communicator は保留トーンをサポートしているのに対し、SIP はサポートしていません。サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco IP Communicator 2.1 は、イメージおよびシグナリング認証をサポートしています。Cisco IP Communicator 2.1 は、認証を使用した Transport Layer Security（TLS）相互認証もサポートし、これにより、Cisco IP Communicator が別の Cisco Unified IP Phone になりすますことができなくなります。Certificate Authority Proxy Function（CAPF）および Locally Significant Certificate（LSC）では、セキュリティを双方向認証で実装されます。Cisco IP Communicator 2.1 は、デバイス認証のための Certificate Trust List（CTL）もサポートしています。

Cisco Unified Client Services Framework

Cisco Unified Client Services Framework（CSF）は、Microsoft Windows ベースのソフトウェア アプリケーションであり、オーディオ、ビデオ、Web コラボレーション、ビジュアル ボイスメールなどの Unified Communications サービスを統合する基礎となるフレームワークをプレゼンスおよびインスタント メッセージング アプリケーションに提供します。Cisco Unified Client Services Framework を使用することで、ユーザは Cisco Unified Communications Manager（Unified CM）、Cisco Unity、Cisco

Unity Connection、Cisco Unified MeetingPlace、および Lightweight Directory Access Protocol（LDAP）バージョン 3（v3）サーバにインターフェイスするさまざまな通信サーバにアクセスできます。Cisco Unified Client Services Framework を使用する Cisco Unified Communications の統合の詳細については、「Cisco Unified Presence」（P.23-1）の章を参照してください。

Cisco Unified Client Services Framework は Cisco Unified CM の新規デバイスであり、ソフトフォン モードまたはデスクフォン モードのいずれかで動作して Unified IP Phone を制御します。

ソフトフォン モードの動作

Cisco Unified Client Services Framework がソフトフォン モードで動作する場合、Cisco Unified CM に新規デバイスを設定する必要があります。すると、Cisco Unified Client Services Framework は SIP ベースの単一回線である Cisco Unified IP Phone として動作し、Cisco Unified IP Phone の完全な登録と冗長性メカニズムをサポートするようになります。

デスクフォン制御モードの動作

Cisco Unified Client Services Framework がデスクフォン制御モードで動作する場合、このアプリケーションでは関連付けられた Cisco Unified IP Phone の制御に CTI/JTAPI（Java Telephony API）が使用されます。Unified Client Services Framework では、Unified CM の Cisco CallManager Cisco IP Phone Services（CCMCIP）サービスを使用して、制御する有効な Cisco Unified IP Phones のリストを提供します。

Cisco Unified Client Services Framework を配置する際は、次の設計上の考慮事項に注意してください。

- 管理者は、組織における Unified Client Services Framework のインストール、配置、および設定方法を決定する必要がある。アプリケーションのインストールには Altris などの有名なインストール パッケージを使用し、TFTP サーバ、CTI Manager、CCMCIP サーバ、ボイスメール パイロット、LDAP サーバ、LDAP ドメイン名、および LDAP 検索コンテキストといった必要なコンポーネントのユーザ レジストリ設定にグループ ポリシーを使用することを推奨します。
- Unified Communications とバックエンドのディレクトリ コンポーネントのシームレスな統合を可能にするため、Cisco Unified Client Services Framework ユーザのユーザ ID とパスワードの設定は、LDAP サーバに保存されているユーザのユーザ ID とパスワードに一致する必要がある。
- Cisco Unified CM のディレクトリ番号設定と LDAP の電話番号属性は、完全な E.164 番号で設定する必要がある。プライベート企業ダイヤル プランを使用できますが、それに伴ってアプリケーション ダイヤル ルールとディレクトリ ルックアップ ルールの使用が必要になる場合があります。
- Cisco Unified IP Phone の制御にデスクフォン モードを使用する場合は、CTI を使用する。したがって、Unified CM 配置のサイジングを行うときは、CTI の使用を必要とする他のアプリケーションも考慮に入れる必要があります。

ビデオ設計上の考慮事項

Cisco Unified Client Services Framework（CSF）では、最大 720p（1280 x 720）解像度の高品位ビデオ コールがサポートされています。高品位ビデオに対応できるように、リージョン間ビット レートが適切に設定されていることを確認してください。また、必要に応じて、ロケーションベースのコール アドミッション制御の帯域幅設定も高品位使用のために調整されていることを確認してください。

Cisco Unified Client Services Framework は、デスクフォン制御モードでビデオに対して使用される場合、CAST プロトコルを使用してデスクフォンとのアソシエーションを確立します。SIP ベースの電話機は、現在、CAST プロトコルをサポートしていないため、この方法で使用することはできません。

Cisco Unified Client Services Framework は、動作しているコンピュータ上でビデオを処理します。デコーディングとエンコーディングの品質は、コンピュータの CPU とメモリ リソースの可用性によって決まります。

ワイヤレス エンドポイント

Cisco ワイヤレス エンドポイントは、ワイヤレス Access Point（AP; アクセス ポイント）経由でワイヤレス LAN（WLAN）インフラストラクチャを使用して、テレフォニー機能を提供します。このタイプのエンドポイントは、エリア内でモバイル ユーザの必要性がある環境で、従来の有線電話機では不適切であったり問題が生じたりする場合に理想的です（ワイヤレス ネットワークの設計の詳細については、「ワイヤレス LAN インフラストラクチャ」（P.3-57）を参照してください）。

シスコでは、次の Voice over WLAN（VoWLAN）IP Phone を提供しています。

- Cisco Unified Wireless IP Phone 7921G
- Cisco Unified Wireless IP Phone 7925G および 7925G-EX
- Cisco Unified Wireless IP Phone 7926G
- Cisco Unified IP Phone 9971

すべてが、組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。Cisco Unified Wireless IP Phone 7921G、7925G、7925G-EX、および 7926G、ならびに無線で接続された Cisco Unified IP Phone 9971 では、ネットワークへの 802.11b 接続、802.11g 接続、または 802.11a 接続が有効になります。Cisco Unified Wireless IP Phone は Skinny Client Control Protocol（SCCP）を使用して Unified CM に登録されますが、Cisco Unified IP Phone 9971 は Session Initiation Protocol（SIP; セッション開始プロトコル）を使用して登録されます。これらの電話機の詳細については、次の Web サイトで入手可能な該当する電話機マニュアルを参照してください。

http://www.cisco.com

サイト調査

Cisco Unified Wireless IP Phone を配置する前に、サイト全体の調査を実行して、無線周波数（RF）カバレッジを提供するのに最適な AP の数と場所を判別する必要があります。サイト調査では、最適なカバレッジを提供するアンテナ タイプや RF 干渉の送信元が存在している可能性がある場所を考慮する必要があります。また、サイト調査では Cisco Unified Wireless IP Phone の Site Survey ツール（7921G、7925G、7925G-EX、および 7926G の場合は [Settings] > [Status] > [Site Survey]、9971 の場合は [Applications Button] > [Administrator Settings] > [Network Setup] > [WLAN Setup] を選択してアクセス）を使用する必要があります。追加のサードパーティ ツールもサイト調査で使用できますが、アンテナの感度と調査アプリケーションの制限によって各エンドポイントまたはクライアント無線の動作が異なるため、Cisco Unified Wireless IP Phone 7921G、7925G、7925G-EX、および 7926G、ならびに Cisco Unified IP Phone 9971 を使用して最終サイト調査を実行することを強く推奨します。

認証

無線の Cisco Unified IP Phone をワイヤレス ネットワークに接続するには、最初に次のいずれかの認証方式を使用して、AP に関連付けて通信する必要があります。

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）

  この方法では、クライアントと EAP 準拠のリモート認証、認可、アカウンティングのサーバとの間に Protected Access Credential（PAC）でセキュア認証トンネルが確立されると、無線で接続された Cisco Unified IP Phone をユーザ名とパスワードで AP に対し 802.1X で認証できます。認証時、ワイヤレス デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。802.1X 認証方式および PAC 認証トンネル交換を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Extensible Authentication Protocol-Transport Layer Security（EAP-TLS）

  この方法では、クライアントと Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）を持つ TLS プロトコルを使用する認証サーバ間でセキュア認証トンネルが確立されると、無線で接続された Cisco Unified IP Phone をユーザ名とパスワードで AP に対し 802.1x で認証できます。認証時、ワイヤレス デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。TLS は、ユーザおよびサーバ認証とダイナミック セッション キーの生成の両方で証明書を使用する機能を提供します。認証に使用される証明書は、製造元でインストールされる証明書（MIC）、またはユーザによりインストールされる証明書のいずれかになります。EAP-TLS は Cisco Unified IP Phone 9971 ではサポートされていません。

- Protected Extensible Authentication Protocol（PEAP）

  この方法では、クライアントと認証サーバとの間で暗号化された SSL/TLS トンネルを通して、ユーザ名とパスワードにより、無線で接続された Cisco Unified IP Phone は AP に対して 802.1x で認証できます。暗号化された SSL/TLS トンネルはサーバ側の公開キー証明書を使用して作成され、Microsoft's Challenge Handshake Authentication Protocol（MS-CHAP）のバージョン 2 を使用した認証情報の交換の暗号化、およびユーザ クレデンシャルの盗難防止を確実にします。認証時、ワイヤレス デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。PEAP は Cisco Unified IP Phone 9971 ではサポートされていません。

- Wi-Fi Protected Access（WPA）

  この方法では、ユーザ名とパスワードによって、無線で接続された Cisco Unified IP Phone を AP に対し 802.1X で認証できます。認証時、ワイヤレス デバイスとの間のトラフィックは Temporal Key Integrity Protocol（TKIP）を使用して暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Wi-Fi Protected Access 2（WPA2）

  この方法は WPA の 802.11i 拡張版であり、ワイヤレス デバイスとの間のトラフィックを暗号化するために、TKIP ではなく、Advanced Encryption Standards（AES; 高度暗号化規格）を使用します。

- Wi-Fi Protected Access Pre-Shared Key（WPA-PSK）

  この方法では、Cisco Unified Wireless IP Phone および AP 上の共有キーの設定により、無線で接続された Cisco Unified IP Phone を AP に対し認証できます。認証時、ワイヤレス デバイスとの間のトラフィックは TKIP を使用して暗号化されます。この認証方法は、企業での配置には推奨しません。

- Wi-Fi Protected Access 2 Pre-Shared Key（WPA2-PSK）

  この方法は WPA-PSK の 802.11i 拡張版であり、ワイヤレス デバイスとの間のトラフィックを暗号化するために、TKIP ではなく、AES を使用します。

- Cisco Centralized Key Management（Cisco CKM）

  この方法では、ユーザ名とパスワードによって、無線で接続された Cisco Unified IP Phone を AP に対し 802.1x で認証できます。認証時、ワイヤレス デバイスとの間のトラフィックは WEP 128 または TKIP を使用して暗号化されます。802.1X 認証方法には、Cisco ACS などの EAP 準拠の RADIUS 認証サーバが必要です。このサーバは、最初の認証要求のためにユーザ データベースへのアクセスを提供します。以降の認証要求は、AP において Wireless Domain Service（WDS; 無線ドメイン サービス）によって検証されるため、再認証時間が短縮され、高速で安全なローミングが保証されます。

- Cisco LEAP

  この方法では、ユーザ名とパスワードに基づいて、無線で接続された Cisco Unified IP Phone と AP を相互に認証できます。認証時に動的なキーが生成され、Cisco Unified Wireless IP Phone と AP の間のトラフィックの暗号化に使用されます。ユーザ データベースへのアクセスを提供するため、Cisco Secure Access Control Server（ACS）などの、LEAP 準拠の Radius 認証サーバが必要です。

- 共有キー

  この方法では、無線で接続された Cisco Unified IP Phone と AP に、静的な 10 文字（40 ビット）または 26 文字（128 ビット）のキーを設定します。この方法は AP ベースの認証方法で、一致するキーがデバイスに存在する場合にネットワークへのアクセスが許可されます。

- Open 認証

  この方法では、ワイヤレス IP 電話機と AP の間で、識別情報を交換する必要はありません。この方法では音声またはシグナリングの安全な交換が提供されず、偽装したデバイスを AP に関連付けることができるため、この方法は*推奨しません*。

キャパシティ

各 AP のキャパシティは、AP 無線タイプ、関連するクライアント無線タイプ、使用可能なデータ レート、およびチャネル使用率などの種々の要素により異なります。

802.11b クライアントを持つ 11 Mbps のデータ レート 802.11b 専用 AP の場合、AP は最大 7 つのアクティブな G.711 音声ストリームまたは 8 つの G.729 ストリームをサポートできます。これらの数を超えると、音声パケットのドロップや遅延、またはコールのドロップが原因で、品質が低下する場合があります。AP レートが 11 Mbps より低く設定されている場合、各 AP のコール キャパシティが低下します。

802.11a を 54 Mbps のデータ レートで使用する場合、アクティブ音声ストリームの最大数は、AP あたり 14 ～ 18 に増加します。

54 Mbps のデータ レートの 802.11g 環境の場合、理論上のアクティブ音声ストリームの最大数も、AP あたり 14 ～ 18 に増加します。ただし、ほとんどの 802.11g 環境は混合されたものであり、802.11b クライアント（したがって 11 Mbps のデータ レート）および 802.11g クライアントが含まれるため、キャパシティは通常かなり低くなり、AP あたりのアクティブ音声ストリームの最大数は 8 ～ 12 になります。

802.11 無線タイプに関係なく、コール キャパシティは、データ トラフィックのためにチャネル使用率が高い場合は低下する場合があります。

コール キャパシティ、無線タイプ、およびデータ レートの詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』の最新バージョンの 設計上の推奨事項を参照してください。

http://www.cisco.com/go/designzone

（注）　同じ AP に関連付けられた 2 台の電話機間のコールは、2 つのアクティブ音声ストリームとしてカウントされます。

これらのアクティブ コール キャパシティの限界と Erlang 比率に基づいて、各 AP がサポートできる Cisco Unified Wireless IP Phone の数を計算できます。たとえば、802.11b クライアントを持つ 802.11b AP で、標準的なユーザ対コールのキャパシティ比率を 3:1 とすると、使用するコーデックが G.711 か G.729 かに応じて、1 つの AP で 21 ～ 24 台の Cisco Unified Wireless IP Phone をサポートできます。また、802.11a クライアントを持つ 54 Mbps のデータ レートの 802.11a AP で、ユーザ対コールのキャパシティ比率を 3:1 とすると、1 つの AP で 42 ～ 54 台の Cisco Unified Wireless IP Phone 7921G をサポートできます。ただし、これらの数には、他の Cisco Unified Wireless IP Phone が AP にローミングする可能性は加味されていません。実際は、AP あたりの電話機の数は上記の数より少なくなります。

これらのキャパシティは、音声アクティビティ検出（VAD）が無効で、パケット化のサンプル サイズが 20 ミリ秒（ms）であることを前提としています。VAD とは、コール中に音声が発生しないときに RTP パケットを送信しないことにより、帯域幅を節約するメカニズムです。ただし、VAD の有効化または無効化は、Unified CM で、クラスタ全体のグローバル設定パラメータで設定します（Unified CM では無音圧縮と呼ばれます）。したがって、無線で接続された Cisco Unified IP Phone で VAD を有効にすると、VAD は Unified CM クラスタ内のすべてのデバイスで有効になります。全体の音声品質を良好に保つため、VAD（無音圧縮）を *disabled* のままにすることを推奨します。

サンプリング レートを 20 ms に設定すると、片方向の音声コールで 50 パケット/秒（pps）が生成されます。通常は、サンプル レートを 20 ms に設定するように推奨します。それより大きいサンプル サイズ（30 または 40 ms）を使用すると、AP あたりの同時コールの数を増分できますが、エンドツーエンドの遅延も大きくなります。また、サンプル サイズを大きくすると、1 つのパケットが失われたときに欠落する会話の量が大きくなるため、ワイヤレス環境で許容される音声パケットの損失率は大幅に減少します。音声サンプリング サイズの詳細については、「帯域幅のプロビジョニング」（P.3-47）を参照してください。

電話機設定

Cisco Unified Wireless IP 電話の設定方法については、次の URL で入手できる Cisco Unified Wireless IP Phones 7921G、7925G、7925G-EX、および 7926G のアドミニストレーション ガイドを参照してください。

http://www.cisco.com/en/US/products/hw/phones/ps379/prod_maintenance_guides_list.html

Cisco Unified Wireless Network 上の Cisco Unified IP Phone 9971 の設定と配置については、次の URL で入手可能な『*Cisco Unified IP Phone 9971 Wireless LAN Deployment Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps10453/tsd_products_support_series_home.html

ローミング

現在、Cisco Unified Wireless IP Phone は、レイヤ 2（同一の VLAN またはサブネット内）にローミングし、引き続きアクティブなコールを保持できます。レイヤ 2 ローミングは、次の状況で発生します。

- 無線で接続された Cisco Unified IP Phone の初期ブートアップ中に、電話機は初めて新しい AP にローミングします。
- 無線で接続された Cisco Unified IP Phone が、現在関連付けられている AP からビーコンまたは応答を受信しない場合、電話機はその AP が使用不可であると見なし、新しい AP へのローミングと関連付けを試行します。
- Cisco Unified Wireless IP Phone と無線で接続された Cisco Unified IP Phone 9971 は利用可能な AP ローミング ターゲットのリストを保持します。現在の AP の状態が変更されると、電話機は、使用可能な AP ローミング ターゲットのリストを参照します。ローミング ターゲットの 1 つが、より適切な選択肢であると判別された場合、電話機はその新しい AP にローミングします。
- 無線で接続された Cisco Unified IP Phone の設定済みの SSID または認証タイプが変更された場合、電話機は AP にローミングして再度関連付けする必要があります。

ローミングで適格な AP ローミング ターゲットの判別を試行するとき、ワイヤレス IP Phone は、次の変数を使用して、関連付ける最適な AP を判別します。

- Relative Signal Strength Indicator（RSSI）

  無線で接続された IP 電話機が、シグナルの長さと、RF カバレッジ エリア内で使用可能な AP の品質を判別するときに使用されます。電話機は、RSSI 値が最高で、認証/暗号化タイプが一致する AP との関連付けを試行します。

- QoS Basic Service Set（QBSS）

  AP が、チャネル使用率情報をワイヤレス電話機に通信するのを可能にします。チャネル使用率が高い AP は VoIP トラフィックを効率的に処理できない場合があるため、電話機は、QBSS 値を使用して、別の AP へのローミングを試行する必要があるかどうかを判別します。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

  WMM TSPEC は 802.11e QoS メカニズムであり、新しい AP が、現在の使用率に基づく、電話機の帯域幅要件を処理できるかどうかを判断するためにローミングしながら、電話機が TSPEC 表示を通して帯域幅および優先順位処理を要求できるようにすることによって、ワイヤレス IP Phone のローミングを支援します。

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を超えて AP から別の AP に移動します。WLAN ネットワーク インフラストラクチャが自律分散型 AP で構成されている場合、Cisco Catalyst 6500 シリーズ Wireless Services Module（WiSM）によって、無線で接続された Cisco Unified Wireless IP Phone は、IP アドレスを保持し、アクティブ コールを維持しながらレイヤ 3 でローミングできます。シームレスなレイヤ 3 ローミングは、クライアントが同じモビリティ グループ内で移動するときだけに行われます。Cisco WiSM およびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な Cisco WiSM 製品資料を参照してください。

http://www.cisco.com

Lightweight アクセス ポイント インフラストラクチャ上のクライアントへのシームレスなレイヤ 3 ローミングは、ダイナミック インターフェイス トンネリングを使用する WLAN コントローラによって実現されます。WLAN コントローラと VLAN にわたってローミングする Cisco Unified Wireless IP Phone は、同じ SSID を使用する場合、IP アドレスを保持できるので、アクティブ コールを維持できます。

WPA や EAP などのより強力な認証方法を使用すると、情報交換の回数が増加し、ローミング中の遅延が大きくなります。遅延の増加を防止するには、Cisco Centralized Key Management（Cisco CKM）を使用して認証を管理します。レイヤ 2 または レイヤ 3 のどちらの場合も、Cisco CKM を使用すれば、検知できる遅延を発生させずにローミングできます。Cisco CKM は、Access Control Server（ACS）に送信する必要がある認証要求の数を減らすことによって、ACS の負荷も軽減します。

（注）　二重帯域 WLAN（2.4 GHz と 5 GHz の両方の帯域を持つ WLAN）では、同じ SSID の 802.11b/g と 802.11a との間でのローミングは、クライアントが両方のボードをサポートできれば可能です。ただし、これにより、音声パスにギャップが発生する場合があります。これらのギャップを防止するには、音声通信に 1 つの帯域だけを使用します。

AP コール アドミッション制御

Unified CM またはゲートキーパー内のコール アドミッション制御メカニズムは、WAN 帯域幅の利用率を制御し、既存のコールの QoS を提供できますが、どちらのメカニズムも、コールの開始時にしか適用されません。静的なデバイス間のコールでは、このタイプのコール アドミッション制御で十分です。しかし、2 つのモバイルワイヤレス デバイス間のコールの場合、ワイヤレス デバイスが 1 つの AP から別の AP へと順にローミングする可能性があるため、AP レベルにもコール アドミッション制御メカニズムが必要です。

Cisco AP およびワイヤレス音声クライアントには、コール アドミッション制御に使用される 2 つのメカニズムがあります。

- QoS Basic Service Set（QBSS）

  QBSS はビーコン情報要素であり、この情報要素により、AP はワイヤレス IP 電話機にチャネル使用率情報を送信します 前述のとおり、電話機はこの QBSS 値を使用して、別の AP にローミングする必要があるかどうかを判別します。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、電話機がその AP にローミングするべきでないことを示しています。

  この QBSS 情報は便利ですが、コールが適切な QoS を保持することを保障するものではなく、またコールを処理するのに十分な帯域幅が存在することを保証するものではないため、真のコール アドミッション制御メカニズムではありません。無線で接続された Cisco Unified IP Phone が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側の電話機に Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、ワイヤレス IP Phone と別のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

- Wi-Fi Multimedia Traffic Specification（WMM TSPEC）

  WMM TSPEC は QoS メカニズムであり、このメカニズムによって、WLAN クライアントはその帯域幅と QoS 要件を通知して、AP がその要件に対応できるようにします。クライアントは、コールを行う準備をする場合、関連付けられた AP に Add Traffic Stream（ADDTS）メッセージを送信して、TSPEC を示します。次に、AP は、帯域幅とプライオリティ処理が使用できるかどうかに応じて、ADDTS 要求を受け入れるかまたは拒否します。コールが拒否された場合、電話機は Network Busy メッセージを受信します。ローミング中、TSPEC をサポートしている通話中のクライアントは、ADDTS メッセージを新しい AP にアソシエーション プロセス の一部として送信して、プライオリティ処理に使用可能な帯域幅を確保します。十分な帯域幅がない場合、ローミングは、隣接する AP が使用可能であれば、それにロードバランスされます。

Bluetooth のサポート

Cisco Unified Wireless IP Phones 7925G、7925G-EX、および 7926G、ならびに Cisco Unified IP Phone 9971 は Bluetooth 対応デバイスです。これらの Cisco Unified IP Phone 内の Bluetooth 無線またはモジュールにより、電話機で Bluetooth ヘッドセットがサポートされるようになります。Bluetooth デバイスは 802.11 b および g デバイスとして同じ 2.4 GHz 無線帯域を使用するため、Bluetooth および 802.11 b または g デバイスが互いに干渉して、接続上の問題が発生する場合があります。

Bluetooth モジュールと 802.11 WLAN モジュールが Cisco Unified Wireless IP Phone 7925G、7925G-EX、および 7926G、ならびに Cisco Unified IP Phone 9971 で共存し、Bluetooth と 802.11b/g 無線との間の無線干渉が大幅に減少する一方で、これらの無線で接続された電話機の Bluetooth 無線は近くに配置されている他の 802.11 b または g デバイスと干渉を起こすことがあります。802.11 b および g WLAN 音声デバイスの干渉または中断（これにより、音質低下、未登録、コール セットアップ の遅延のすべて、またはいずれかが発生する場合があります）の可能性があるため、すべての WLAN 音声デバイスを、5 GHz 無線帯域を使用する 802.11a に配置することを推奨します。ワイヤレス電話機を 802.11a 無線帯域に配置することで、Bluetooth デバイスによって引き起こされる干渉を回避できます。

（注）　Cisco Unified Wireless IP Phone 7925G、7925G-EX、および 7926G で Bluetooth 無線ヘッドセットを使用すると、電話のバッテリ電力消費が増加し、バッテリ寿命が短くなります。

Cisco Unified IP Conference Station

Cisco Unified IP Conference Station は、会議室のスピーカーフォン テクノロジーと、Cisco Unified Communications テクノロジーを結合します。Cisco Unified IP Conference Station は、360 度の室内カバレッジを提供する会議環境に最適です。

Cisco では、次の IP conference phone を提供しています。

- Cisco Unified IP Conference Station 7936
- Cisco Unified IP Conference Station 7937G

どちらの IP conference phone もコール シグナリング プロトコルとして SCCP を使用します。

Cisco Unified IP Conference Station 7936 は、外部スピーカー 1 つと組み込み型のマイク 3 つを備えています。Cisco Unified IP Conference Station 7936 は、バックライト付きのピクセルベース LCD 画面も備えています。大きい部屋でマイクのカバレッジを拡張するため、オプションの拡張マイクも接続できます。

Cisco Unified IP Conference Station 7937G には、ワイドバンド アコースティック、拡張された室内カバレッジ、大型バックライト LCD、および追加ソフトキーが加えられています。Cisco Unified IP Conference Station 7937G は、IEEE 802.3af Power over Ethernet もサポートしており、また、外部電源アダプタ（シスコ部品番号 CP-PWR-CUBE-3）も使用できます。

ビデオ エンドポイント

Cisco Unified CM は、次のタイプのビデオ対応エンドポイントをサポートしています。

- Cisco Unified IP Phone 7911、7940、7941、7942、7945、7960、7961、7962、7965、7970、7971、または 7975 に関連付けられている Cisco Unified Video Advantage、あるいは Skinny Client Control Protocol（SCCP）を実行している Cisco IP Communicator に関連付けられている Cisco Unified Video Advantage
- オプションの USB カメラが接続された Cisco Unified IP Phone 9971 および 9951。カメラがない場合、これらの電話機はビデオの受信だけできます。
- Cisco IP Video Phone 7985
- Cisco E20 Video Phone
- SCCP を実行している Tandberg 社製 2000 MXP、1500 MXP、1000 MXP、770 MXP、550 MXP、T-1000、および T-550 モデル
- SCCP を実行している Sony 社製 PCS-1、PCS-TL30、および PCS-TL50 モデル
- H.323 および SIP クライアント（Polycom、Sony、PictureTel、EyeBeam、Tandberg、VCON、VTEL、Microsoft NetMeeting など）
- Cisco Unified Personal Communicator（ソフトフォン モードで動作）
- Cisco Unified Client Services Framework（CSF）クライアント
- Skinny Client Control Protocol（SCCP）を実行する Cisco Unified IP Phone 7941、7942、7945、7961、7962、7965、7971、または 7975 に関連付けられた Cisco Unified Personal Communicator および Cisco Unified Client Services Framework（CSF）クライアント（デスクフォン モードで実行）

Cisco Unified Video Advantage

Cisco Unified Video Advantage は、Windows 2000、Windows XP、または Windows Vista が動作しているパーソナル コンピュータにインストールできる Windows ベースのアプリケーションおよび USB カメラです。Skinny Client Control Protocol を実行している Cisco Unified IP Phone 7911、7940、7941、7942、7945、7960、7961、7962、7965、7970、7971 または 7975 の PC ポートに PC を物理的に接続すると、Cisco Unified Video Advantage アプリケーションは電話機と「アソシエーション」を行い、それによってユーザはいつもの電話操作が可能になり、ビデオ機能も追加されます。Cisco Unified Video Advantage Release 2.0 では、このアソシエーションを同じ PC 上で SCCP を実行している Cisco IP Communicator にも関連付けることもできます。

システム管理者は、このアソシエーションをどの IP Phone に許可するかを制御するために、Unified CM Administration の IP Phone 設定ページで [Video Capabilities: Enabled/Disabled] 設定の切り替えを行います。この機能を有効にすると、カメラを表すアイコンが IP Phone ディスプレイの右下に表示されます。デフォルトでは、Cisco Unified Video Advantage は無効になっています。Bulk Administration Tool を使用すると、この設定を多数の電話機で一度に修正することもできます。注意する点としては、Cisco Unified Video Advantage がハードウェア IP Phone で動作するには [PC Port: Enabled/Disabled] 設定も有効にする必要がありますが、[PC Access to Voice VLAN] 設定を有効にする必要はありません。

上記のハードウェア IP Phone とのアソシエーションのために、Cisco Unified Video Advantage は Cisco Discovery Protocol（CDP; シスコ検出プロトコル）ドライバを PC のイーサネット インターフェイスにインストールします。CDP を使用すると、PC と ハードウェア IP Phone は相互に自動検出できるようになります。このため、Cisco Unified Video Advantage を動作させるために、ユーザは PC ま

たは ハードウェア IP Phone 上で何も設定する必要はありません。したがって、ユーザがビデオ対応ハードウェア IP Phone に PC を差し込めば、自動的にアソシエーションが行われます（図 18-1 を参照）。

Cisco Unified Video Advantage 2.0 は、同じ PC 上で SCCP を実行している Cisco IP Communicator 存在を検出するために CDP を使用することはありません。代わりに、Cisco IP Communicator プロセスから送信されたプライベート Windows メッセージを監視します。Cisco IP Communicator が検出されると、アソシエーション プロセスは、ハードウェア IP 電話機に対する場合とまったく同じ動作をします（図 18-2 を参照）。

（注）　Cisco Unified Video Advantage をインストールすると、CDP パケット ドライバが PC のすべてのイーサネット インターフェイスにインストールされます。新しい Network Interface Card（NIC; ネットワーク インターフェイス カード）を追加するか、古い NIC を新しいものと置き換えたときは、Cisco Unified Video Advantage を再インストールして、CDP ドライバが新しい NIC にもインストールされるようにしてください。

図 18-1　Cisco Unified Video Advantage の動作の概要

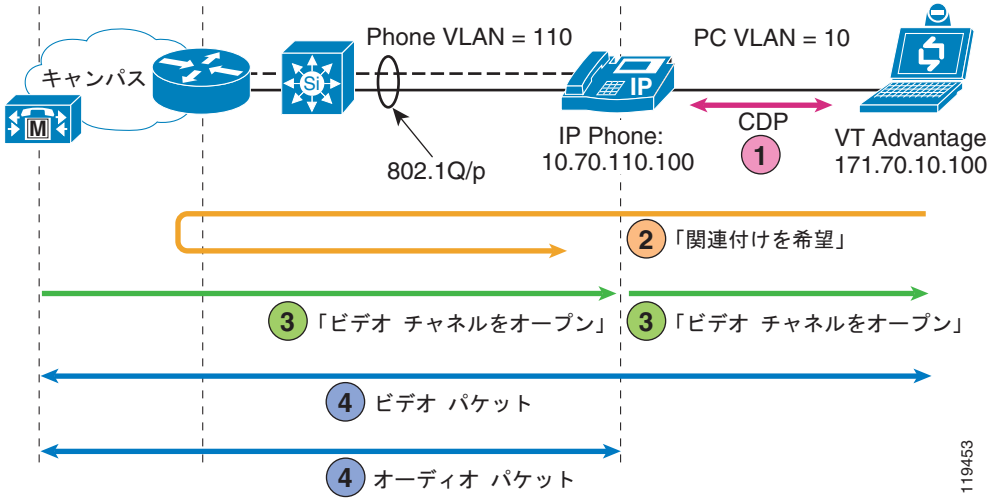


図 18-1 は次のイベントを示しています。

1. IP Phone と PC exchange Cisco Discovery Protocol（CDP）メッセージ。電話機は、その隣接した CDP ネイバーの IP アドレスから TCP ポート 4224 の PC アソシエーション パケットを監視します。
2. PC は、アソシエーション メッセージを電話機に TCP/IP で開始します。アソシエーション パケットは、VLAN 間 でレイヤ 3 までルーティングされます。ファイアウォールと Access Control List（ACL; アクセス コントロール リスト）の両方またはいずれかは、TCP ポート 4224 を許可する必要があります。
3. 電話機は、Cisco Unified Video Advantage と Unified CM の間で SCCP プロキシとして機能します。Unified CM は、コール用のチャネルをオープンするように電話機に指示し、電話機は PC に対してそのメッセージのプロキシを行います。
4. 電話機は音声を送受信し、PC はビデオを送受信します。音声トラフィックもビデオ トラフィックも、DSCP AF41 としてマーキングされています。ビデオ トラフィックは UDP ポート 5445 を使用します。

図 18-2　Cisco IP Communicator の Cisco Unified Video Advantage への関連付け

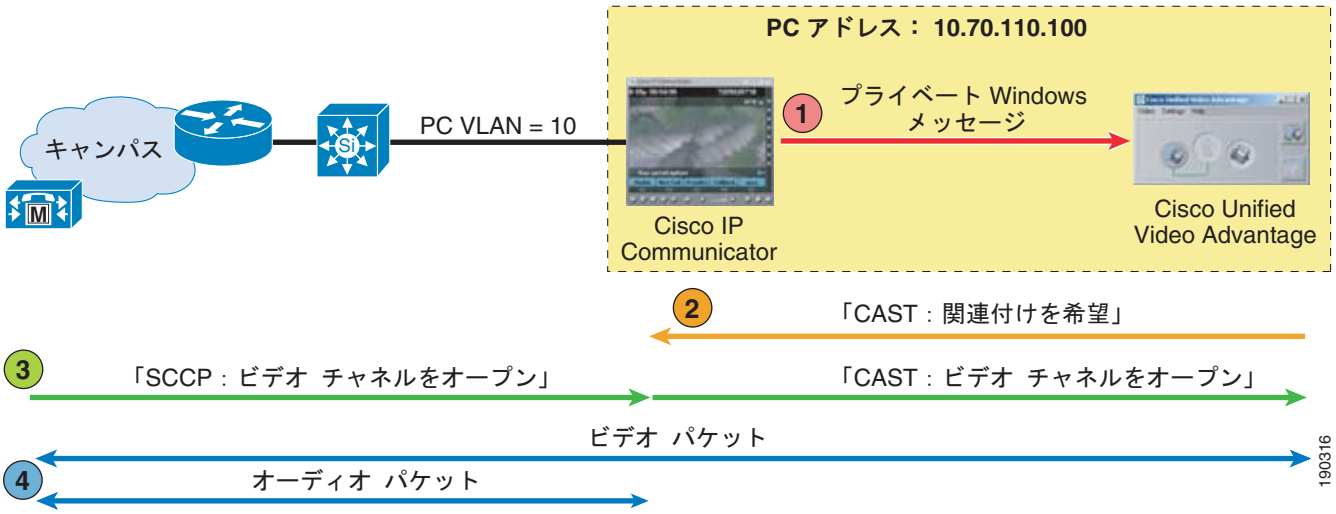


図 18-2 は次のイベントを示しています。

1. Cisco IP Communicator は、プライベート Windows メッセージを Cisco Unified Video Advantage に送信します。このメッセージには、Cisco IP Communicator の IP アドレスと CAST メッセージのポート番号が含まれています。
2. Cisco Unified Video Advantage は、CAST メッセージを Cisco IP Communicator に TCP/IP で開始します。CAST メッセージは接続アドレスであるため、PC から出力されません。
3. Cisco IP Communicator は、Cisco Unified Video Advantage と Unified CM との間の SCCP プロキシとして機能します。Unified CM は、IP Communicator にコール用のビデオ チャネルをオープンするように指示し、IP Communicator は、CAST プロトコル を介して Cisco Unified Video Advantage にそのメッセージのプロキシを行います。
4. Cisco IP Communicator は音声を送受信し、Cisco Unified Video Advantage はビデオを送受信します。音声トラフィックもビデオ トラフィックも、DSCP AF41 としてマーキングされています。ビデオ トラフィックは UDP ポート 5445 を使用します。

Cisco Unified Video Advantage を使用したコールの発信では、オーディオは IP Phone で処理されますが、ビデオは PC で処理されます。2 台のデバイス間に同期メカニズムが存在しないため、ジッタ、遅延、断片化パケット、および不良パケットを最小限に抑えるために QoS が不可欠です。

ハードウェア IP Phone を使用する場合、電話機 は音声 VLAN 内に存在しますが、PC はデータ VLAN 内に存在します。つまり、アソシエーションが行われるために、レイヤ 3 のルーティング パスが音声 VLAN とデータ VLAN の間に必要です。これらの VLAN の間にアクセス コントロール リスト（ACL）またはファイアウォールがある場合は、アソシエーション プロトコル（両方向で TCP ポート 4224 を使用）の通過を許可するように設定する必要があります。Cisco IP Communicator を使用すると、この通信が PC 内で発生し、通過するレイヤ 3 境界はありません。

Cisco Unified Video Advantage は、Differentiated Services Code Point（DSCP）によるトラフィックの分類をサポートしています。Unified CM は、電話機に送信する SCCP メッセージに DSCP 値を指定します。オーディオだけのコールの発信時に IP Phone は、SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィックに DSCP EF とマーキングします。ただし、ビデオ コールの発信時には、IP Phone は SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィックに DSCP AF41 とマーキングし、Cisco Unified Video Advantage アプリケーションからはビデオ RTP メディア トラフィックにも DSCP AF41 とマーキングされます。IP Phone と Cisco Unified Video Advantage アプリケーションの両方が「アソシエーション」プロトコル メッセージに DSCP CS3 とマーキングするのは、それがシグナリング トラフィックであると考慮され、SCCP など、他のすべてのシグナリング トラフィックと一緒にグループ分けされるためです。

（注）　Cisco Unified IP Phone 7970 および 7971 は、Transport Layer Security（TLS）および Secure RTP（SRTP）を使用して、シグナリング トラフィックとオーディオ メディア トラフィックの認証と暗号化が行えます。アソシエーション プロトコルでは、この認証または暗号化が使用されることはなく、ビデオ RTP メディア ストリームが暗号化されることもありません。ただし、SCCP シグナリングとオーディオ RTP メディア ストリームは、暗号化が設定されていれば暗号化されます。

（注）　音声 VLAN をデータ VLAN と同じ設定にしないでください。接続に問題が起きる可能性があります。

考慮すべき点として、Cisco Unified Video Advantage は、PC 上で実行する他のアプリケーションと同様に、システム パフォーマンスに実際に影響します。Cisco Unified Video Advantage 1.0 は、H.263 と Cisco VT Camera ワイドバンド ビデオ コーデックという、2 タイプのビデオ コーデックをサポートしています。Cisco Unified Video Advantage 2.0 は、H.263 と H.264 という、2 タイプのコーデックをサポートしています。Cisco VT Camera ワイドバンド ビデオ コーデックでは、PC への要求が最少になりますが、ネットワークへの要求は最多になります。H.263 では、ネットワークへの要求は少なく、PC への要求は多くなります。最後に、H.264 では、ネットワークへの要求が最少になりますが、PC への要求は最多になります。したがって、利用可能な帯域幅がネットワークに豊富にある場合は、Cisco VT Camera ワイドバンド ビデオ コーデックを使用すると PC 上で CPU およびメモリ リソースを節約できます。

H.263 および H.264 のコーデックは、最高 1.5 Mbps までの範囲をサポートしています。要約すると、Cisco Unified Video Advantage を配置するときに、お客様が PC パフォーマンスとネットワーク使用率のバランスを取る必要があります。

システム要件

PC 要件の詳細については、次の Web サイトで入手可能な『*Cisco Unified Video Advantage Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps5662/products_data_sheet0900aecd8044de04.html

Cisco IP Video Phone 7985G

Cisco IP Video Phone 7985G は、パーソナル デスクトップ ビデオ電話機です。PC 上で実行するアプリケーションである Cisco Unified Video Advantage とは異なり、Cisco IP Video Phone 7985G は、ビデオ機能が統合された独立型の電話機です。この電話機は、ビデオ コールの発信用に 8.4 インチのカラー LCD 画面とビデオ カメラを備えています。最高 8 つのライン アピアランスをサポートし、2 つの 10/100 Base-T イーサネット接続と、Directories、Messages、Settings、および Services の各ボタンを備えています。他の Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は CDP を使用して VLAN および CoS の情報を接続スイッチから取得し、802.1p/q マーキングで使用します。

Cisco Unified IP Phone 9971 および 9951

Cisco Unified IP Phone 9971 および 9951 は、ネイティブで画面上にビデオを受信および表示する機能を備えています。特別に設計されたオプションの USB カメラを接続すれば、ビデオを伝送することもできます。これらの電話機の両方の画面には、QCIF（176 x 144）（10 fps）から VGA（640 x 480）

（24 fps）に至るまで、さまざまなビデオ解像度とフレーム レートが表示されます。ベース電話機が着信ビデオ ストリームをデコードして表示し、カメラがリモート エンドへの転送のためにビデオをエンコードします。

カメラ接続の電力所要量が増えたため、これらの電話機には、802.3AF PoE インターフェイスまたは AC アダプタを使用して電力を供給する必要があります。

Cisco E20 Video Phone

Cisco E20 Video Phone は、ビデオ機能と統合された個人のスタンドアロン型デスクトップフォンです。この電話機は、ビデオ コールの発信用に 10.6 インチの LCD 画面とビデオ カメラを備えています。また、単一ライン アピアランスをサポートし、2 つの 10/100/1000 Base-T イーサネット接続があります。この電話はワイドバンド オーディオ ヘッドセット、スピーカー、およびハンドセットを組み込み、XML アプリケーションをサポートしています。

サポートされる機能の全リストについては、「エンドポイント機能の要約」（P.18-53）を参照してください。

Cisco E20 Video Phone は通常、Tandberg VCS 呼制御と共に配置されます。ただし、Cisco E20 Video Phone は、最新のファームウェア リリースと Unified CM 8.5 を使用している場合、Cisco SIP ビデオ フォンとして直接 Cisco Unified CM に登録できます。Cisco E20 Video Phone は、Unified CM 8.0 を使用している場合、サードパーティ SIP エンドポイントとして Unified CM に直接登録する機能しかありません。

Cisco E20 Video Phone の製品マニュアルについては、http://www.tandberg.com を参照してください。

Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、Cisco Unified IP Phone 9971 および 9951、ならびに Cisco E20 Video Phone でサポートされるコーデック

表 18-6 に、Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、Cisco Unified IP Phone 9951 および 9971、ならびに Cisco E20 Video Phone でサポートされるコーデックを示します。

表 18-6　Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、Cisco Unified IP Phone 9971 および 9951、ならびに Cisco E20 Video Phone でサポートされるコーデック

コーデックまたは機能	Cisco Unified Video Advantage	Cisco IP Video Phone 7985G	Cisco Unified IP Phone 9951	Cisco Unified IP Phone 9971	Cisco E20 Video Phone
H.264	あり（Release 2.0）	あり	あり	あり	あり
H.263	あり	あり	なし	なし	あり
H.261	なし	あり	なし	なし	なし
G.711	あり	あり	あり	あり	あり
G.722	なし	あり	あり	あり	あり
G.722.1	なし	なし	なし	なし	あり
G.723.1	なし	なし	なし	なし	なし
G.728	なし	なし	なし	なし	なし
G.729	あり	あり	あり	あり	あり

表 18-6　Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、Cisco Unified IP Phone 9971 および 9951、ならびに Cisco E20 Video Phone でサポートされるコーデック（続き）

コーデックまたは機能	Cisco Unified Video Advantage	Cisco IP Video Phone 7985G	Cisco Unified IP Phone 9951	Cisco Unified IP Phone 9971	Cisco E20 Video Phone
最高帯域幅	Release 1.0 の場合は 7 Mbps、Release 2.0 の場合は 1.5 Mbps	768 kbps	1 Mbps	1 Mbps	1.152 Mbps
ビデオ解像度	CIF、QCIF	NTSC：4SIF、SIF PAL：4CIF、QCIF、SQCIF	QCIF、CIF、VGA	QCIF、CIF、VGA	**送受信：** 768x448@30fps（w448p） 576x448@30fps（448p） 512x288@30fps（w288p） 352x288@30fps（CIF） 176x144@30fps（QCIF） **受信のみ：** 1024x768@7.5fps（XGA） 1024x576@7.5fps（w576） 800x600@7.5fps（SVGA） 704x480@15fps（4SIF） 704x576@15fps（4CIF） 640x480@15fps（VGA） 352x240@30fps（SIF）

サードパーティ製 SCCP ビデオ エンドポイント

ビデオ エンドポイントの 2 つの製造業者である Sony 社と Tandberg 社は現在、次の製品で Cisco Skinny Client Control Protocol（SCCP）をサポートしています。Sony 社製と Tandberg 社製の両方のエンドポイントでの SCCP は Cisco Unified IP Phone 7940 での SCCP に従ってモデル化されています。複数のライン アピアランス、ソフトキー、およびボタン（Directories、Messages、Settings、Services）など、Cisco Unified IP Phone 7940 ユーザ インターフェイスにある機能のほとんどが、Sony 社製エンドポイントと Tandberg 社製エンドポイントでもサポートされています。Sony 社製と Tandberg 社製のエンドポイントは、TFTP サーバの IP アドレス検出用に DHCP の Option 150 フィールドもサポートし、TFTP サーバから設定をダウンロードします。ただし、Sony 社製および Tandberg 社製のエンドポイントのソフトウェア アップグレードは、TFTP を介しては行われません。代わりに、ベンダーから提供されるツールを使用して、お客様が各エンドポイントを手動でアップグレードする必要があります（Tandberg 社製では FTP による方法が使用され、Sony 社製では FTP または物理メモリ

スティックが使用されます）。Sony 社製および Tandberg 社製のエンドポイントは、最大で 3 台の Unified CM サーバに登録され、1 次サーバが通信不能になったときに、2 次サーバまたは 3 次サーバにフェールオーバーします。

Sony 社製および Tandberg 社製のエンドポイントは Cisco Unified IP Phone 7940 および 7960 のソフトキー機能と類似したソフトキー機能をサポートしていますが、実際の機能サポートはベンダーおよびモデルによって異なります。サポートされる機能については、製造業者のマニュアルで確認してください。現在、一部のプラットフォーム上にない機能として、次のものがあります。

- Messages ボタン
- Directories ボタン（発信コール、受信コール、不在コール、および社内ディレクトリ）
- Settings ボタンと Services ボタン
- 一部の XML サービス（エクステンション モビリティや Berbee InformaCast など）

Sony 社製および Tandberg 社製のエンドポイントは SCCP を使用するため、エンドポイントでのビデオ コールのダイヤルは、Cisco Unified IP Phone でのオーディオ コールのダイヤルと似ています。Cisco Unified IP Phone に慣れているユーザであれば、Sony 社製および Tandberg 社製のエンドポイントも直感的に使いこなせるはずです。ユーザ インターフェイスの主な相違点は、Sony 社製および Tandberg 社製のエンドポイントに電話機のようなボタン キーパッドや受話器がないことです。代わりに、リモート コントロールを使用して機能にアクセスし、番号をダイヤルします。

（注）　Sony 社製および Tandberg 社製のエンドポイントは、Cisco Discovery Protocol（CDP）または IEEE 802.Q/p をサポートしていません。したがって、その接続先のイーサネット スイッチで、VLAN ID および Quality of Service の信頼境界を手動で設定する必要があります（詳細については、「ネットワーク インフラストラクチャ」（P.3-1）を参照してください）。

Sony 社製と Tandberg 社製の SCCP エンドポイントでサポートされているコーデック

サードパーティ製 SCCP エンドポイントのコーデック サポートは、ベンダー、モデル、およびソフトウェア バージョンによって異なります。サポートされるコーデックについては、ベンダーの製品マニュアルで確認してください。

サードパーティ製 SIP IP Phone

サードパーティ製電話機には、機能アクセス ボタン（固定または可変）など、呼制御シグナリング プロトコルとは関係しない、固有のローカル機能が備わっています。基本的な SIP RFC サポートでは、特定のデスクトップ機能が Cisco Unified IP Phone と同じになるように対応し、特定機能の相互運用性にも対応します。ただし、これらのサードパーティ製 SIP 電話機は、Cisco Unified IP Phone の機能をフル装備しているわけではありません。

シスコは、新しい Unified CM および Cisco Unified Communication Manager Express（Unified CME）の SIP 機能を利用するソリューションの開発に携わっている、Cisco Technology Development Partner Program の一員としての主要なサードパーティ ベンダーと協力して活動しています。このようなベンダーとしては、IPCelerate（教育スペース用の統一クライアント）、RIM（Blackberry 7270 ワイヤレス LAN ハンドセット）、および IP blue（ソフトフォン）があります。シスコは、サードパーティ ベンダーの Grandstream とも協力して Grandstream GXP 2000 のテストを行い、相互運用性を保証しています。

シスコは、tekVizion が提供する独立したサードパーティのテストおよび相互運用性検証プロセスにも参加しています。tekVizion が提供するこの独立サービスは、サードパーティ ベンダーのエンドポイントが Unified CM および Unified CME との相互運用性をテストおよび検証できるようにするために確立されました。

シスコの回線側 SIP 相互運用性およびサードパーティ検証の詳細については、http://www.cisco.com を参照してください。

QoS の推奨事項

この項では、IP テレフォニー エンドポイントで配置される一般的な Cisco Catalyst スイッチでの、基本的な QoS ガイドラインおよび設定について説明します。詳細については、次の Web サイトで入手可能な『*Quality of Service*』を参照してください。

http://www.cisco.com/go/designzone

Cisco VG224 および VG248

アナログ ゲートウェイは、信頼できるエンドポイントです。Cisco VG224 および VG248 ゲートウェイの場合、VG248 パケットの DSCP 値を信頼するようにスイッチを設定します。次の項では、Cisco VG224 および VG248 アナログ ゲートウェイで配置される一般的な Cisco Catalyst スイッチを設定するためのコマンドをリストします。

（注）　次の項では、*vvlan_id* は Voice VLAN ID を表し、*dvlan_id* はデータ VLAN ID を表します。

Cisco 2950

```
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust dscp
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport access vlan vvlan_id
```

（注）　**mls qos trust dscp** コマンドは、Enhanced Image（EI）でだけ使用できます。

Cisco 2970 または 3750

```
CAT2970(config)#mls qos
CAT2970(config)interface interface-id
CAT2970(config-if)#mls qos trust dscp
CAT2970(config-if)#switchport mode access
CAT2970(config-if)#switchport access vlan vvlan_id
```

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)interface interface-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#switchport mode access
Cat3550(config-if)#switchport access vlan vvlan_id
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)#qos
CAT4500(config)interface interface-id
CAT4500(config-if)#qos trust dscp
CAT4500(config-if)#switchport mode access
CAT4500(config-if)#switchport access vlan vvlan_id
```

Cisco 6500

```
CAT6500>(enable)set qos enable
CAT6500>(enable)set port qos 2/1 vlan-based
CAT6500>(enable)set vlan vvlan_id mod/port
CAT6500>(enable)set port qos mod/port  trust trust-dscp
```

Cisco ATA 186 および IP Conference Station

Cisco Analog Telephone Adaptor（ATA）186 および IP Conference Station は、信頼されているエンドポイントであるため、それらの QoS 設定は、「Cisco VG224 および VG248」（P.18-36）の項で説明されている設定とまったく同じです。

Cisco ATA 188 および IP Phone

Cisco Analog Telephone Adaptor（ATA）188 および IP Phone の場合、Voice VLAN をデータ VLAN から分離することを推奨します。Cisco ATA 186、7902、7905、7906、7910、および IP Conference Station の場合は、従来どおり、Voice VLAN とデータ VLAN を分離することと、Auxiliary VLAN を設定することを推奨します。これにより、同じアクセス レイヤの設定を、異なる IP Phone モデルや ATA に使用できます。またエンド ユーザは、IP Phone または ATA を、スイッチ上の異なるアクセス ポートに接続して、同じ処理を受けることができます。Cisco ATA 186、7902、7905、7906、7910、および IP Conference Station の場合、これらのデバイスは PC に接続されていないため、接続された PC からのフレームの CoS 値を上書きするためのコマンドは何の効果もありません。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の IP Phone に対して実行できるコンフィギュレーション コマンドをリストします。

Cisco 2950

```
CAT2950(config)#
CAT2950(config)#class-map VVLAN
CAT2950(config-cmap)# match access-group name VVLAN
CAT2950(config-cmap)#class-map DVLAN
CAT2950(config-cmap)# match access-group name DVLAN
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map IPPHONE-PC
CAT2950(config-pmap)# class VVLAN
CAT2950(config-pmap-c0#  set ip dscp 46
CAT2950(config-pmap-c)#  police 1000000 8192 exceed-action-drop
CAT2950(config-pmap)# class DVLAN
CAT2950(config-pmap-c0#  set ip dscp 0
CAT2950(config-pmap-c)#  police 5000000 8192 exceed-action-drop
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust device cisco-phone
CAT2950(config-if)#mls qos trust cos
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport voice vlan vvlan_id
CAT2950(config-if)#switchport access vlan dvlan_id
CAT2950(config-if)#service-policy input IPPHONE-PC
CAT2950(config-if)#exit
CAT2950(config)#
```

```
CAT2950(config)#ip access-list standard VVLAN
CAT2950(config-std-nacl)# permit voice_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#exit
CAT2950(config)#ip access-list standard DVLAN
CAT2950(config-std-nacl)# permit data_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#end
```

（注）　**mls qos map cos-dscp** コマンドは、Enhanced Image（EI）でだけ使用できます。Standard Image（SI）では、このコマンドを使用できません。CoS から DSCP へのデフォルトのマッピングは、次のとおりです。

CoS 値	0	1	2	3	4	5	6	7
DSCP 値	0	8	16	24	32	40	48	56

Cisco 2970、3560 または 3750

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map IPPHONE-PC
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# switchport access vlan dvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input IPPHONE-PC
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
```

```
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 2443 dscp cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
CAT2970#
```

Cisco 3550

```
CAT3550(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT3550(config)# mls qos map policed-dscp 0 24 26 46 to 8
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)# match ip dscp 46
CAT3550(config-cmap)#class-map match-all CALL SIGNALING
CAT3550(config-cmap)# match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map CALL SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)# match access-group name ACL_Name
CAT3550(config-cmap)#
CAT3550(config-cmap)# class-map match-all VVLAN-ANY
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)# match vlan dvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE-PC
CAT3550(config-pmap)# class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class DVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#exit
CAT3550(config-pmap)#exit
CAT3550(config)#interface interface-id
CAT3550(config-if)# switchport voice vlan vvlan_id
CAT3550(config-if)# switchport access vlan dvlan_id
CAT3550(config-if)# mls qos trust device cisco-phone
CAT3550(config-if)# service-policy input IPPHONE-PC
```

```
CAT3550(config-if)# exit
CAT3550(config)#
CAT3550(confiig)#ip access list standard ACL_ANY
CAT3550(config-std-nacl)# permit any
CAT3550(config-std-nacl)# end
CAT3550#
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)# qos map cos 5 to dscp 46
CAT4500(config)# qos map cos 0 24 26 46 to dscp 8
CAT4500(config)#
CAT4500(config)#class-map match-all VVLAN-VOICE
CAT4500(config-cmap)# match access-group name VVLAN-VOICE
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT4500(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-ANY
CAT4500(config-cmap)# match access-group name VVLAN-ANY
CAT4500(config-cmap)#
CAT4500(config-cmap)# policy-map IPPHONE-PC
CAT4500(config-pmap)#class VVLAN-VOICE
CAT4500(config-pmap-c)# set ip dscp 46
CAT4500(config-pmap-c)# police 128 kps 8000 byte exceed-action drop
CAT4500(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT4500(config-pmap-c)# set ip dscp 24
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class VVLAN-ANY
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class class-default
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 5 mpbs 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# exit
CAT4500(config-pmap)# exit
CAT4500(config)#
CAT4500(config)#
CAT4500(config)#interface interface-id
CAT4500(config-if)# switchport voice vlan vvlan_id
CAT4500(config-if)# switchport access vlan dvlan_id
CAT4500(config-if)# qos trust device cisco-phone
CAT4500(config-if)# service-policy input IPPHONE-PC
CAT4500(config-if)# exit
CAT4500(config)#
CAT4500(confiig)#ip access list extended VVLAN-VOICE
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 2443 dscp cs3
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-ANY
CAT4500(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT4500(config-ext-nacl)# end
CAT4500#
```

Cisco 6500

```
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate VVLAN-VOICE rate 128 burst 8000 drop
CAT6500> (enable) set qos policer aggregate VVLAN-CALL-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate VVLAN-ANY rate 5000 burst 8000 policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 46 aggregate VVLAN-VOICE udp
Voice_IP_Subnet Subnet_Mask any range 16384 32767
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any  range 2000 2002
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any eq 2443
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Wildcard_bits any  range 5060 5061
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING udp
Voice_IP_Subnet Wildcard_bits  any  eq 5060
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate VVLAN-ANY Voice_IP_Subnet
Subnet_Mask any
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl IPPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust-device ciscoipphone
CAT6500> (enable) set qos acl map IPPHONE-PC mod/port
CAT6500> (enable)
```

（注）　DSCP の再マーキングは、レイヤ 3 対応のスイッチが行う必要があります。アクセス レイヤ スイッチ（Cisco Catalyst 2950 with Standard Image または Cisco 3524XL など）にこの機能がない場合、DSCP の再マーキングは分散レイヤ スイッチで行う必要があります。

ソフトウェアベースのエンドポイント

Cisco Unified Personal Communicator および Cisco Unified Video Advantage を搭載した Cisco IP Communicator は両方とも音声とビデオの機能を備えており、パケット分類および DSCP 再マーキング用の ACL とポリシー マップを使用する場合に、2 つの問題が生じます。第 1 に、Cisco Unified Personal Communicator は、ソース音声とビデオ ストリームに対して、同じ IP アドレスと UDP ポート範囲を使用します。IP アドレス と ポート番号に基づく ACL は、適切な DSCP 再マーキング を適用するために音声コールとビデオ コールを区別するほど十分にきめ細かく対応していません。第 2 に、Cisco IP Communicator は、その音声パケットを送信するために、同じ IP アドレス と UDP ポートを使用します。同様に、ACL は、音声専用コールのボイス ストリームと、ビデオ コールのボイス ストリームを区別するほど十分にきめ細かく対応していません。したがって、パケット分類および DSCP 再マーキングのために ACL とポリシー マップを使用することは、ソフトウェア ベースのエンドポイントに適した QoS ソリューションにはなりません。

Cisco Unified Personal Communicator も Cisco Unified Video Advantage を搭載した Cisco IP Communicator も、シグナリング パケットおよびメディア パケットを、ネットワークに入力されるにつれて正しくマーキングするため、着信トラフィックの DSCP マーキングを信頼してトラフィック ポリシーとレート制限を適用するようにポリシー マップを設定することを推奨します。次の項では、一般的に配置されている Cisco Catalyst スイッチ上の Cisco Unified Personal Communicator および Cisco IP Communicator に対して実行できるコンフィギュレーション コマンドをリストします。

（注）　Cisco Catalyst 2950 シリーズ スイッチを、ソフトウェアベースのエンドポイント QoS の実装で使用することは推奨されていません。その理由は、Cisco 2950 が、FastEthernet ポートで 1 Mbps の増分だけサポートしているからです。これにより、許可されていないネットワーク トラフィックにかなり大きいホールが発生し、コール シグナリングまたはメディアの模倣が発生することがあります。

Cisco 2970、3560 または 3750

```
CAT2970 (config)#mls qos
CAT2970 (config)#mls qos map policed-dscp 0 24 26 46 to 8
CAT2970 (config)#
CAT2970 (config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-cmap)#  match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-cmap)#  match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-cmap)#exit
CAT2970 (config)#
CAT2970 (config)#policy-map SOFTWARE-BASED-ENDPOINT
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-pmap-c)# police 50000000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)#class class-default
CAT2970 (config-pmap-c)# set ip dscp 0
CAT2970 (config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c)# exit
CAT2970 (config-pmap)#exit
CAT2970 (config)#
CAT2970 (config)#interface FastEthernet interface-id
CAT2970 (config-if)# switchport access vlan dvlan_id
CAT2970 (config-if)# switchport mode access
CAT2970 (config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
CAT2970 (config-if)# exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
CAT2970 (config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
CAT2970 (config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
CAT2970 (config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
CAT2970 (config-ext-nacl)#exit
CAT2970 (config)#exit
```

Cisco 3550

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
```

```
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 34, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-VOICE rate 128 burst
8000 drop
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-VIDEO rate 5000 burst
8000 policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-SIGNAL rate 32 burst
8000 policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTWARE-BASED-ENDPOINT-DEFAULT rate 5000
burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-VOICE ip PC_Subnet_Source wildcard_bits any dscp-field 46
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-VIDEO ip PC_Subnet_Source wildcard_bits any dscp-field 34
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT trust-dscp aggregate
SOFTWARE-BASED-ENDPOINT-SIGNAL ip PC_Subnet_Source wildcard_bits any dscp-field 24
CAT6500> (enable) set qos acl ip SOFTWARE-BASED-ENDPOINT  dscp 0 aggregate
SOFTWARE-BASED-ENDPOINT-DEFAULT any
CAT6500> (enable) commit qos acl SOFTWARE-BASED-ENDPOINT
CAT6500> (enable) set vlan dvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust untrusted
CAT6500> (enable) set qos acl map SOFTWARE-BASED-ENDPOINT  mod/port
```

Cisco Unified Wireless IP Phones

デフォルトでは、Cisco Unified Wireless IP Phone および無線で接続された Cisco Unified IP Phones 9971 は、Per-Hop Behavior（PHB）値 CS3、または Differentiated Services Code Point（DSCP）値 24（ToS 値 0x60 に相当）を使用して SCCP シグナリング メッセージをマーキングし、PHB 値 EF、または DSCP 値 46（ToS 値 0xB8 に相当）を使用して RTP 音声パケットをマーキングし

ます。AP でキューイングが正しく設定されており、アップストリームの最初のホップのスイッチが AP のポートを信頼するように設定されている場合、ワイヤレス IP Phone のトラフィックは、有線 IP Phone のトラフィックと同じように処理されます。この方法により、LAN と WLAN 環境で QoS 設定の一貫性を保つことができます。

また、Cisco Unified Wireless IP Phone および Cisco Unified IP Phone 9971 は、無線で接続されたときに Cisco Discovery Protocol（CDP）を使用してその存在を AP に自動的にアナウンスします。CDP パケットはワイヤレス IP Phone から AP に送信され、これらのパケットにより電話機が特定されます。これにより、AP は、その IP Phone へのすべてのトラフィックを高プライオリティ キューに入れることができます。

設定例が示しているとおり、AP から送られるパケットは信頼されている必要があり、各パケットの VLAN タグに基づいて DSCP マーキングを保持またはダウンとマーキングする必要があります。このように、音声 VLAN 上の Cisco Unified Wireless IP Phone が送信元であるパケットは、適切な DSCP マーキングを保持する必要があり、データ VLAN 上のデータ デバイスが送信元であるパケットは、DSCP 値 0 に再マーキングする必要があります。

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE-SIGNALING
CAT3550(config-cmap)#match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE
CAT3550(config-cmap)#match ip dscp 46
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DATA
CAT3550(config-cmap)#match any
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE-SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DVLAN
CAT3550(config-cmap)#match vlan dvlan-id
CAT3550(config-cmap)#match class-map INGRESS-DATA
CAT3550(config-cmap)#
CAT3550(config-pmap-c)#policy-map INGRESS-QOS
CAT3550(config-pmap)#class INGRESS-VVLAN-VOICE
CAT3550(config-pmap-c)#set ip dscp 46
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-pmap-c)#set ip dscp 24
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-DVLAN
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#interface interface id
CAT3550(config-if)#description Wireless Access Point
CAT3550(config-if)#switchport access dvlan-id
CAT3550(config-if)#switchport voice vvlan-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#service-policy input INGRESS-QOS
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS trust-dscp ip any any
CAT6500> (enable) set qos acl ip AP-DATA-INGRESS dscp 0 ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl map AP-VOICE-INGRESS vvlan-id input
CAT6500> (enable) set qos acl map AP-DATA-INGRESS dvlan-id input
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port vlan-based
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port trust trust-dscp
CAT6500> (enable)
```

ビデオ テレフォニー エンドポイント

ここでは、次のタイプのエンドポイント デバイスでトラフィックがどのように分類されるかについて説明します。

- 「Cisco Unified Video Advantage と Cisco Unified IP Phone」（P.18-45）
- 「Cisco IP Video Phone 7985G」（P.18-47）
- 「Sony 社製と Tandberg 社製の SCCP エンドポイント」（P.18-48）
- 「H.323 と SIP のビデオ エンドポイント」（P.18-49）

Cisco Unified Video Advantage と Cisco Unified IP Phone

ユーザの PC 上にある Cisco Unified Video Advantage アプリケーションは、DSCP を使用したビデオ トラフィックの分類をサポートし、レイヤ 3 だけで分類を行えます。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するよう設定する必要があります。PC パケットは 802.1Q タグを持つ可能性が低いため、802.1p CoS ビットはサポートできません。このように PC が 802.1p をサポートしないため、次のオプションで Cisco Unified Video Advantage に QoS を実現できます。

オプション 1

現在の QoS モデルで信頼を IP Phone にまで広げた場合、ネットワークへの着信時に音声パケットとシグナリング パケットは正しくマーキングされます。ポートに UDP ポート 5445 と一致する ACL を追加すると、ビデオ メディア チャネルも PHB AF41 に分類されます。この ACL がないと、ビデオ メディアは Best Effort に分類されて、画像の品質低下やリップシンクの問題が起きます。同じ ACL を使用すると、TCP ポート 4224（CS3 と分類）を使用した、Cisco Unified Video Advantage PC と IP Phone 間の CAST 接続の照合も可能ですが、このことで得られる利点はほとんどありません。データ VLAN 上にある PC からのシグナリング パケットは、同じ高速ポート経由で音声 VLAN に返されます。したがって、パケットで輻輳が発生する可能性は非常に低くなります。

次の例は、このオプションの設定方法を示しています。

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
```

```
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 24
3550(config-ext-nacl)#permit tcp PC_Subnet_Source wildcard_bits eq 4224 any
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip PC_Subnet_Source wildcard_bits any dscp 34
3550(config-ext-nacl)#permit udp PC_Subnet_Source wildcard_bits eq 5445 any
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

オプション 2

『*Enterprise QoS Solution Reference Network Design Guide, Version 3.1*』（http://www.cisco.com/go/designzone で入手可能）には、別の方法が示されています。この方法で推奨されていることは、CoS を信頼する代わりに、着信トラフィックの DSCP を信頼するようにポートを変更し、一連の Per-Port/Per-VLAN アクセス コントロール リストに着信パケットを通過させることです。このアクセス コントロール リストでは、そのとき他の基準とともに TCP/UDP ポートに基づいてパケットが照合され、適切なレベルにポリシングされます。たとえば、DSCP を信頼するようにスイッチ ポートが設定されている状態では、Cisco Unified Video Advantage はビデオ パケットに DSCP AF41 とマーキングします。パケットは ACL で照合されますが、その照合は、パケットが UDP ポート 5445 を使用し、DSCP AF41 とマーキングされ、データ VLAN 上に着信していることに基づいて行われます。この ACL は、その後、DSCP を信頼してトラフィックを N kbps（N はポートごとに許可するビデオ帯域幅）にポリシングするために、クラス マップまたはポリシー マップで使用されます。類似した ACL やポリシング機能が、音声 VLAN 内の IP Phone からの音声パケットやシグナリング パケットに存在します。

次の例は、このオプションの設定方法を示しています。

```
3550(config)#class-map match-all SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#match access-group name SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name SOFTWARE-BASED-ENDPOINT-SIGNALING
```

```
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map SOFTWARE-BASED-ENDPOINT
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input SOFTWARE-BASED-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended SOFTWARE-BASED-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit tcp PC_Subnet_Source wildcard_bits eq 4224 any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit udp PC_Subnet_Source wildcard_bits eq 5445 any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended SOFTWARE-BASED-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip PC_Subnet_Source wildcard_bits any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Cisco IP Video Phone 7985G

他の多くの Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は、電話機からの発信トラフィック用に 802.1p/Q タギングをサポートしています。また、Cisco IP Video Phone 7985G は PC アクセス用に別のイーサネット インターフェイスを備えているため、接続デバイスからの発信トラフィックもサポートしています。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するよう設定する必要があります。信頼を電話機の PC ポートにまで広げないことを推奨しますが、スイッチでサポートされているときは、音声、ビデオ、およびシグナリングのトラフィックの最大量を制限するようにポリシング機能を設定することを推奨します。

次に、このタイプの設定例を示します。

```
3550(config)#class-map match-all C7985-ENDPOINT-VOICE
3550(config-cmap)#match access-group name C7985-ENDPOINT-VOICE
3550(config-cmap)#class-map match-all C7985-ENDPOINT-VIDEO
3550(config-cmap)# match access-group name C7985-ENDPOINT-VIDEO
3550(config-cmap)#class-map match-all C7985-ENDPOINT-SIGNALING
3550(config-cmap)# match access-group name C7985-ENDPOINT-SIGNLAING
3550(config-cmap)#exit
3550(config)#
3550(config)#policy-map C7985-ENDPOINT
3550(config-pmap)#class C7985-ENDPOINT-VOICE
3550(config-pmap)# police 128000 8000 exceed-action drop
3550(config-pmap)#class C7985-ENDPOINT-VIDEO
3550(config-pmap)#set ip dscp 34
3550(config-pmap)# police 50000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class C7985-ENDPOINT-SIGNALING
```

```
3550(config-pmap)#set ip dscp 24
3550(config-pmap)# police 32000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)#class class-default
3550(config-pmap)# set ip dscp 0
3550(config-pmap)# police 5000000 8000 exceed-action policed-dscp-transmit
3550(config-pmap)# exit
3550(config)#exit
3550(config)#
3550(config)#interface FastEthernet interface_id
3550(config-if)# switchport access vlan dvlan_id
3550(config-if)# switchport mode access
3550(config-if)# service-policy input C7985-ENDPOINT
3550(config-if)# exit
3550(config)#ip access-list extended C7985-ENDPOINT-SIGNALING
3550(config-ext-nacl)#permit ip Voice_IP_Subnet Subnet_Mask any dscp 24
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended C7985-ENDPOINT-VIDEO
3550(config-ext-nacl)#permit ip Voice_IP_Subnet Subnet_Mask any dscp 34
3550(config-ext-nacl)#exit
3550(config-if)# ip access-list extended C7985-ENDPOINT-VOICE
3550(config-ext-nacl)# permit ip Voice_IP_Subnet Subnet_Mask any dscp 46
3550(config-ext-nacl)#exit
3550(config)#exit
```

Sony 社製と Tandberg 社製の SCCP エンドポイント

Sony 社製と Tandberg 社製の SCCP エンドポイントは、DSCP を使用してレイヤ 3 でメディア パケットおよびシグナリング パケットを正しくマーキングします。ただし、802.1Q をサポートしていないため、802.1p CoS を使用して分類できません。UDP と TCP のポート照合オプションを使用した場合、SCCP シグナリングを CS3 として、またビデオ メディアを AF41 として正しく分類できますが、UDP ポートが音声だけのコールで使用されている場合は判別ができないため、EF としての分類が必要になります。そのような場合、コール アドミッション制御メカニズムは帯域幅を正しく処理できません。この状況を避けるために、Sony 社製または Tandberg 社製のエンドポイントからのトラフィックを分類して信頼する方法として実行可能なオプションは、次の 1 つだけです。

オプション 1

Sony 社製または Tandberg 社製のエンドポイントで使用されているポート上で DSCP を信頼します。スイッチで許可されている場合は、そのポート上で受信可能な EF、AF41、CS3 トラフィックの最大量を制限するようにポリシング機能を設定します。そのポートに接続された他のデバイスは、DSCP を使用してパケットが分類されていても、信頼できるとは限りません。このオプションは、Sony 社製または Tandberg 社製のシステムがオフィスや小規模な会議室に固定的に設置されている場合に適しています。

Sony 社製または Tandberg 社製のデバイスは CDP をサポートしていないため、このエンドポイントを音声 VLAN に配置する必要がある場合は、VLAN に配置するときに手動の修正が必要です。音声 VLAN にエンドポイントを直接配置することの利点は、システム内の他の IP テレフォニー エンドポイントと同様に扱えることです。欠点は、ポートが音声 VLAN に直接アクセスするため、セキュリティ上のリスクが発生する可能性があることです。一方、Sony 社製または Tandberg 社製のエンドポイントをデータ VLAN に残すこともできますが、Unified CM に対する SCCP シグナリングを許可し、UDP メディア ストリームが音声コール中またはビデオ コール中にデータ VLAN および音声 VLAN 間を通過できるようにするには、データ VLAN と音声 VLAN 間のアクセスでのプロビジョニングが必要です。

次の例は、このオプションの設定方法を示しています。

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
```

```
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#class-map match-all VVLAN-VIDEO
CAT2970(config-cmap)# match access-group name VVLAN-VIDEO
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)# policy-map SCCP-VIDEO-ENDPOINT
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap)#class VVLAN-VIDEO
CAT2970(config-pmap-c)# set ip dscp 34
CAT2970(config-pmap-c)# police 1500000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input SCCP-VIDEO-ENDPOINT
CAT2970(config-if)# exit
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(confiig)#ip access list extended VVLAN-VIDEO
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
dscp af41
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002 dscp
cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
```

H.323 と SIP のビデオ エンドポイント

このタイプのエンドポイントは、H.323 および SIP ビデオ エンドポイントにはさまざまなものがあり、実装と機能も多様なため、QoS の点で大きな課題があります。これらのエンドポイントには主に 2 つの QoS オプションがあります。1 つは、H.323 または SIP のビデオ エンドポイントに依存してすべてのトラフィックのマーキングを正しく行う方法で、もう 1 つは、使用する TCP ポートおよび UDP ポートの詳細な認識に依存する方法です。

オプション 1

エンドポイントがメディア トラフィックおよびシグナリング トラフィックのマーキングを正しく行った場合は（シグナリングには SIP、H.225、H.245、および RAS が含まれる）、その分類を信頼できます。エンドポイントで 802.1Q（結果的に 802.1p CoS）がサポートされる可能性は低いため、この場合は IP Precedence または DSCP を使用します。分類タイプの選択は、そのベンダー、モデル、およびソフトウェア バージョンに左右されます。

（注）　H.323 または SIP のエンドポイントがそのパケットのマーキングを正しく行う可能性は非常に低くなります。

（注）　Unified CM 8.5 および最新のデバイス ファームウェアよりも前のリリースでは、Cisco E20 はトラフィックにマーキングせず、Cisco Discovery Protocol（CDP）をサポートしていません。さらに、Tandberg ビデオ エンドポイントも、トラフィックにマーキングせず、CDP をサポートしていません。そのため、マッチングのための ACL と、「オプション 2」（P.18-50）のようにトラフィックの適切な分類を使用する必要があります。同様に、CDP がサポートされない場合、このエンドポイントの VLAN の配置で、音声 VLAN にデバイスを配置するには、手動の変更が必要です。前述のように、音声 VLAN にエンドポイントを直接配置することの利点は、システム内の他の IP テレフォニー エンドポイントと同様に扱えることです。ただし、音声 VLAN に直接アクセスする機能があるため、結果としてセキュリティ リスクが発生する可能性があります。また、エンドポイントはデータ VLAN に残る可能性もありますが、データおよび音声 VLAN 間のアクセスを許可して、Unified CM に対する SIP シグナリングを可能にし、音声またはビデオ コール時のデータおよび音声 VLAN 間で UDP メディア ストリームを渡すことができるようにする必要があります。

オプション 2

送信元、宛先、または TCP と UDP の両方のポート番号（多くは、IP アドレスも含む）を組み合せて使用することによって、トラフィックを正しく照合および分類する ACL を定義できます。さらに、ポリシング機能も適用し、ネットワークで許可されるトラフィック クラスごとにその量を制限することも推奨します。このオプションには、オプション 1 と同様に、音声だけのコールを誤って分類する可能性があります。

次の例は、このオプションの設定方法を示しています。

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VIDEO
CAT2970(config-cmap)# match access-group name VVLAN-VIDEO
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map SCCP-VIDEO-ENDPOINT
CAT2970(config-pmap)#class VVLAN-VIDEO
CAT2970(config-pmap-c)# set ip dscp 34
CAT2970(config-pmap-c)# police 1500000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
```

```
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input SCCP-VIDEO-ENDPOINT
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VIDEO
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384 32767
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 1719 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any eq 1720 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 11000 65535
dscp cs3
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061 dscp
cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
```

（注）　上記の設定方法は、音声専用コールの場合でも、音声トラフィックをビデオ トラフィックと同様にマーキングします。シグナリングおよび RTP ポートの使用方法はベンダーごとに異なるため、上記の例での使用方法と異なる場合は、適切なポート範囲を使用する必要があります。

Unified Communications エンドポイントのハイ アベイラビリティ

Unified CM サブスクライバまたは他のサーバの障害発生時にもサービスが停止しないように、Cisco Unified Communications エンドポイントは、複数のサーバを使用して設定できます。たとえば、直接設定によって、またはブートアップ フェーズ中に DHCP によって、エンドポイントは複数の TFTP サーバ アドレスを受け入れて処理できます。エンドポイントのブートアップ中にプライマリ TFTP サーバが停止した場合、エンドポイントはセカンダリ TFTP サーバから設定ファイルを取得できます。

各エンドポイントは、デバイス プールとも関連付けられています。デバイス プールには、1 つ以上の Unified CM サブスクライバを持つ Unified CM Group が含まれます。これらのサブスクライバのリストが、各エンドポイントの設定ファイル内に送信されます。エンドポイントは、リスト内の最初の（プライマリ）サブスクライバへの登録を試行します。その Unified CM サブスクライバが使用できない場合、エンドポイントは、リスト内の 2 番めのサブスクライバ（セカンダリ）への登録を試行します。3 番め以降も同様に続きます。サブスクライバへの登録後は、現在のサブスクライバに障害が発生すると、エンドポイントは、Unified CM Group 内の優先順位リスト内の別のサブスクライバにフェールオーバーできます。優先順位の高いサブスクライバが復旧されると、エンドポイントはそのサブスクライバに再登録します。

Unified CM クラスタから WAN を介して配置されているエンドポイントのネットワーク障害に備えるために、エンドポイントの登録に使用するサーバ リスト内に、Survivable Remote Site Telephony（SRST）が搭載されたローカルで使用可能な Cisco Integrated Services Router（ISR; サービス統合型

ルータ）を構成することもできます。WAN の障害発生時には、エンドポイントは SRST ルータに登録し、継続してテレフォニー サービスを提供します（SRST モードでは、サポートされる機能セットがこれより小さい場合もあります）。

1 台のサーバのオーバーロードを回避するために、クラスタ内のサーバ間で均等にエンドポイントを分散する必要があります。クラスタ サブスクライバ間の冗長構成方法の詳細については、「コール処理」（P.8-1）の章を参照してください。

Unified Communications エンドポイントのキャパシティ プランニング

Unified CM クラスタは、次の機能をサポートしています。

- Cisco MCS-7845 サーバ、Cisco UCS B200 M1 ブレード サーバ、または Cisco UCS C210 M1 ラックマウント サーバで、最大 30,000 のエンドポイント
- クラスタあたり最大 10,000 個のエンドポイント（Cisco MCS-7835 サーバ使用時）
- クラスタあたり最大 4,000 個のエンドポイント（Cisco MCS-7825 サーバ使用時）
- クラスタあたり最大 2,000 個のエンドポイント（Cisco MCS-7815 または MCS-7816 サーバ使用時）

上記の数字は、通常の最大キャパシティです。クラスタでサポートされる最大エンドポイント数は、サーバが実行しているその他すべての機能や、ユーザの Busy Hour Call Attempts（BHCA; 最繁時呼数）などによって決まります。このため、実際のキャパシティは公称の最大キャパシティよりも小さくなることがあります。適切なシステム サイジングを確実に行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用してください。シスコの従業員およびパートナーは（要求された適切なログイン アカウントを使用して）、サイジング ツールを入手できます。

http://tools.cisco.com/cucst

Unified Communications エンドポイントの設計上の考慮事項

次のリストは、Cisco Unified Communications エンドポイント セットから適切なエンドポイントを選択する際のハイレベルな推奨事項を要約したものです。

- 低密度アナログ接続には、Cisco Analog Telephone Adapter（ATA）または低密度アナログ インターフェイス モジュールを使用する。
- 中密度から高密度のアナログ接続には、高密度アナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco Communication Media Module（CMM; コミュニケーション メディア モジュール）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG224、または Cisco VG248 を使用する。
- XML やその他の電話ベースのサービスをほとんど、あるいはまったく使用しない音声中心のユーザには、Cisco Unified IP Phones 6921、6941、および 6961 を使用する。
- トラフィックの発生量が少量で、コール機能に制限を受けるテレフォニー ユーザには、Cisco Unified SIP Phone 3911 または Cisco Unified IP Phone 7902G、7905G、7906G、7910G、7910G+SW、7911G、7912G、7912G-A を使用する。
- トラフィックの発生量が中程度で、トランザクション タイプのテレフォニー ユーザには、Cisco Unified IP Phone 7931G、7940G、7941G、7941G-GE、7942G、または 7945G を使用する。

- テレフォニー トラフィックの発生量が中程度から大量の、マネージャおよびアシスタントには、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7962G、7965G、または 8961 を使用する。
- テレフォニー トラフィックの発生量が多い、拡張コール機能を使用する経営幹部には、Cisco Unified IP Phone 7970G、7971G-GE、7975G、9951、または 9971 を使用する。
- 外勤職員および在宅勤務者には、Cisco IP Communicator を使用する。
- モバイル IP Phone が必要なユーザには、Cisco Unified Wireless IP Phone 7921G、7925G、7925G-EX、または 7926G を使用する。
- ビデオ コールにマーキングする場合、Cisco Unified IP Phone または Cisco IP Communicator に関連付けられた Cisco Unified Video Advantage、Cisco Unified Personal Communicator、および Cisco Unified Client Services Framework（CSF）といったソフトウェアベースのクライアントを使用する。または、Cisco IP Video Phone 7985G、Cisco Unified IP Phone 9951 または 9971（オプションで USB カメラ付属）、Tandberg ビデオ エンドポイント（Cisco E20 Video Phone など）、Sony などのサードパーティ エンドポイント デバイスといった、ハードウェア ビデオ統合デバイスを使用する。
- 音声、ビデオ、ドキュメント共有、および単一の統合インターフェイスからの現在の情報にアクセスするには、Cisco Unified Personal Communicator を使用する。
- フォーマルな会議環境には、Cisco Unified IP Conference Station 7936 または 7937G を使用する。

エンドポイント機能の要約

次の各表は、この章で説明した各種のエンドポイント デバイスでサポートされる機能を要約したものです。

- 表 18-7 は、Cisco アナログ ゲートウェイの Cisco Unified Communications 機能を要約したものです。
- 表 18-8 は、Skinny Client Control Protocol（SCCP）を使用する Cisco ベーシック IP Phone の機能を要約したものです。
- 表 18-9 は、Session Initiation Protocol（SIP）を使用する Cisco ベーシック IP Phone の機能を要約したものです。
- 表 18-10 は、SCCP を使用する Cisco ビジネス IP Phone の機能を要約したものです。
- 表 18-11 は、SIP を使用する Cisco ビジネス IP Phone の機能を要約したものです。
- 表 18-12 は、SCCP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 18-13 は、SIP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 18-14 は、Cisco Unified IP Phones 7921G、7925G、7925G-EX、7926G、7936、7937G、7985G、および Cisco E20 Video Phone などの専用エンドポイントの機能を要約したものです。
- 表 18-15 は、Cisco Unified Personal Communicator および Cisco IP Communicator を含むソフトウェア ベースのデバイスの機能を要約したものです。
- 表 18-16 は、Cisco Unified IP Phones 7985G、9951、9971、および Cisco E20 Video Phone のビデオの機能を要約したものです。

表 18-7　Cisco アナログ ゲートウェイの機能

機能	アナログ インターフェイス カード	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG202	VG204	VG224	VG248	ATA 186 および 188
イーサネット接続	×	×	×	○[1]	○[1]	○[1]	○[2]	○[3]
アナログ ポートの最大数	24[4]	72	24	2	4	24	48	2
発信者 ID	○	×	×	○	○	○	○	○
コール ウェイティング	×	×	×	○	○	○	○	○
コール ウェイティング時の発信者 ID	×	×	×	○	○	○	○	○
保留	×	×	×	○	○	○[5]	○	○
コール転送	×	×	×	○	○	○[5]	○	○
自動転送	×	×	×	○	○	○	○[6]	○
自動応答	×	×	×	×	×	×	×	×
Ad Hoc 会議	×	×	×	○	○	○	○	○
Meet-Me 会議	×	×	×	○	○	×	×	○
コール ピックアップ	×	×	×	○	○	○	×	○
グループ ピックアップ	×	×	×	○	○	○	×	○
リダイヤル	×	×	×	○	○	○	○[7]	○[7]
スピード ダイヤル	×	×	×	○	○	○	○	○
オンフック ダイヤル	×	×	×	×	×	×	×	×
ボイスメールへのアクセス	○	○	○	○	○	○	○	○[8]
メッセージ待機インジケータ（MWI）	×	×	×	○	○	×	○	○[8]
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	×	×	×	○	○	○	○	○[8]
Survivable Remote Site Telephony（SRST）サポート	×	×	×	○	○	○	○	○
保留音（MoH）	○	○	○	○	○	×	○	○
消音	×	×	×	×	×	×	×	×
Multilevel Precedence and Preemption（MLPP）	×	×	×	○	○	×	×	×
割り込み	×	×	×	×	×	×	×	×
C 割り込み	×	×	×	×	×	×	×	×
ワンボタン割り込み	×	×	×	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×	×	×	×
コール保持	×	×	×	×	×	×	○[9]	×

表 18-7　Cisco アナログ ゲートウェイの機能（続き）

機能	アナログ インターフェイス カード	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG202	VG204	VG224	VG248	ATA 186 および 188
コール アドミッション制御	○	×	×	×	×	×	×	×
ローカル ボイス ビジーアウト	○	×	×	×	×	×	×	×
PLAR（Private Line Automatic Ringdown）	○	×	×	×	×	×	×	○
ハント グループ	○	×	×	×	×	×	×	×
ダイヤル プランのマッピング	○	×	×	×	×	×	×	×
監視切断	○	×	×	×	×	×	×	×
シグナリング パケット ToS 値のマーキング	0x68	0x68[10]	0x68	0x68	0x68	0x68	0x68	0x68
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
FAX パススルー	○[11]	○	○[12]	○	○	○	○[11]	○
FAX リレー	○	○	×	○	○	○	○	×
Skinny Client Control Protocol（SCCP）	×	×	×	○	○	○	○	○
セッション開始プロトコル（SIP）	×	×	×	○	○	○	×	○
H.323	○	○	×	○	○	○	×	○
メディア ゲートウェイ コントロール プロトコル（MGCP）	○	○	○	○	○	○	×	○[13]
G.711	○	○	○	○	○	○	○	○
G.722	×	×	×	×	×	×	×	×
G.723	○	○	×	×	×	×	×	○
G.726	○	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○	○
音声アクティビティ検出（VAD）	○	○	×	○	○	○	×	○
コンフォート ノイズ生成（CNG）	○	○	×	○	○	○	×	○

1. 2 つの 10/100 Base-T。
2. 1 つの 10/100 Base-T。
3. ATA 188 では 2 つの 10/100 Base-T、ATA 186 では 1 つの 10 Base-T。
4. EVM-HD-8FXS/DID は、基本ボード上に 8 つのポートがあり、FXS または DID シグナリング用に構成可能です。また、EM-HDA-8FXS には 2 つの拡張モジュールを取り付けることができます。
5. H.323 および SIP での呼制御。
6. Call Forward All。
7. リダイヤル。
8. SCCP および SIP バージョンだけ。
9. VG248 バージョン 1.2 以降でサポート。
10. UDP ポート 2427 では MGCP シグナリングをマーキングしますが、TCP ポート 2428 ではベストエフォート型の MGCP キープアライブ パケットをマーキングします。
11. FAX パススルーおよび FAX リレー。
12. FAX パススルー。
13. Unified CM は、ATA を使用する MGCP をサポートしていません。

表 18-8　SCCP を使用する Cisco Basic IP Phone

機能	6901	6911	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
イーサネット接続	○	○	○[1]	○[1]	○[2]	○[1]	○[3]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	×	○	×	×	○	×	○	○	○[4]
Cisco Power-Over-Ethernet（PoE）	×	×	○	○	○	○	○	○	○
IEEE 802.3af Power-Over-Ethernet（PoE）	○	○	×	×	○	×	×	○	×
ローカリゼーション	○	○	×	○	○	×	×	○	○
ディレクトリ番号	1	1	1	1	1	1	1	1	1
回線あたりの最大コール数	2	2	200	200	200	200	200	200	200
液晶ディスプレイ	×	×	×	○	○	○	○	○	○
発信者 ID	×	×	×	○	○	○	○	○	○
コール ウェイティング	○	○	×	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	×	×	×	○	○	○	○	○	○
保留	○	○	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○	○	○
自動応答	×	○	×	○[5]	○[5]	×	×	○[5]	○[5]
Ad Hoc 会議	○	○	○	○	○	○	○	○	○
Meet-Me 会議	×	○	×	○	○	○	○	○	○
コール ピックアップ	×	○	×	○	○	○	○	○	○
グループ ピックアップ	×	○	×	○	○	○	○	○	○
リダイヤル	○	○	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]
スピード ダイヤル	×	○	○	○	○	○	○	○	○
オンフック ダイヤル	×	○	×	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	○	×	×	○	×	×	○	×
ビデオ コール	×	×	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○	○	○

表 18-8　SCCP を使用する Cisco Basic IP Phone（続き）

機能	6901	6911	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
保留トーン	○	○	○	○	○	○	○	○	○
スピーカー	×	○	×	○[5]	○[5]	○[5]	○[5]	○[5]	○[5]
ヘッドセット ジャック	×	×	×	×	×	×	×	×	×
消音	×	○	×	×	×	○	○	×	×
Multilevel Precedence and Preemption（MLPP）	×	×	○	○	○	○	○	○	○
割り込み	×	×	×	×	○	×	×	○	○
C 割り込み	○	○	×	○	○	×	×	○	○
ワンボタン割り込み	×	×	×	×	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×	×	×	×	×
プログラム可能な回線キー	×	○[7]	×	×	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	○	○	×	×	×	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	○	○	×	×	○	×	×	○	×
シグナリングの完全性	○	○	×	×	○	×	×	○	×
製造元でインストールされる証明書（X.509v3）	○	○	×	×	○	×	×	○	×
現場でインストールされる証明書	○	○	×	×	○	×	×	○	×
サードパーティの XML サービス	○	○	×	○	○	×	×	○	○
外部マイクおよびスピーカー	×	○	×	×	×	×	×	×	×
ダイヤル プラン	×	×	×	×	×	×	×	×	×
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート[8]	○	○	×	×	○	×	×	○	×
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○	○	○
G.722	×	×	×	×	○	×	×	○	×
G.723	×	×	×	×	×	×	×	×	×
G.726	×	×	×	○	×	×	×	×	×
G.729	○	○	○	○	○	○	○	○	○
iLBC	×	×	×	×	○	×	×	○	×

表 18-8　SCCP を使用する Cisco Basic IP Phone（続き）

機能	6901	6911	7902G	7905G	7906G	7910G	7910 +SW	7911G	7912G/G-A
ワイドバンド オーディオ	×	×	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○	○	○
DTMF：RFC2833	○	○	×	×	○	×	×	○	×
DTMF：KPML	×	×	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×	×	×

1. 1 つの 10 Base-T。
2. 1 つの 10/100 Base-T。
3. 2 つの 10/100 Base-T。
4. Cisco Unified IP Phone 7912G-A は、イーサネット スイッチの拡張バージョンを備えています。
5. 一方向のオーディオ モニタ モード。
6. リダイヤル。
7. Cisco Unified IP Phone 6911 は、1 つのプログラマブル機能キーをサポートします。
8. SCCP バージョン 20 以降が必要です。

表 18-9　SIP を使用する Cisco Basic IP Phone

機能	3911	6901	6911	7905G	7906G	7911G	7912G/G-A
イーサネット接続	○[1]	○	○	○[2]	○[1]	○[3]	○[1]
イーサネット スイッチ（PC ポート）	×	×	○	×	○	○	○[4]
Cisco Power-Over-Ethernet（PoE）	×	×	×	○	○	○	○
IEEE 802.3af Power-Over-Ethernet（PoE）	○	○	○	×	○	○	×
ローカリゼーション	○	○	○	×	○	○	×
ディレクトリ番号	1	1	1	1	1	1	1
回線あたりの最大コール数	2	2	2	2	50	50	2
液晶ディスプレイ	○	×	×	○	○	○	○
発信者 ID	○	×	×	○	○	○	○
コール ウェイティング	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	×	×	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	○	○	○	○
初期在席転送	○	○	○	×	○	○	×
打診転送	○	○	○	○	○	○	○
自動転送	○[5]	○	○	○[5]	○	○	○[5]
自動応答	×	×	○	×	○[6]	○[6]	×

表 18-9　SIP を使用する Cisco Basic IP Phone（続き）

機能	3911	6901	6911	7905G	7906G	7911G	7912G/G-A
Ad Hoc 会議	○	○	○	○	○	○	○
Meet-Me 会議	×	×	○	×	○	○	×
コール ピックアップ	×	×	○	×	○	○	×
グループ ピックアップ	×	×	○	×	○	○	×
リダイヤル	○[7]	○	○	○[7]	○	○	○[7]
スピード ダイヤル	○[8]	×	○	○[8]	○	○	○[8]
オンフック ダイヤル	○	×	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	○	○	×	○	○	×
ビデオ コール	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	×	○	○	×	○	○	×
保留トーン	×	○	○	×	×	×	×
スピーカー	○[6]	×	○	○[6]	○[6]	○[6]	○[6]
ヘッドセット ジャック	×	×	×	×	×	×	×
消音	○	×	○	×	×	×	×
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×	×	×
割り込み	×	×	×	×	○	○	×
C 割り込み	×	○	○	×	○	○	×
ワンボタン割り込み	×	×	×	×	×	×	×
回線をまたいで参加	×	×	×	×	×	×	×
プログラム可能な回線キー	×	×	○[9]	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	○	○	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	×	○	○	×	○	○	×
シグナリングの完全性	×	○	○	×	○	○	×
製造元でインストールされる証明書（X.509v3）	×	○	○	×	○	○	×
現場でインストールされる証明書	×	○	○	×	○	○	×
サードパーティの XML サービス	×	○	○	×	○	○	×

表 18-9　SIP を使用する Cisco Basic IP Phone（続き）

機能	3911	6901	6911	7905G	7906G	7911G	7912G/G-A
外部マイクおよびスピーカー	×	×	○	×	×	×	×
ダイヤル プラン	○	○	○	○	○	○	○
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート	○	○	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○
G.722	×	×	×	×	○	○	×
G.723	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×
G.729	○[10]	○	○	○[10]	○[10]	○[10]	○[10]
iLBC	×	×	×	×	○	○	×
ワイドバンド オーディオ	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	×	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	×	×	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○	○	○
DTMF：KPML	×	×	×	×	○	○	×
DTMF：無指定の NOTIFY	×	×	×	×	○	○	×

1. 1 つの 10/100 Base-T。
2. 1 つの 10 Base-T。
3. 2 つの 10/100 Base-T。
4. Cisco Unified IP Phone 7912G-A は、イーサネット スイッチの拡張バージョンを備えています。
5. Cisco Unified IP Phone 7905G、7912G で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の [User] ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の [User] ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. Cisco Unified SIP Phone 3911 は半二重のスピーカー フォンを備えているのに対し、Cisco Unified IP Phone 7905G、7906G、7911G、および 7912G/GA は片通話モードをサポートしています。
7. リダイヤル。
8. スピード ダイヤルは、これらのモデルの電話機だけに設定可能です。
9. Cisco Unified IP Phone 6911 は、1 つのプログラマブル機能キーをサポートします。
10. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 18-10　SCCP を使用する Cisco ビジネス IP Phone

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
イーサネット接続	○[1]	○[1]	○[1]	○[1]	○[2]	○[2]	○[2]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	×	×	○	○[3]	○	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	○	○	×	○[3]	○	○
ローカリゼーション	○	○	○	○	○	○	○
ディレクトリ番号	2	12	24	2	2	2	2
回線あたりの最大コール数	1	1	1	200	200	200	200
液晶ディスプレイ	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○
コール ウェイティング	○[4]	○[4]	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○
自動応答	○	○	○	○	○	○	○
Ad Hoc 会議	○	○	○	○	○	○	○
Meet-Me 会議	○	○	○	○	○	○	○
コール ピックアップ	○	○	○	○	○	○	○
グループ ピックアップ	○	○	○	○	○	○	○
リダイヤル	○	○	○[5]	○[5]	○[5]	○[5]	○[5]
スピード ダイヤル	○	○	○	○	○	○	○
オンフック ダイヤル	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	○	○	×	○	○	○
ビデオ コール	×	×	×	○	○	○	○
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○
保留トーン	○	○	○	○	○	○	○
スピーカー	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○

表 18-10　SCCP を使用する Cisco ビジネス IP Phone（続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
Multilevel Precedence and Preemption（MLPP）	×	×	○	○	○	○	○
割り込み	×	×	○	○	○	○	○
C 割り込み	○	○	○	○	○	○	○
ワンボタン割り込み	×	×	○	×	○	○	○
回線をまたいで参加	○	○	○	○	○	○	○
プログラム可能な回線キー	○	○	○	×	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	○	○	×	×	×	×
ビジー ランプ フィールド	○[6]	○[6]	○	○	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	○	○	○	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	○	○	○	○	○	○	○
シグナリングの完全性	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	○	○	○	×	○	○	○
現場でインストールされる証明書	○	○	○	○	○	○	○
サードパーティの XML サービス	○	○	○	○	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○	○	○
ダイヤル プラン	×	×	×	×	×	×	×
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート[7]	○	○	○	×	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○
G.722	×	×	○	×	○	○	○
G.723	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○
iLBC	×	×	○	×	×	○	○
ワイドバンド オーディオ	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○
DTMF：RFC2833	○	○	○	○	○	○	○

表 18-10　SCCP を使用する Cisco ビジネス IP Phone（続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
DTMF：KPML	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7941G および 7942G は、2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7941G-GE および 7945G は、2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. Cisco Unified IP Phone 7941G は Cisco Prestandard Power over Ethernet（PoE）および IEEE 802.3af PoE をサポートしており、Cisco Unified IP Phone 7941G-GE は IEEE 802.3af PoE だけをサポートしています。
4. Cisco Unified IP Phones 6921 および 6961 にコール ウェイティングを実装するには、両方の回線（異なるパーティション内）に同じ DN を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
5. リダイヤル。
6. スピード ダイヤルに限る。コール履歴エントリは対象外。
7. SCCP バージョン 20 以降が必要です。

表 18-11　SIP を使用する Cisco ビジネス IP Phone

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
イーサネット接続	○[1]	○[1]	○[1]	○[1]	○[2]	○[2]	○[2]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	×	×	○	○[3]	○	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	○	○	×	○[3]	○	○
ローカリゼーション	○	○	○	×	○	○	○
ディレクトリ番号	2	12	24	2	2	2	2
回線あたりの最大コール数	1	1	1	2	50	50	50
液晶ディスプレイ	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○
コール ウェイティング	○[4]	○[4]	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	○	○	○	○
初期在席転送	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○
自動転送	○	○	○	○[5]	○	○	○
自動応答	○	○	○	○[6]	○[7]	○	○
Ad Hoc 会議	○	○	○	○[8]	○	○	○
Meet-Me 会議	○	○	○	×	○	○	○
コール ピックアップ	○	○	○	×	○	○	○
グループ ピックアップ	○	○	○	×	○	○	○
リダイヤル	○	○	○[9]	○[9]	○[9]	○[9]	○[9]
スピード ダイヤル	○	○	○[10]	○[10]	○	○	○
オンフック ダイヤル	○	○	○	×	○	○	○

表 18-11　SIP を使用する Cisco ビジネス IP Phone（続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
ボイスメールへのアクセス	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	○	○	×	○	○	○
ビデオ コール	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○
保留トーン	○	○	○	×	×	×	×
スピーカー	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×	×	×
割り込み	×	×	○	×	○	○	○
C 割り込み	○	○	○	×	○	○	○
ワンボタン割り込み	×	×	○	×	○	○	○
回線をまたいで参加	○	○	○	×	○	○	○
プログラム可能な回線キー	○	○	○	×	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	○	○	×	×	×	×
ビジー ランプ フィールド	○[11]	○[11]	○	×	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	○	○	×	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	○	○	○	×	○	○	○
シグナリングの完全性	○	○	○	×	○	○	○
製造元でインストールされる証明書（X.509v3）	○	○	○	×	○	○	○
現場でインストールされる証明書	○	○	○	×	○	○	○
サードパーティの XML サービス	○	○	○	○[12]	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○	○	○
ダイヤル プラン	○	○	○	○	○	○	○
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート	○	○	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60

表 18-11　SIP を使用する Cisco ビジネス IP Phone（続き）

機能	6921	6961	7931G	7940G	7941G/G-GE	7942G	7945G
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○
G.722	×	×	○	×	○	○	○
G.723	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×
G.729	○	○	○[13]	○[13]	○[13]	○[13]	○[13]
iLBC	×	×	○	×	×	○	○
ワイドバンド オーディオ	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	×	×	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○	○	○
DTMF：KPML	×	×	○	×	○	○	○
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7941G および 7942G は、2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7941G-GE および 7945G は、2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. Cisco Unified IP Phone 7941G は Cisco Prestandard Power over Ethernet（PoE）および IEEE 802.3af PoE をサポートしており、Cisco Unified IP Phone 7941G-GE は IEEE 802.3af PoE だけをサポートしています。
4. Cisco Unified IP Phones 6921 および 6961 にコール ウェイティングを実装するには、両方の回線（異なるパーティション内）に同じ DN を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
5. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の [User] ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の [User] ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. この機能は、電話機でローカルに設定できます。
7. 一方向のオーディオ モニタ モード。
8. IP を使用する Unified IP Phone 7940 でサポートされているのは、Ad Hoc 会議用のローカル ミキシングと最大 3 者による会議だけです。
9. リダイヤル。
10. スピード ダイヤルは、電話機だけで設定可能です。
11. スピード ダイヤルに限る。コール履歴エントリは対象外。
12. 限定的なサポート。
13. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 18-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
イーサネット接続	○[1]	○[1]	○[2]	○[2]	○[2]	○[1]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	○	○[4]	○	×	○	×	×

表 18-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）（続き）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
IEEE 802.3af Power-Over-Ethernet（PoE）	○	×	○[4]	○	○	○	○	○
ローカリゼーション	○	○	○	○	○	○	○	○
ディレクトリ番号	4	6	6	2	6	8	8	8
回線あたりの最大コール数	1	200	200	200	200	200	200	200
液晶ディスプレイ	○	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○	○
コール ウェイティング	○[5]	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○	○
自動応答	○	○	○	○	○	○	○	○
Ad Hoc 会議	○	○	○	○	○	○	○	○
Meet-Me 会議	○	○	○	○	○	○	○	○
コール ピックアップ	○	○	○	○	○	○	○	○
グループ ピックアップ	○	○	○	○	○	○	○	○
リダイヤル	○	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]	○[6]
スピード ダイヤル	○	○	○	○	○	○	○	○
オンフック ダイヤル	○	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	×	○	○	○	○	○	○
ビデオ コール	×	○	○	○	○	○	○	○
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○	○
保留トーン	○	○	○	○	○	○	○	○
スピーカー	○	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	○	○	○	○	○	○	○
割り込み	×	○	○	○	○	○	○	○
C 割り込み	○	○	○	○	○	○	○	○

表 18-12　Cisco マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）（続き）

機能	6941	7960G	7961G/G-GE	7962G	7965G	7970G	7971G-GE	7975G
ワンボタン割り込み	×	×	○	○	○	○	○	○
回線をまたいで参加	○	○	○	○	○	○	○	○
プログラム可能な回線キー	○	×	○	○	○	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	×	×	×	×	×	×	×
ビジー ランプ フィールド	○[7]	○	○	○	○	○	○	○
+ ダイヤリングを使用する発番号の標準化	○	×	○	○	○	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	○	○	○	○	○	○	○	○
シグナリングの完全性	○	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	○	×	○	○	○	○	○	○
現場でインストールされる証明書	○	○	○	○	○	○	○	○
サードパーティの XML サービス	○	○	○	○	○	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○	○	○	○
ダイヤル プラン	×	×	×	×	×	×	×	×
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート[8]	○	×	○	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○	○
G.722	×	×	○	○	○	○	○	○
G.723	×	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○	○
iLBC	×	×	×	○	○	×	×	○
ワイドバンド オーディオ	×	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×	×
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	○	○
DTMF：RFC2833	○	○	○	○	○	○	○	○
DTMF：KPML	×	×	×	×	×	×	×	×
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。

2. Cisco Unified IP Phones 7961G および 7962G は 2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7961G-GE および 7965G は 2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. 2 つの 10/100/100 Mbps イーサネット接続。
4. Cisco Unified IP Phone 7961G は Cisco Prestandard PoE と IEEE 802.3af PoE の両方をサポートしており、Cisco Unified IP Phone 7961G-GE は IEEE 802.3af POE だけをサポートしています。
5. Cisco Unified IP Phone 6941 にコール ウェイティングを実装するには、その 2 つの回線に同じ DN（異なるパーティション）を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
6. リダイヤル。
7. スピード ダイヤルに限る。コール履歴エントリは対象外。
8. SCCP バージョン 20 以降が必要です。

表 18-13　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）

機能	6941	7960G	7961G /G-GE	7962G	7965G	7970G	7971 G-GE	7975G	8961	9951	9971
イーサネット接続	○[1]	○[1]	○[2]	○[2]	○[2]	○[1]	○[3]	○[3]	○[3]	○[3]	○[3]
イーサネット スイッチ（PC ポート）	○	○	○	○	○	○	○	○	○	○	○
Cisco Power-Over-Ethernet（PoE）	×	○	○[4]	○	×	○	×	×	×	×	×
IEEE 802.3af Power-Over-Ethernet（PoE）	○	×	○[4]	○	○	○	○	○	○	○	○
IEEE 802.3at Power-Over-Ethernet（PoE）	○	×	×	×	×	×	×	×	×	○	○
USB ポート	×	×	×	×	×	×	×	×	○	○	○
Bluetooth ヘッドセット	×	×	×	×	×	×	×	×	×	○	○
IEEE 802.11a/b/g	×	×	×	×	×	×	×	×	×	×	○
ローカリゼーション	○	×	○	○	○	○	○	○	○	○	○
ディレクトリ番号	4	6	6	6	6	8	8	8	5	5	6
回線あたりの最大コール数	1	2	50	50	50	50	50	50	200	200	200
液晶ディスプレイ	○	○	○	○	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○	○	○	○	○
コール ウェイティング	○[5]	○	○	○	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○	○	○	○	○
ブラインド転送	×	○	×	×	×	×	×	×	×	×	×
初期在席転送	○	○	○	○	○	○	○	○	○	○	○
打診転送	○	○	○	○	○	○	○	○	○	○	○
自動転送	○	○[6]	○	○	○	○	○	○	○	○	○
自動応答	○	○[7]	○	○	○	○	○	○	○	○	○
Ad Hoc 会議	○	○[8]	○	○	○	○	○	○	○	○	○
Meet-Me 会議	○	×	○	○	○	○	○	○	○	○	○
コール ピックアップ	○	×	○	○	○	○	○	○	○	○	○

表 18-13　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	6941	7960G	7961G /G-GE	7962G	7965G	7970G	7971 G-GE	7975G	8961	9951	9971
グループ ピックアップ	○	×	○	○	○	○	○	○	○	○	○
リダイヤル	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]	○[9]
スピード ダイヤル	○	○	○	○	○	○	○	○	○	○	○
オンフック ダイヤル	○	×	○	○	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	○	○	○	○	○	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	○	○	○	○	○	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	○	×	○	○	○	○	○	○	○	○	○
ビデオ コール	×	×	×	×	×	×	×	×	×	×	×
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○	○	○	○	○	○
ユニキャスト MoH	○	○	○	○	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	○	○	○	○	○	○
保留トーン	○	×	×	×	×	×	×	×	×	×	×
スピーカー	○	○	○	○	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	○	○	○	○	○	○	○	○
消音	○	○	○	○	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	×	×	×	×	×	×	×	×	×	×
割り込み	×	×	○	○	○	○	○	○	×	×	×
C 割り込み	○	×	○	○	○	○	○	○	○	○	○
ワンボタン割り込み	×	×	○	○	○	○	○	○	○	○	○
回線をまたいで参加	○	×	○	○	○	○	○	○	○	○	○
プログラム可能な回線キー	○	×	○	○	○	○	○	○	○	○	○
「Single Call per Line」ユーザ エクスペリエンス	○	×	×	×	×	×	×	×	×	×	×
ビジー ランプ フィールド	○[10]	×	○	○	○	○	○	○	○[10]	○[10]	○[10]
+ ダイヤリングを使用する発番号の標準化	○	×	○	○	○	○	○	○	○	○	○
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	○	○	○	○	○	○	○	○
シグナリングおよびメディア暗号化	○	×	○	○	○	○	○	○	○	○	○
シグナリングの完全性	○	×	○	○	○	○	○	○	○	○	○
製造元でインストールされる証明書（X.509v3）	○	×	○	○	○	○	○	○	○	○	○

表 18-13　Cisco マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	6941	7960G	7961G /G-GE	7962G	7965G	7970G	7971 G-GE	7975G	8961	9951	9971
現場でインストールされる証明書	○	×	○	○	○	○	○	○	○	○	○
サードパーティの XML サービス	○	○[11]	○	○	○	○	○	○	○	○	○
Java MIDlet アプリケーション	○	×	○	○	○	○	○	○	○	○	○
外部マイクおよびスピーカー	○	○	○	○	○	○	○	○	○	○	○
ダイヤル プラン	○	○	○	○	○	○	○	○	○	○	○
SIP トランク経由の発信コールのための、MTP なしの SIP アーリー オファーのサポート	○	○	○	○	○	○	○	○	○	○	○
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	○	○	○	○	○	○	○	○	○	○	○
G.722	×	×	○	○	○	○	○	○	○	○	○
G.723	×	×	×	×	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×	×	×	×	×
G.729	○	○[12]	○[12]	○[12]	○[12]	○[12]	○[12]	○[12]	○	○	○
iLBC	×	×	×	○	○	×	×	○	○	○	○
iSAC	×	×	×	×	×	×	×	×	○	○	○
ワイドバンド オーディオ	×	×	×	×	×	×	×	×	×	×	×
ワイドバンド ビデオ	×	×	×	×	×	×	×	×	×	×	×
ワイドバンド アコースティック	×	×	×	○	○	×	×	○	○	○	○
音声アクティビティ検出（VAD）	○	○	○	○	○	○	○	○	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	○	○	○	○	○
DTMF：H.245	×	×	×	×	×	×	×	×	×	×	×
DTMF：SCCP	×	×	×	×	×	×	×	×	×	×	×
DTMF：RFC2833	○	○	○	○	○	○	○	○	○	○	○
DTMF：KPML	×	×	○	○	○	○	○	○	○	○	○
DTMF：無指定の NOTIFY	×	×	×	×	×	×	×	×	×	×	×

1. 2 つの 10/100 Base-T イーサネット接続。
2. Cisco Unified IP Phones 7961G および 7962G は 2 つの 10/100 Mbps イーサネット接続を備えており、Cisco Unified IP Phones 7961G-GE および 7965G は 2 つの 10/100/1000 Mbps イーサネット接続を備えています。
3. 2 つの 10/100/100 Mbps イーサネット接続。

4. Cisco Unified IP Phone 7961G は Cisco Prestandard PoE と IEEE 802.3af PoE の両方をサポートしており、Cisco Unified IP Phone 7961G-GE は IEEE 802.3af PoE だけをサポートしています。
5. Cisco Unified IP Phone 6941 にコール ウェイティングを実装するには、その 2 つの回線に同じ DN（異なるパーティション）を設定し、第 1 の回線が通話中に第 2 の回線に転送されるようにします。
6. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Unified CM で電話機の設定が認識されないため、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Unified CM の [User] ページで有効にされている場合、Unified CM はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Unified CM の [User] ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
7. この機能は、電話機でローカルに設定できます。
8. IP を使用する Cisco Unified IP Phone 7960G でサポートされているのは、Ad Hoc 会議用のローカル ミキシングと最大 3 者による会議だけです。
9. リダイヤル。
10. スピード ダイヤルに限る。コール履歴エントリは対象外。
11. 限定的なサポート。
12. これらの IP 電話機のモデルは、G.729b または G.729ab をサポートしていません。

表 18-14　専用エンドポイント

機能	7921G	7925G および 7925G-EX	7926G	7936	7937G	7985G	Cisco E20
イーサネット接続	×	×	×	○[1]	○[1]	○[2]	○[3]
イーサネット スイッチ（PC ポート）	×	×	×	×	×	○	○
Cisco Power-Over-Ethernet（PoE）	×	×	×	×	×	×	×
IEEE 802.3af Power-Over-Ethernet（PoE）	×	×	×	×	○	○	×
ローカリゼーション	○	○	○	×	○	○	○
ディレクトリ番号	6	6	6	1	1	2	1
回線あたりの最大コール数	2	2	2	2	6	100	5
液晶ディスプレイ	○	○	○	○	○	○	○
発信者 ID	○	○	○	○	○	○	○
コール ウェイティング	○	○	○	○	○	○	○
コール ウェイティング時の発信者 ID	○	○	○	○	○	○	○
保留	○	○	○	○	○	○	○
ブラインド転送	×	×	×	×	×	×	○
初期在席転送	○	○	○	○	○	○	×
打診転送	○	○	○	○	○	○	○
自動転送	○	○	○	○	○	○	○
自動応答	○	○	○	×	○	○	○
Ad Hoc 会議	○	○	○	○	○	○	×
Meet-Me 会議	○	○	○	○	○	○	×
コール ピックアップ	○	○	○	○	○	○	×
グループ ピックアップ	○	○	○	○	○	○	×
リダイヤル	○[4]	○[4]	○[4]	○	○	○	○
スピード ダイヤル	○	○	○	×	○	○	○

表 18-14　専用エンドポイント（続き）

機能	7921G	7925G および 7925G-EX	7926G	7936	7937G	7985G	Cisco E20
オンフック ダイヤル	○	○	○	○	○	○	○
ボイスメールへのアクセス	○	○	○	×	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○	×	×	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	×	×	×	×	×	×	×
ビデオ コール	×	×	×	×	×	○	○
Survivable Remote Site Telephony（SRST）サポート	○	○	○	○	○	○[5]	×
ユニキャスト MoH	○	○	○	○	○	○	○
マルチキャスト MoH	○	○	○	○	○	×	×
保留トーン	○	○	○	○	○	○	○
スピーカー	○	○	○	○	○	○	○
ヘッドセット ジャック	○	○	○	×	×	○	○
消音	○	○	○	○	○	○	○
Multilevel Precedence and Preemption（MLPP）	○	○	○	×	○	○	○
割り込み	○	○	○	×	○	○	×
C 割り込み	○	○	○	×	○	○	○
ワンボタン割り込み	×	×	×	×	×	×	×
回線をまたいで参加（Join Across Lines）	×	×	×	×	×	×	×
プログラム可能な回線キー	×	×	×	×	×	×	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×	×	×	×	×
ビジー ランプ フィールド	×	×	×	×	×	×	×
+ ダイヤリングを使用する発番号の標準化	×	×	×	×	×	×	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	○	○	○	×	○	×	×
シグナリングおよびメディア暗号化	○	○	○	×	×	×	×
シグナリングの完全性	○	○	○	×	×	×	×
製造元でインストールされる証明書（X.509v3）	○	○	○	×	×	×	×
現場でインストールされる証明書	○	○	○	×	×	×	×
サードパーティの XML サービス	○	○	○	×	○	×	○
外部マイクおよびスピーカー	○	○[6]	○[6]	×	○[7]	×	×
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0x88	0x88
G.711	○	○	○	○	○	○	○

表 18-14　専用エンドポイント（続き）

機能	7921G	7925G および 7925G-EX	7926G	7936	7937G	7985G	Cisco E20
G.722	○	○	○	×	○	○	○
G.723	×	×	×	×	×	×	×
G.726	×	×	×	×	×	×	×
G.729	○	○	○	○	○	○	○
iLBC	○	○	○	×	×	×	×
ワイドバンド オーディオ	×	×	×	×	×	×	○
H.261	×	×	×	×	×	○	×
H.263	×	×	×	×	×	○	○
H.263+	×	×	×	×	×	○	○
H.264	×	×	×	×	×	○	○
音声アクティビティ検出（VAD）	○	○	○	○	○	○	×
コンフォート ノイズ生成（CNG）	○	○	○	○	○	○	×
DTMF：H.245	×	×	×	×	×	×	×
DTMF：SCCP	○	○	○	○	○	○	×
DTMF：RFC2833	×	×	×	×	○	×	○

1. 1 つの 10/100 Base-T。
2. 2 つの 10/100 Base-T。
3. 2 つの 10/100/1000 Mbps イーサネット接続。
4. リダイヤル。
5. SRST ではオーディオだけがサポートされます。
6. Bluetooth ヘッドセットがサポートされています。
7. 無線ラペルマイクがサポートされています。

表 18-15　ソフトウェアベースのエンドポイントの機能

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
ディレクトリ番号	1	8	8
発信者 ID	○	○	○
コール ウェイティング	○	○	○
コール ウェイティング時の発信者 ID	○	○	○
保留	○	○	○
コール転送	○[1]	○	○
自動転送	×	○	○
自動応答	○	○	○
Ad Hoc 会議	○[2]	○	○
Meet-Me 会議	×[3]	○	×

表 18-15　ソフトウェアベースのエンドポイントの機能（続き）

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
Web 会議	○	×	×
コール ピックアップ	×	○	○
グループ ピックアップ	×	○	○
リダイヤル	○[4]	○[4]	○[4]
スピード ダイヤル	○[5]	○	○
オンフック ダイヤル	○	○	○
ボイスメールへのアクセス	○	○	○
メッセージ待機インジケータ（MWI）	○	○	○
断続ダイヤル トーンまたは音声メッセージ待機インジケータ（AMWI）	×	○[6]	○[6]
ビデオ コール	○	○[7]	×
Survivable Remote Site Telephony（SRST）サポート	×	○	○
ユニキャスト保留音（MoH）	○	○	○
マルチキャスト保留音（MoH）	○	○	○
保留トーン	×	○	×
消音	○	○	○
Multilevel Precedence and Preemption（MLPP）	×	○	×
割り込み	×	○	○
C 割り込み	×	○	○
ワンボタン割り込み	×	○	×
回線をまたいで参加	×	○	×
プログラム可能な回線キー	×	○	×
「Single Call per Line」ユーザ エクスペリエンス	×	×	×
ビジー ランプ フィールド	×	○	○
+ ダイヤリングを使用する発番号の標準化	×	○	×
Gratuitous Address Resolution Protocol（GARP）を無効にする	×	×	×
シグナリングおよびメディア暗号化	×	○	○
シグナリングの完全性	×	×	×
製造元でインストールされる証明書（X.509v3）	×	×	×
現場でインストールされる証明書	×	×	×
サードパーティの XML サービス	×	○	○

表 18-15　ソフトウェアベースのエンドポイントの機能（続き）

機能	Unified Personal Communicator	SCCP を使用する IP Communicator	SIP を使用する IP Communicator
シグナリング パケット ToS 値のマーキング	×	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8
Skinny Client Control Protocol（SCCP）	×	○	×
セッション開始プロトコル（SIP）	○	×	○
G.711	○	○	○
G.722	×	○[6]	○[6]
G.723	×	×	×
G.726	×	×	×
G.729	○	○	×
iLBC	○	○[6]	○[6]
ワイドバンド オーディオ	×	○	×[8]
ワイドバンド ビデオ	×	×	×
H.261	×	×	×
H.263	○	×	×
H.264	○	×	×
音声アクティビティ検出（VAD）	○	○	○
コンフォート ノイズ生成（CNG）	○	○	○
DTMF：H.245	×	×	×
DTMF：SCCP	×	○	×
DTMF：RFC2833	○	○	○
DTMF：KPML	○	×	○

1. Cisco Unified Personal Communicator は明示的な転送機能を備えていません。Cisco Unified Personal Communicator ユーザがコールを転送するには、2 つのコールをマージした後に接続解除して転送結果を取得します。
2. Cisco Unified Personal Communicator は、「consult, then merge」機能（IP Phone での会議に相当）をサポートしていませんが、電話会議の **merge**（IP Pone での **join** に相当）はサポートしています。
3. Cisco Unified Personal Communicator は Meet-Me 会議を作成できませんが、ユーザは正しい番号をダイヤルして会議に参加できます。
4. リダイヤル。
5. Cisco Unified Personal Communicator は Unified CM スピード ダイヤル ページをサポートしていませんが、同様の方法で個人連絡表などの Contacts（buddy）リストからのクリックコールをサポートしています。
6. この機能は、Cisco IP Communicator Release 2.1 ではサポートされていません。
7. Cisco IP Communicator を Cisco Unified Video Advantage と組み合せて SCCP モードで動作させると、ビデオコールがサポートされます。
8. Cisco IP Communicator 2.1 は、ワイドバンド オーディオをサポートしていません。

表 18-16　Cisco Unified IP Phones 9951 と 9971、Cisco IP Video Phone 7985G、および Cisco E20 Video Phone

ビデオ機能	9951	9971	7985G	Cisco E20
ディスプレイ サイズ	5 インチ（10.2 cm × 7.6 cm）	5.6 インチ（11.2 cm × 8.6 cm）	8.4 インチ	10.6 インチ
ディスプレイ解像度	VGA（640 x 480）	VGA（640 x 480）	XGA（1024 x 768）	WXGA（1280 x 768）
ピクチャ イン ピクチャ	あり	あり	あり	あり
ビデオ ミュート	あり	あり	あり	あり
ビデオ コーデックのサポート	H.264 レベル 3.0（ベースライン プロファイル）	H.264 レベル 3.0（ベースライン プロファイル）	H.264、H.263+、H.263、および H.261	H.264、H263+、H.263
カメラ解像度（9951 および 9971 のオプション接続）	VGA（640 x 480）（24 fps） CIF（352 x 288）（30 fps）	VGA（640 x 480）（24 fps） CIF（352 x 288）（30 fps）	SIF（352 x 240 ピクセル）（30 fps） 4SIF（704x480）（15 fps） 4SIF（704x576）（15 fps）	w488p（768x448）（30 fps） 488p（576x448）（30 fps） w288p（512x288）（30 fps） CIF（352 x 288）（30 fps） QCIF（176 x 144）（30 fps）

CHAPTER 19

Cisco Unified CM アプリケーション

Cisco Unified CM アプリケーションは、基礎的な IP テレフォニーに多数の動作および機能の拡張を提供します。外部の eXtensible Markup Language（XML）生産性向上アプリケーションまたは IP Phone Service は、Web サーバまたはほとんどの Cisco Unified IP Phone 上のクライアント（あるいはその両方）で実行できます。たとえば、ユーザのデスク上の IP Phone を使用して、株式相場、天気情報、フライト情報など各種の Web ベースの情報を取得できます。また、カスタム IP Phone サービス アプリケーションを作成すると、ユーザが在庫を追跡したり、時間単位で顧客に課金したり、会議室の環境（照明、ビデオ画面、室温など）を制御できます。Cisco Unified CM には、次に示すような追加機能を提供する統合アプリケーションも多数あります。

- Cisco Extension Mobility（EM）

  Extension Mobility（EM; エクステンション モビリティ）機能では、モバイル ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をそのユーザ用に 設定できます。

- Cisco Unified Communications Manager Assistant（Unified CM Assistant）

  Unified CM Assistant は、アシスタントが 1 人以上のマネージャあて着信電話コールを処理できるようにする Cisco Unified CM に統合されたアプリケーションです。

- Cisco WebDialer

  WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。

場合によっては、これらの統合アプリケーションが追加機能を提供するために、IP Phone Service を呼び出すこともあります。

この章では、次の Cisco Unified CM アプリケーションについて説明します。

この章の新規情報

表 19-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 19-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco エクステンション モビリティ アプリケーション サービスおよび Cisco エクステンション モビリティ サービス	「エクステンション モビリティ」（P.19-8）	2011 年 6 月 2 日
アテンダント コンソールのキャパシティ プランニング	「アテンダント コンソールのキャパシティ プランニング」（P.19-47）	2010 年 4 月 2 日
クラスタ間のエクステンション モビリティ（EMCC）	「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10） 「クラスタ間のエクステンション モビリティ（EMCC）の設計上の考慮事項」（P.19-19）	2010 年 4 月 2 日
セキュア IP Phone Service URL	「IP Phone Service のアーキテクチャ」（P.19-2）	2010 年 4 月 2 日

IP Phone Service

Cisco Unified IP Phone Service は、Web クライアントやサーバ、および Cisco Unified IP Phone の XML 機能を利用するアプリケーションです。Cisco Unified IP Phone のファームウェアには、限定的な Web ブラウジング機能を可能にするマイクロブラウザが含まれています。これらの電話サービス アプリケーションを、ユーザのデスクトップ電話機上で直接実行することで、付加価値サービスが提供され、生産性も向上する可能性があります。この章で *phone service* という用語は、Cisco Unified IP Phone を宛先および発信元としてコンテンツを送受信するアプリケーションを指します。

ここでは、IP Phone Service 機能の設計について次の項目を説明します。

- 「IP Phone Service のアーキテクチャ」（P.19-2）
- 「IP Phone Service のハイ アベイラビリティ」（P.19-6）
- 「IP Phone Service のキャパシティ プランニング」（P.19-7）
- 「IP Phone Service の設計上の考慮事項」（P.19-8）

IP Phone Service のアーキテクチャ

IP Phone サービスは、次のような複数の方法で開始できます。

- ユーザ起動（プル）

  IP Phone ユーザが Services ボタンを押すと、ユーザ加入電話サービスのリストを表示するために、HTTP GET メッセージが Cisco Unified CM に送信されます。図 19-1 は、この機能を示しています。

- 電話機起動（プル）

  IP Phone ファームウェア内で、アイドル時間の値は URL Idle Time パラメータによって設定できます。このタイムアウト値を超えた場合、IP Phone のファームウェア自体が URL Idle パラメータで指定されるアイドル状態の URL の場所に対して、HTTP GET を開始します。

- 電話サービス起動（プッシュ）

  電話サービス アプリケーションは、電話機に HTTP POST メッセージを送信することによって、IP Phone にコンテンツをプッシュできます。

（注）　電話サービスを呼び出すために電話機の Web クライアントが使用されるユーザ起動および電話機起動のプル機能とは異なり、電話サービス起動のプッシュ機能は、電話機の（クライアントではなく）Web サーバに（HTTP POST を通じて）コンテンツをポストすることによって、電話機上の処理を呼び出します。

図 19-1 は、ユーザが開始する IP Phone サービス処理の詳細を示しています。ユーザが Services ボタンを押したときに Services Provisioning で外部 URL にセットされる場合、デフォルトでは、HTTP GET メッセージが IP Phone から Cisco Unified CM の getservicesmenu.jsp スクリプトに送信されます（ステップ 1）。URL Services パラメータを変更することによって、異なるスクリプトを指定できます。getservicesmenu.jsp スクリプトは、個々のユーザが加入している電話サービス URL ロケーションのリストを返します（ステップ 2）。HTTP 応答は、IP Phone にこのリストを返します（ステップ 3）。ユーザによって選択される追加の電話サービス メニュー オプションは、ユーザと選択された電話サービス アプリケーションを含む Web サービス間で HTTP メッセージングを継続します（ステップ 4）。

（注）　Service Provisioning エンタープライズ パラメータが内部にセットされる場合は、ステップ 1 からステップ 3 まで がバイパスされ、電話サービスの処理はステップ 4 から開始します。

図 19-1　ユーザ起動の IP Phone Service のアーキテクチャ

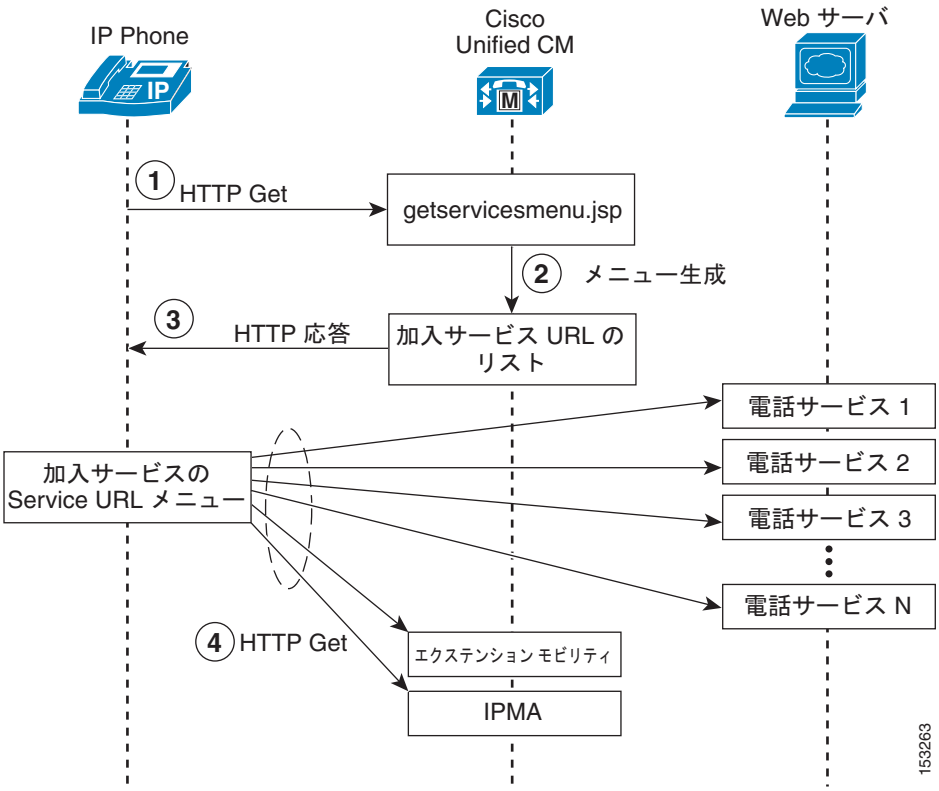
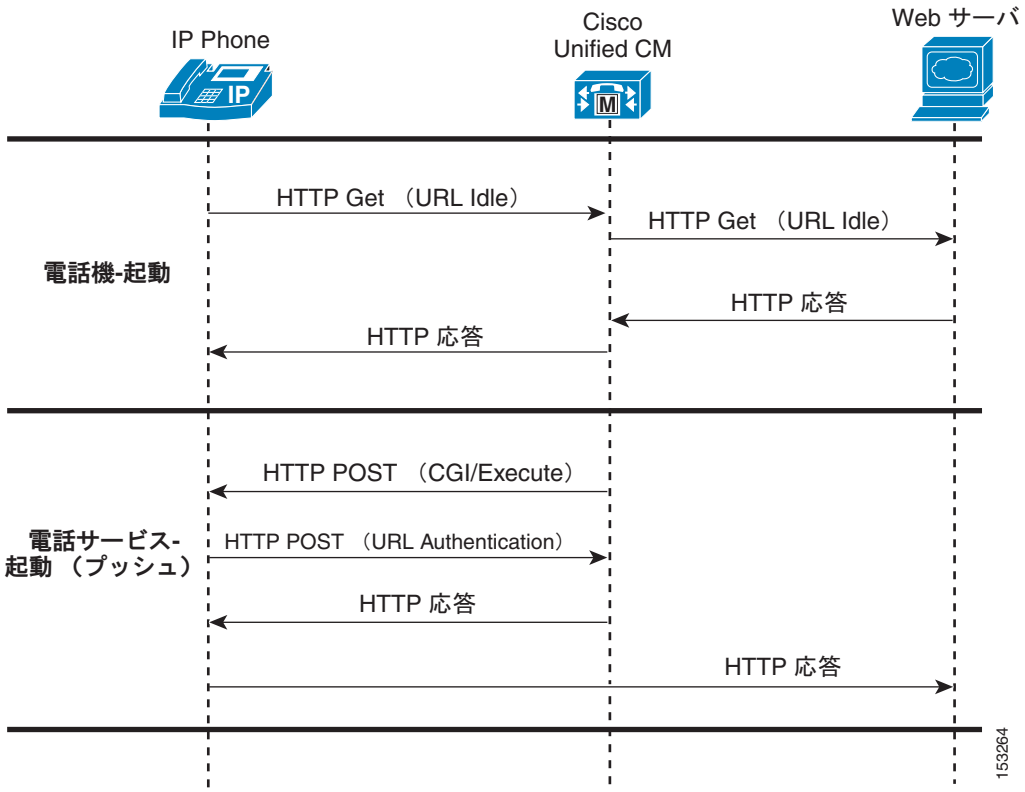


図 19-2 は、電話機起動と電話サービス起動の両方のプッシュ機能の例を示しています。電話機起動の例では、URL Idle Time に到達した時点で、自動的に、電話機から URL Idle パラメータで指定されたロケーションに HTTP GET が送信されます。HTTP GET は、Cisco Unified CM を通じて外部 Web サーバに転送されます。この Web サーバは HTTP 応答を返し、この応答は Cisco Unified CM によって電話機にリレーされ、電話機は画面にテキストまたはイメージ（あるいはその両方）を表示します。

電話サービス起動のプッシュの例で、外部 Web サーバ上の電話サービスは電話機の Web サーバに対して、Common Gateway Interface（CGI）または Execute 呼び出しで HTTP POST を送信します。CGI または Execute 呼び出しを実行する前に、電話機は URL Authentication パラメータで指定されるプロキシ認証サービスを使用して要求を認証します。このプロキシ認証サービスは、電話機に対する直接の要求を検証するための、電話機と Cisco Unified CM ディレクトリ間のインターフェイスを提供します。要求が認証された場合、Cisco Unified CM は電話機に HTTP 応答を転送します。次に、電話機の Web サーバは要求された処理を実行し、電話機は外部 Web サーバに HTTP 応答を返します。認証に失敗した場合、Cisco Unified CM は、HTTP 否定応答を転送し、電話機は要求された CGI または Execute 処理を実行しないで、HTTP 否定応答を外部 Web サーバに転送します。

図 19-2　電話機起動および電話サービス起動の IP Phone Service のアーキテクチャ



XML Services に加えて、[Service Category] が [Java MIDlet] の新しいサービスを作成できます。Java MIDlet タイプのサービスが起動されると、設定された Service URL には、MIDlet JAD ファイルを取得できる URL を含みます。アプリケーション サーバは JAD ファイルの要求を受信すると、そのサーバは適切な JAR ファイルを対応デバイスに返します。この対応デバイスでは、電話の MIDlet インストーラがダウンロードし、処理しまします。

Cisco IP Phone の Java MIDlet サポートの詳細については、http://www.cisco.com の Cisco IP Phone データ シートを参照してください。

（注）　電話機はその設定ファイルを TFTP を介してダウンロードした後、電話機はリストのサービスが変わっていないかどうか判断するためサービス設定を解析し、変わっている場合にはそのローカル（持続）サービス設定を更新します。変更されたサービスが Java MIDlet（これは明示的にプロビジョニングされ、電話機に保存されます）の場合は、次に、電話機は必要なインストール処理、アップグレード処理、ダウングレード処理、およびアンインストール処理を、設定ファイルにプロビジョニングされたものに応じて順次実行します。MIDlet インストールが失敗の場合、電話機がその設定ファイルをチェックする次回（ブート、リセット、または再スタート時）に MIDlet インストールを再試行します。

管理者は、設定されたサービスの [Service Type] を [IP Phone Services]、[Directories]、または [Messages] のいずれかに指定する追加機能を使用できます。これは、ユーザが IP phone で新しいサービスにアクセスするため押すボタンを管理する柔軟性を管理者に与えます。新しいサービスはオプションとして Enterprise Subscriptions と同様に設定できます。これにより、それらサービスは個々の電話機ごとに加入を更新する必要がなく、自動的にすべての IP phone に表示されます。さらに、サービスは Unified CM データベースからそのサービスを削除する必要がなく有効にできたり無効にできたりします。

（注）　Missed Calls、Placed Calls、および Corporate Directory などのデフォルトのサービスも無効にできます。これは、管理者が Service URL で指定されたデフォルト サービスをもとにしてカスタム サービスを作成できるようにします。

Unified CM 8.*x* は、非セキュア URL 以外に、HTTPS を使用してセキュア IP Phone Service URL を設定する機能を提供します。HTTPS をサポートする電話機は、自動的にセキュア URL を使用します。IP Phone の信頼検証サービスとセキュリティ認証処理の詳細、および HTTPS をサポートする電話機の全リストについては、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Security Guide*』で、HTTPS の情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

IP Phone Service のハイ アベイラビリティ

電話機のユーザに対して信頼性の高いサービスを確保するには、システムの障害時に冗長システムにシームレスに移行することにより、高レベルのシステムの可用性を維持する必要があります。

Services Provisioning で内部にセットされる場合、電話機は加入した電話サービスが設定された設定ファイルを受信し、これら（および対応するサービス URL）をフラッシュ メモリに保存します。これにより電話機は、最初に Cisco CallManager IP Phone Service を参照せずにサービス URL に直接アクセスできます。Services Provisioning で内部にセットされる場合、Corporate および Personal Directories デフォルト サービス には電話機に組み込まれた追加レベルの冗長性もあります。これらサービスが選択された場合、電話機は適切な URL ストリング を使用して現在登録されている Unified CM に、HTTP メッセージの送信を試行します。したがって、電話機のデバイス プールの Unified CM Group の設定が、これらサービスの冗長性を提供します。

Services Provisioning が External URL、または両方にセットされる場合、電話サービスのほとんどのバックエンド処理は Web サーバで発生しますが、電話機はやはり加入電話サービスのそれらサービス URL を通知するには Unified CM に依存します。図 19-1 および図 19-2 に示す IP Phone サービス機能のアーキテクチャおよびメッセージ フローでは、次の 2 つの主な障害のシナリオを検討する必要があります。

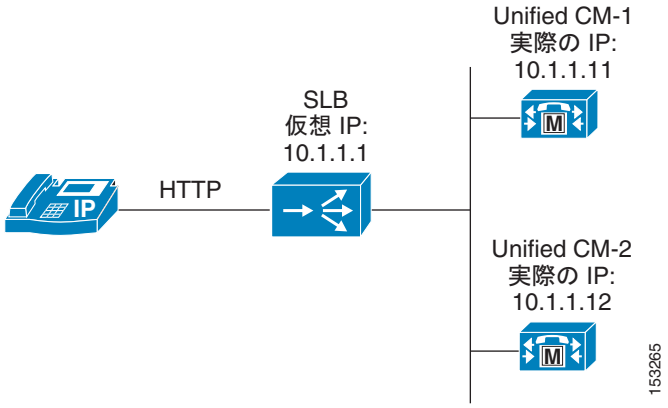
障害シナリオ 1：Cisco Unified CallManager の Cisco Unified IP Phone Service サーバの障害

この場合の冗長性は、図 19-3 に示すように、ある種の Server Load Balancing（SLB; サーバ ロード バランシング）に依存します。この SLB では、1 つ以上の Unified CM サーバを指すために仮想 IP アドレス（または DNS による解決可能なホスト名）が使用されます。この仮想 IP アドレス（または DNS による解決可能なホスト名）は、URL Services パラメータの設定時に使用されます。SLB デバイスは、Unified CM サブスクライバ ノードの実 IP アドレスを使用して設定されます。このため、Cisco Unified CM サーバに障害が発生しても、電話機の Services ボタンが押されたときに、IP Phone Service 加入リストは電話機に正常に返されます。また、Cisco Unified CM サーバで実行されるエクステンション モビリティおよび Unified CM Assistant などの電話サービスも、この方法によって冗長性を持つ可能性があります（「エクステンション モビリティのハイ アベイラビリティ」（P.19-15）および「Unified CM Assistant のハイ アベイラビリティ」（P.19-24）を参照）。

Cisco Application Control Engine（ACE）など多くの SLB デバイスは、障害発生時の複数のサーバと自動転送要求のステータスをモニタするように設定できます。Cisco Application Control Engine（ACE）の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

図 19-3　電話サービスに冗長性を提供する方法



障害シナリオ 2：特定の IP Phone Service をホストしている外部 Web サーバの障害

このシナリオでは、Cisco Unified CM サーバへの接続は保持されますが、ユーザ加入電話サービスをホストしている Web サーバへのリンクに障害が発生します。Services ボタンが押されたときに IP Phone は引き続き Cisco Unified CM サーバにアクセスできるため、これは冗長性を提供するための比較的容易なシナリオです。この場合、IP Phone は Web サーバにアクセスする他の任意 HTTP クライアントに似ています。このため、（図 19-3 に示すような）SLB 機能を再び使用して、電話機から、ユーザ加入電話サービスをホストしている 1 つ以上の冗長 Web サーバに HTTP 要求を転送できます。

IP Phone Service のキャパシティ プランニング

Cisco Unified IP Phone サービスの大部分は、HTTP クライアントとして機能します。ほとんどの場合、加入サービスのロケーションへの転送サーバとしてだけ Cisco Unified CM が使用されます。Cisco Unified CM は電話サービスへの転送サーバとして機能するため、ユーザが Service キーを押して電話サービスを要求したときに、Cisco Unified CM へ与えるパフォーマンスの影響は最小限になります。

（注）　エクステンション モビリティおよび Unified CM Assistant 電話サービスの場合、Cisco Unified CM は転送サーバ以上の役割を果たすので、パフォーマンスへの影響を検討する必要があります。これらのアプリケーションの特定のパフォーマンスおよびスケーラビリティの考慮事項については、「エクステンション モビリティ」（P.19-8）および「Unified CM Assistant」（P.19-20）の項を参照してください。

IP Phone はクライアントまたはサーバのいずれかであるため、IP Phone サービスで使用される必要帯域幅の推定は、Web 運用サーバにある HTTP コンテンツと同じテキストにアクセスする HTTP ブラウザの帯域幅の推定に似ています。

IP Phone Service の設計上の考慮事項

統合エクステンション モビリティおよび Unified CM Assistant アプリケーションの電話サービスを除き、IP Phone サービスは独立したオフクラスタの Unified CM 以外の Web サーバに存在する必要があります。Unified CM サーバ ノードで、エクステンション モビリティおよび Unified CM Assistant 以外の電話サービスを実行することはサポートされていません。

ほとんどのシスコ製 IP 電話がテキストとグラフィックスを含むコンテンツをサポートしています。Cisco Unified IP Phone 7911G などの一部の電話機は、テキストベースの XML アプリケーションしかサポートしていません。

エクステンション モビリティ

Cisco Extension Mobility（EM; エクステンション モビリティ）機能では、ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone をユーザ個別の設定に設定 することが可能です。ユーザがログインすると、IP Phone には、回線番号、スピード ダイヤル、サービス リンク、およびその他のユーザ固有の電話機のプロパティなど、ユーザの個別のデバイス プロファイル情報が設定されます。たとえば、ユーザ X がデスクに向かって電話機にログインした場合は、そのユーザのディレクトリ番号、スピード ダイヤル、およびその他のプロパティがその電話機に表示されますが、ユーザ Y が別のときに同じデスクを使用した場合は、ユーザ Y の情報が表示されます。EM 機能では、認証されたユーザのデバイス プロファイルに従って電話機が動的に設定されます。このアプリケーションの利点は、電話機が EM をサポートしている限り、物理的な場所に関係なく、ユーザが Cisco Unified CM クラスタ内の任意の電話機で自分の内線番号に接続できることです。

ここでは、エクステンション モビリティ機能の設計について次の項目を説明します。

エクステンション モビリティ対応 Unified CM Service

EM アプリケーションは、Cisco エクステンション モビリティ サービスに依存します。このサービスは機能サービスであり、サービスアビリティのページから手動でアクティブにする必要があります。

EM は次のネットワーク サービス にも依存します。これらのサービスは、インストール時にすべての Unified CM ノードで自動的にアクティブにされます。

- Cisco エクステンション モビリティ アプリケーション
- Cisco CallManager Cisco IP Phone Services

Cisco エクステンション モビリティ アプリケーション サービスは、EM ユーザ電話機と Cisco エクステンション モビリティ サービスとの間のインターフェイスを提供するネットワーク サービスです。また、Cisco エクステンション モビリティ アプリケーション サービスは、クラスタ内の変更通知インジケータにサブスクライブして、アクティブな Cisco エクステンション モビリティ サービスがあるクラスタ内のノードのリストを維持します。

エクステンション モビリティのアーキテクチャ

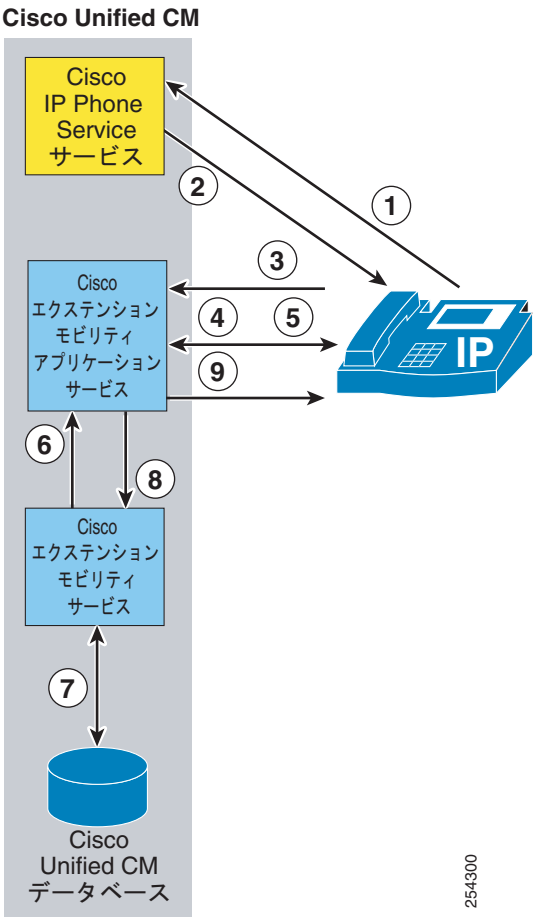
図 19-4 は、EM アプリケーションのメッセージ フローとアーキテクチャを示しています。電話機のユーザが EM アプリケーションにアクセスする場合、次の一連のイベントが発生します。

1. ユーザが電話機の Services ボタンを押すと、[Enterprise Parameter] 設定ページの [URL Services] パラメータで指定された URL に発信されます（図 19-4 のステップ 1 を参照）。
2. HTTP/XML コールが IP Phone Service に対して生成され、このコールはユーザの電話機が加入しているすべてのサービスのリストを返します（図 19-4 のステップ 2 を参照）。

（注）　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、Services Provisioning が外部 URL または両方に設定されている場合、ユーザが回線ボタンまたはスピード ダイヤル ボタンを押して、Cisco エクステンション モビリティ アプリケーション サービスへの直接コールを生成できるように、Service URL ボタンをユーザの電話機の EM に対して設定できます。ステップ 1 およびステップ 2 もバイパスされます。

3. 次に、ユーザはエクステンション モビリティ電話サービスのリストを選択します。この選択によって、電話機と Cisco エクステンション モビリティ サービス間のインターフェイスの役割を果たす Cisco エクステンション モビリティ アプリケーション サービスに対して HTTP コールが生成されます（図 19-4 のステップ 3 を参照）。
4. 次に、Cisco エクステンション モビリティ アプリケーション サービスは、ユーザ ログイン クレデンシャル（ユーザ ID および PIN）を要求している電話機に XML 応答を返すか、またはユーザがすでにログインしている場合は、ユーザに電話機からログオフするかどうかを尋ねる応答を返します（図 19-4 のステップ 4 を参照）。
5. ユーザがログインしようとしている場合、そのユーザは電話機のキーパッドを使用して有効なユーザ ID および PIN を入力する必要があります。ユーザが [Submit] ソフトキーを押した後に、入力したユーザ ID および PIN を含む応答が、Cisco エクステンション モビリティ アプリケーション サービスに返されます（図 19-4 のステップ 5 を参照）。
6. 次に、Cisco エクステンション モビリティ アプリケーション サービスは、このログイン情報を Cisco エクステンション モビリティ サービスに転送します。このサービスは、Unified CM データベースと対話して、ユーザのクレデンシャルを検証します（図 19-4 のステップ 6 を参照）。Cisco エクステンション モビリティ アプリケーション サービスはクラスタの変更通知にサブスクライブして、Cisco エクステンション モビリティ サービスがアクティブになっているクラスタ内の全ノードのリストを維持します。その結果、同じ Unified CM ノードで Cisco エクステンション モビリティ サービスが実行されていない場合、Cisco エクステンション モビリティ アプリケーション サービスは、Cisco エクステンション モビリティ サービスが実行されている他の Unified CM ノードにログイン情報を転送します。
7. ユーザのクレデンシャルの検証に成功したときに、Cisco エクステンション モビリティ サービスも Unified CM データベースと対話して、適切なユーザ デバイス プロファイルを読み取って選択し、デバイスのプロファイルに基づいて電話機の設定に必要な変更を書き込みます（図 19-4 のステップ 7 を参照）。
8. これらの変更が加えられると、Cisco エクステンション モビリティ サービスは、Cisco エクステンション モビリティ アプリケーション サービスに成功応答を返します（図 19-4 のステップ 8 を参照）。
9. 次に Cisco エクステンション モビリティ アプリケーション サービスは電話機にリセット メッセージを送信し、電話機はリセットされ、新しい電話設定を受け入れます（図 19-4 のステップ 9 を参照）。

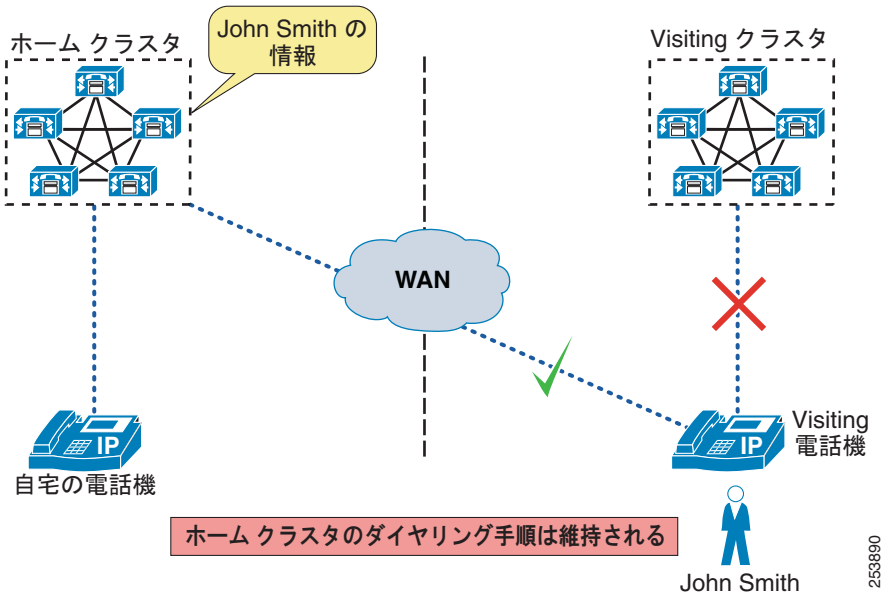
図 19-4　EM アプリケーションのアーキテクチャとメッセージ フロー



クラスタ間のエクステンション モビリティ（EMCC）

Unified CM 8.*x* は、Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）という新機能によって、企業内のクラスタ間でエクステンション モビリティ ログインを実行する機能を提供します。EMCC のアーキテクチャの概要を理解することが重要です。EMCC 機能はホーム クラスタおよび Visiting クラスタという概念を使用します。これらの用語は、ログインを実行するユーザの観点から定義されています。ユーザがオフィスに移動して電話機にログインしようとしたときに、この電話機が登録されているクラスタのデータベースにユーザの情報がない場合、このクラスタは Visiting クラスタと見なされ、この電話機は以降は Visiting 電話機と呼ばれます。図 19-5 に、ホーム クラスタと Visiting クラスタの概念を示します。

図 19-5　EMCC のホーム クラスタと Visiting クラスタ



Visiting クラスタ内の EM サービスは、Unified CM 内で構成されている各 EMCC リモート クラスタに照会を送信して、ユーザのホーム クラスタを見つけようとします。ユーザのホーム クラスタが肯定応答を返した場合、両方のクラスタの EM サービス間で通信が開始され、情報が交換されます。基本的にはデバイス情報がホーム クラスタのデータベースに取り込まれ、ホーム クラスタはこの Visiting 電話機の設定ファイルを作成できます。この設定ファイルには、Visiting クラスタからデバイス設定、ホーム クラスタから設定パラメータ、およびホーム クラスタ内のユーザのデバイス プロファイルが組み込まれます。ホーム クラスタの TFTP サーバにこの Visiting 電話機の設定ファイルができると、Visiting クラスタによって発行されたリセットによって、Visiting 電話機は Visiting クラスタから小さな設定をダウンロードし、これによってさらにホーム クラスタから完全な設定をダウンロードするよう指示されます。最終的には、Visiting 電話機はホーム クラスタにクロス登録されます。つまり、すべての呼制御シグナリングはホーム クラスタの Unified CM サブスクライバと Visiting 電話機の間で発生し、ユーザのホーム クラスタのダイヤリング手順が維持されます。

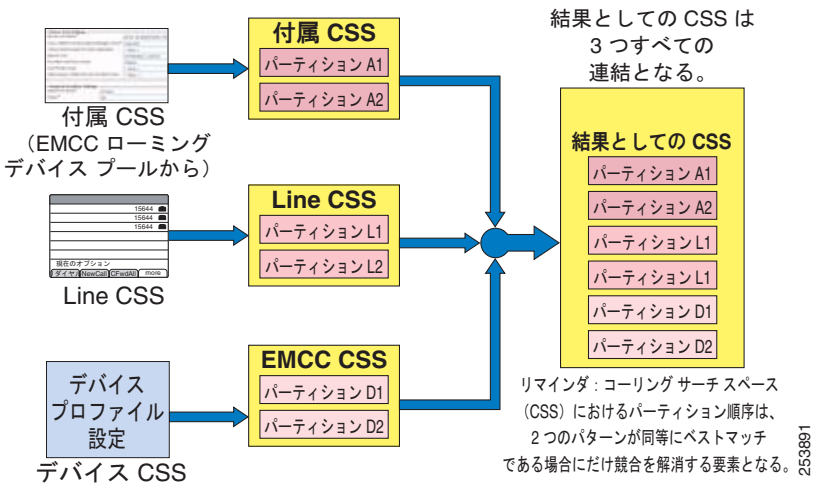
EMCC ログイン プロセスの段階的な説明については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Features and Services Guide*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

コール処理

EMCC コール処理動作はダイヤル プランの設計に影響するため、これを理解することも重要です。ユーザが Visiting クラスタの電話機にログインすると、ユーザがダイヤルした数字はホーム クラスタによって、Visiting 電話機の集合 Call Search Space（CSS; コーリング サーチ スペース）に従って分析されます。これは、Visiting 電話機用のホーム クラスタのデバイス プール（EMCC ローミング デバイス プールと呼ばれる）内の付加 CSS、ユーザのデバイス プロファイルに関連付けられたディレクトリ番号に設定された回線 CSS、およびユーザのデバイス プロファイルに設定された EMCC CSS を連結したものです。図 19-6 に、EMCC 電話機の結果の CSS を示します。

図 19-6　EMCC 電話機の結果の CSS



付加コーリング サーチ スペースは、新規のコール ルーティング設定パラメータです。このパラメータは、EMCC により使用され、Visiting クラスタからユーザに対して緊急番号のインターセプトおよびルーティングを行います。付加 CSS には、911、112、または 999 などのディレクトリ番号の付いたパーティションがあります。このパーティションは、Visiting クラスタにコールをルーティングして、そのコールが電話機の物理的な場所に対してローカルな緊急サービスに連絡できるようにします。付加コーリング サーチ スペースと EMCC ローミング デバイス プールの詳細、および Visiting 電話機に関連付ける方法については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Features and Services Guide*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

（注）　EMCC 機能に関連付けられた EMCC ローミング デバイス プールは、デバイス モビリティ機能に関連付けられたローミング デバイス プールとは関係ありません。

EMCC ユーザは、コールを発信する際に、ホームの Unified CM のルートおよび番号計画が利用されることを承知しておく必要があります。たとえば、クラスタ A のユーザがクラスタ B の電話機にログインして、すぐ隣のクラスタ B 電話機のディレクトリ番号にコールを発信する場合、ユーザは、クラスタ A からクラスタ B の電話機にコールを発信しているものとして、適切なパターンをダイヤルする必要があります。このことは、ホーム クラスタはクラスタ A からクラスタ B へのクラスタ間トランク コールを開始できますが、メディアは Visiting 電話機とリモート電話機間をローカルに流れることを意味します。

EMCC クラスタを +E.164 の番号指定を使用して配置する場合、ユーザはすでに相手の電話番号の完全な番号をダイヤルすることに慣れているので、ダイヤリング手順を変更する必要はありません。

ルーティングされた公衆網コールでは、コール処理動作に影響する次の 2 つの異なる設定があります。

- Local Route Group（LRG; ローカル ルート グループ）機能を使用しないルート パターン
- LRG 機能を使用するルート パターン

EMCC ログイン ユーザが公衆網コールをダイヤルすると、番号分析が（ルート リストおよびルート グループ コンストラクトを通じて、または音声ゲートウェイ宛に直接設定されて）最終的に音声ゲートウェイにつながるルート パターンと一致した場合、コールはゲートウェイに送信されます。Standard Local Route Group（Standard LRG; 標準ローカル ルート グループ）機能が使用されていない場合、

コールはホーム クラスタに関連付けられた音声ゲートウェイを介します。したがって、メディアは Visiting 電話機から（通常は WAN を介して）音声ゲートウェイへ流れます。ルート パターンが、標準 LRG を使用するように設定されたルート リストにつながる場合、動作は変わります（LRG の詳細については、「ローカル ルート グループ」（P.9-92）を参照してください）。Unified CM のロジックは、EMCC ログイン デバイスについて標準 LRG を呼び出す必要がある場合、エンドポイントを EMCC デバイスとして認識し、公衆網コールを、指定された EMCC 固有の SIP トランクを介して、この Visiting 電話機が通常登録される Visiting クラスタに送信します。

（注）　EMCC トランク サービス タイプの SIP トランクは、クラスタごとに 1 つだけ必要です。このトランクには宛先情報は設定されていません。その情報は、EMCC リモート クラスタの追加および更新時に動的に収集されます。

Visiting クラスタ内の EMCC SIP トランクでコール Invite が受信されると、Visiting クラスタは再度、トランクの CSS に従って（または、Visiting 電話機の元のデバイス設定の CSS に従って）コールされた番号に対して番号分析を使用し、それに応じてコールをルーティングします。EMCC SIP トランク上の SIP Invite には追加情報が含まれています。つまり、Visiting 電話機のデバイス名です。これにより、Visiting クラスタはデータベース内にある Visiting 電話機の設定済みデバイス CSS を判別できます（必要な場合）。番号分析の結果が、最終的に標準 LRG を指すルート パターンとの一致である場合、Visiting クラスタはこの Visiting 電話機の設定済み標準 LRG を判別できます。Visiting クラスタ内の標準 LRG には一般に、Visiting クラスタに関連付けられた音声ゲートウェイが含まれているため、公衆網コールは、Visiting 電話機に対してローカルな音声ゲートウェイに送信されます。

緊急番号へのコールを考慮すると、LRG と LRG 以外のコール処理動作の違いは重要です。Local Route Group（LRG; ローカル ルート グループ）の使用は、EMCC 配置の場合、クラスタ全体には必要ありませんが、EMCC ログイン電話機は、緊急コールを正しくルーティングするために LRG にアクセスする必要があります。Visiting 電話機に対して、ローカルである適切な音声ゲートウェイ経由でコールを発信できるように、緊急コールを Visiting クラスタに正しくルーティングするには LRG が必要です。EMCC デバイス用ローミング デバイス プール設定内の付加コーリング サーチ スペースにより、管理者は緊急ルート パターンを追加できます。緊急ルート パターンは、EMCC ログイン デバイスの LRG を使用しますが、ホーム クラスタ内の他のデバイスの緊急ダイヤリングに影響しません。前述したように、EMCC ログイン電話機は、（ジオロケーションにより）別のクラスタのすべての電話デバイスを示すデバイス プールに関連付けられます。デバイス プールの付加コーリング サーチ スペースでは、EMCC ログイン電話機の緊急コールだけを LRG 経由で送信するように、Visiting クラスタの緊急ルート パターンを設定できます。したがって、ホーム クラスタおよび Visiting クラスタが同じ緊急ルート パターンを使用している場合でも、EMCC ログイン 電話機の緊急コールは、LRG 経由で Visiting クラスタにルーティングします。EMCC SIP トランク経由で Visiting クラスタでコールが受信されると、Visiting クラスタのダイヤル プランがコールのその後の処理を行います。

（注）　EMCC をサポートするクラスタが緊急コール処理に Cisco Emergency Responder も使用している場合、その配置をサポートするダイヤル プランの設定方法の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』を参照してください。
http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

（注）　標準 LRG が緊急ルート パターン用にすでに配置されており、ホーム クラスタと Visiting クラスタが同じ緊急ダイヤル ストリングを使用する場合、付加 CSS を使用する必要はありません。

詳細な EMCC コール処理の例と設定については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Features and Services Guide*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

メディア リソース

RSVP Agent を除くすべてのメディア リソースは、Visiting 電話機に割り当てられたデバイス プールのメディア リソース グループ リストに従って、ホーム クラスタから割り当てられます。会議、トランスコーディング、および保留音は、すべて通常どおり機能します。違いは、メディアは Visiting 電話機とメディア リソースの間を、（通常は）ホーム クラスタと Visiting クラスタを隔てる WAN を介してストリーミングされることです。EMCC ログイン ユーザが、RSVP Agent を使用する必要があるコールを行うと、Unified CM EMCC ロジックはそれが Visiting 電話機であることを判別でき、EMCC SIP トランクを介してリソース要求を Visiting 電話機が属するリモート クラスタに送信します。Visiting 電話機のデバイス名はこの要求に含まれています。これにより、Visiting クラスタは、通常この Visiting 電話機に割り当てられる RSVP Agent メディア リソースを確認でき、コールでの使用を割り当てることができます。EMCC の RSVP ベースのコール アドミッション制御の詳細については、「クラスタ間のエクステンション モビリティのアーキテクチャおよび考慮事項」（P.11-59）を参照してください。

エクステンション モビリティのセキュリティ

Unified CM 8.*x* では、HTTPS を使用するエクステンション モビリティ セキュア サービス URL を作成できます。これにより、EM のログイン/ログアウトの交換全体が暗号化されます。エクステンション モビリティではセキュア サービス URL を設定することを推奨します。HTTPS をサポートしない電話機が EM 用に配置されている場合は、非セキュア サービス URL も設定する必要があります。セキュア サービス URL と非セキュア サービス URL がサービスに対して存在する場合、HTTPS をサポートする電話機は、デフォルトでセキュア サービス URL を使用します。HTTPS をサポートする電話機の全リストについては、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Security Guide*』で、HTTPS の情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

EM 機能は、要求のソース IP アドレスを検証することによって、EM ログインおよびログアウト要求にオプション レベルのセキュリティを提供します。デフォルトでは、EM はこの要求の検証を実行しません。したがって、EM セキュリティを有効にするには、管理者はクラスタ全体のサービス パラメータ Validate IP Address を true に設定する必要があります。

EM ログインおよびログアウト HTTP 要求を処理する Web プロキシを実装する組織は、Allow Proxy サービス パラメータを true に設定する必要があります。プロキシ サーバは、HTTP 要求を転送している間に、そのホスト名と共に HTTP ヘッダーの via-field をセットします。デバイスと Unified CM の間に複数のプロキシ サーバがある場合で、すべてのサーバで要求が転送される場合は、次に HTTP ヘッダーの via-field にはフォワーディング パスで各プロキシ サーバのホスト名のカンマ区切りリストが必要になります。Allow Proxy サービス パラメータは、true に設定されている場合、Web プロキシを介して受信した EM ログインおよびログアウトが可能です。また、プロキシされた EM 要求はプロキシ サーバのソース IP アドレスを使用する場合、その IP アドレスは IP サービス パラメータの信頼できるリストにも設定する必要があります。

Unified CM 8.*x* での HTTPS サポートおよびデフォルトのセキュリティの導入により、EMCC のクラスタ間相互作用には、クラスタが相互にセキュアに通信できるようにするための特別な手順が必要になります。特に、EMCC に参加するすべてのクラスタは Tomcat（Web）および TFTP セキュリティ証明書を中央の SFTP サーバにエクスポートする必要があり、証明書はすべて結合され、各クラスタは結合された証明書をクラスタ内にインポートする必要があります。EMCC に参加する可能性がある新しいノードがクラスタに追加されるたびに、または既存のノードで証明書が更新された場合は、エクスポー

ト、結合、およびインポートというプロセスを繰り返す必要があることに留意することが重要です。これらの手順はすべて、Unified CM Serviceability の管理によって簡素化されています。EMCC の設定の詳細については、次の Web サイトで入手可能な最新バージョンの『*Cisco Unified Communications Manager Features and Services Guide*』で、クラスタ間のエクステンション モビリティの情報を参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

エクステンション モビリティのハイ アベイラビリティ

図 19-4 に示す EM アーキテクチャに従って、Cisco Unified CM データベースの読み取りおよび書き込みが要求されます。EM はユーザに面した機能であって、データベースの書き込みは、EM がサブスクライバ ノードで実行できるかどうかに関係します。したがって、Unified CM パブリッシャが利用できない場合、その場合でも EM ログインおよびログアウトはできます。

冗長性の見地から、次のコンポーネント レベルの冗長性については、全面的な EM の復元性を得るよう検討する必要があります。

- Cisco CallManager Cisco IP Phone Services

  CallManager Cisco IP Phone Services のハイ アベイラビリティは、Services Provisioning サービス パラメータの使用、または Cisco CallManager Cisco IP Phone Services を実行する複数の Unified CM ノードを指す SLB デバイスの使用により実現されます。詳細については、「IP Phone Service のハイ アベイラビリティ」（P.19-6）を参照してください。

- Cisco エクステンション モビリティ サービス

  Cisco エクステンション モビリティ サービスのハイ アベイラビリティは、Cisco エクステンション モビリティ サービスを複数の Unified CM ノードでアクティブにすることにより実現されます。

（注）　Cisco エクステンション モビリティ サービスは、3 つ以上のノードでアクティブにできますが、最大 2 つのノードが、ログイン/ログアウト要求を常にアクティブに処理できます。Cisco エクステンション モビリティ サービスを実行している他のノードは、障害が発生した場合にのみログイン/ログアウト要求の処理を開始する必要があります。

2 つの Unified CM ノード間の要求をロード バランシングしたり、冗長性を提供したりするため、Cisco Application Control Engine（ACE）などのサーバ ロード バランサ デバイスの導入を推奨します。サーバ ロード バランサがない場合、ロード バランシングは均等でなく、冗長性には手動で対応します。たとえば、2 つの EM IP Phone サービスをそれぞれの電話機で設定できます。1 つの Unified CM ノードが到達不能の場合、エンド ユーザはもう一方のノードに到達するために、もう一方の EM IP Phone サービスを手動で選択する必要があります。

（注）　EM IP Phone サービスに冗長性を提供することは、EM IP Phone サービスのリストからサービスを手動で選択する作業をエンド ユーザに任せることで可能になりますが、この方法の場合、ハイ アベイラビリティの実現が困難になる可能性があります。ユーザが電話サービス メニュー（または割り当てられた機能キー）から選択可能になる EM IP Phone サービスを制御できないため、EM ログイン/ログアウト要求を処理する Unified CM ノード間で、EM ログイン/ログアウトのロード バランシングを確実にする方法はありません。さらに、EM サービスの応答に遅延が発生した場合のエンド ユーザの行動は、障害シナリオではよくある行動ですが、EM サービス コールをキャンセルして代替 EM IP Phone サービスを選択するというもので、たいていの場合は状況を悪化させます。これは、ネットワークのみならず、EM ログイン/ログアウト要求を処理する残りの Unified CM ノードでの輻輳および負荷の増大につながる場合があります。

Cisco エクステンション モビリティ サービスを実行する 2 つの Unified CM ノードを使用した配置は、1 分あたりのログイン/ログアウト要求の数に関して最高のキャパシティを提供します（詳細については、「エクステンション モビリティのキャパシティ プランニング」（P.19-17）を参照してください）。この配置は、冗長性も提供します。ただし、障害が発生した場合は、1 つのノードしか残っていないので、ログイン/ログアウト要求のキャパシティは減少します。したがって、最高のログイン/ログアウトのキャパシティを実現して、このキャパシティを障害発生時にも維持するには、Cisco エクステンション モビリティ サービスを追加の Unified CM ノードでアクティブにする必要があります。アクティブなノード間で均等にロード バランシングするには、また、2 つのノードだけでのログイン/ログアウト要求処理を常に確保するには、Cisco Application Control Engine（ACE）などのサーバ ロード バランサ デバイスを配置する必要があります。Cisco Application Control Engine には、プライマリ サーバがダウンしているかどうかを検出し、障害が発生した場合にバックアップ サーバに要求の送信を開始する機能があります。Cisco Application Control Engine（ACE）の設定の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6906/tsd_products_support_model_home.html

（注）　複数の IP リストを持つ DNS A レコードまたは SRV レコードを使用した冗長な設計は推奨できません。DNS 要求に対して複数の IP アドレスが戻ると、電話はタイムアウトを待ってから次にリストされた IP アドレスを試します。ほとんどの場合は、この動作よりエンド ユーザにとって許容できない遅延が発生します。また、このために Cisco エクステンション モビリティ アプリケーション サービスが有効である 3 つ以上のサブスクライバ ノードによってログイン/ログアウト要求が処理される場合がありますが、そのような処理はサポートされていません。

EMCC では、管理者により、リモート クラスタで EM サービスを実行している Unified CM サブスクライバ ノードの 1 つの FQDN または IP アドレスを指定し、Unified CM Web 管理画面を経由してリモート クラスタが追加されます。2 つのクラスタ間の EM サービスは、Unified CM バージョンに関する情報、EMCC EM サービス通信の EM サービス ノードの順序付きのリスト、リモート クラスタで使用可能な EMCC SIP トランク サービス（公衆網アクセスまたは RSVP Agent、あるいはその両方）、および各 EMCC サービスの EMCC SIP トランク操作を処理する最大 3 つのリモート Unified CM ノードの順序付きのリストを提供します。HTTPS 経由の EMCC EM サービス通信には、ユーザのホーム クラスタの検索、EMCC ログイン時の情報交換、およびリモート クラスタ更新が含まれます。最初の更新で、リモート クラスタの エクステンション モビリティ アプリケーション サービスが照会され、そのリスト内の最初の 3 つの EM サービス ノードが返されます。この順序付きのリストによって、EMCC 通信に使用されるリモート クラスタ EM サービス ノードが決まります。

リモート クラスタは、EMCC の公衆網アクセス サービスおよび RSVP Agent サービスのプライマリ、セカンダリ、および 3 次オプションに関する情報を、それらのサービスの割り当て済み EMCC SIP トランクのデバイス プールに関連付けられた Unified CM Group から取得します。これにより、EMCC SIP トランクを処理するプライマリ Unified CM サブスクライバがオフラインの場合、EMCC SIP トランク コールはセカンダリ Unified CM サブスクライバなどによって処理されます。

電話機に EMCC 経由でログインすると、割り当て済み EMCC デバイス プール内に設定された Unified CM Group の形式で、電話機に冗長性が提供されます。Visiting 電話機がリモート サイトに設置されており、Visiting クラスタおよびホーム クラスタの両方が到達不能になる WAN 障害があった場合、Visiting クラスタの SRST リファレンスは、EMCC 電話機により維持されます。そのため、EMCC ログイン電話機は、設置されたサイト内の適切な SRST ルータに登録可能になっています。EMCC ログイン ユーザの DID は、この SRST サイトにあるローカル ゲートウェイに関連付けられることはほとんどないため、着信コールはユーザのホーム クラスタ上のコール転送ルールに基づいてルーティングされることになります。SRST モードの間、そのユーザは SRST フェールオーバー登録中に Visiting SRST サイトで設定されたダイヤル手順に適応する必要もあります。ネットワーク障害発生

中の EMCC ログイン電話機の動作のさらなる例は、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の「Cisco Extension Mobility Cross Cluster」のセクションを参照してください。

http://cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

ホーム クラスタへの登録を可能にする EMCC 設定ファイルをダウンロードするために Visiting 電話機が使用する、デフォルトおよびバックアップの Unified CM TFTP サーバを設定することも推奨します。これは、[EMCC Feature Configuration] で設定します。

エクステンション モビリティのキャパシティ プランニング

Cisco EM アプリケーションは、次のクラスタ全体のログインおよびログアウトのキャパシティをサポートしています。

- Cisco MCS 7845-H2/I2 サーバは、1 分あたり最大 250 回の順次ログインまたはログアウト（あるいはその両方）をサポート
- Cisco MCS 7835-H2/I2 サーバは、1 分あたり最大 235 回の順次ログインまたはログアウト（あるいはその両方）をサポート
- Cisco MCS 7825-H2/I2 サーバは、1 分あたり最大 200 回の順次ログインまたはログアウト（あるいはその両方）をサポート

（注）　旧サーバ モデルを配置するとキャパシティが低下します。

Cisco エクステンション モビリティ ログインおよびログアウト機能は、ログイン/ログアウトのクラスタ キャパシティを増加するためにサブスクライバ ノードのペアに分散できます。SLB デバイスを使用できます。または、手動で EM 負荷を 2 つのサブスクライバ ノード間で均等に分散するには、サブスクライバ ノードの 1 つを指している EM 電話サービスに加入している 1 つの電話機グループと、2 番めのサブスクライバ ノードを指している別の EM 電話サービスに加入している別の電話機グループの、2 つのグループに電話機を分割する必要があります。EM 負荷がこの方法で分散され、2 つの MCS 7845-H2/I2 サーバの間で均等な場合、1 分あたりのクラスタ全体のキャパシティは最大で 375 回の順次ログインまたはログアウト（あるいはその両方）になります。

（注）　Cisco エクステンション モビリティ サービスは、冗長性を目的として 3 つ以上のノードでアクティブにできますが、最大 2 つのサブスクライバ ノードによるログイン/ログアウトのアクティブな処理を常にサポートしています。

（注）　EM セキュリティの有効化はパフォーマンスを低下しません。

EMCC ログイン/ログアウト処理は、クラスタ内 EM ログイン/ログアウトよりも多くの処理リソースを必要とします。したがって、サポートされるログイン/ログアウトの最大レートは低くなります。クラスタ内 EM ログイン/ログアウトがない場合、Unified CM 8.*x* は、Cisco MCS 7845-H2/I2 および MCS 7845-I3 サーバで 1 分あたり 75 回の EMCC ログイン/ログアウトという最大レートをサポートします。ほとんどの配置では、クラスタ内ログイン/ログアウトとクラスタ間ログイン/ログアウトの組み合せが発生します。より一般的なこのシナリオでは、EMCC ログイン/ログアウトの混合（ホーム クラスタまたは Visiting クラスタのどちらとして機能する場合でも）は、1 分あたり 40 回のモデルにする必要があります。同時にクラスタ内 EM ログインは、シングル EM ログイン サーバを使用する場

合、185 回のログイン/ログアウトのモデルにする必要があります。クラスタ内 EM ログイン レートは、デュアル EM サービス設定で MCS 7845-H2/I2 または MCS 7845-I3 サーバを使用する場合、1 分あたり 280 回のログイン/ログアウトまで増大できます（表 19-2 を参照）。

表 19-2　クラスタ内ログイン/ログアウトおよびクラスタ間ログイン/ログアウトの最大数

ログイン/ログアウトのタイプ	シングル EM ログイン サーバ（I2/H2）	デュアル EM ログイン サーバ（I2/H2）
クラスタ内のみ	250	375
クラスタ間のみ	75	90
クラスタ間およびクラスタ内	225（40 EMCC および 185 EM）	320（40 EMCC および 280 EM）

EMCC ログイン デバイス（Visiting 電話機）は、クラスタ内の他のエンドポイントの 2 倍のリソースを消費します。EMCC ログイン デバイスの最大サポート数はクラスタあたり 2,500 台ですが、これによっても、クラスタあたりの他のデバイスの理論的な最大数は 30,000 から 25,000 に減少します。クラスタ内の他の登録デバイス数を削減しても、EMCC ログイン デバイスの最大サポート数は 2,500 台のままです。

クラスタに追加できる EMCC リモート クラスタ数に技術的な制限はありません。ただし、リモート クラスタ数が増えると、フルメッシュ要件によって EM サービスの負荷は増大します。サイト数が多い（10 を超える）場合、Cisco Real Time Monitoring Tool（RTMT）を使用して EM の CPU をモニタする必要があります。

エクステンション モビリティの設計上の考慮事項

次のガイドラインと制限は、Cisco Unified CM テレフォニー環境内の EM の配置と動作に関連して適用されます。

- EM ユーザは、Automated Alternate Routing（AAR）または Voice over PSTN（VoPSTN）、あるいはその両方の配置モデルが使用されている場合、クラスタ内のロケーションまたはサイト間で移動できません。

  EM 機能は、コール ルーティングを IP ネットワークの使用に依存します。E.164 公衆網番号は静的で、公衆網はホーム サイトからの EM ユーザのディレクトリ番号（DN）の移動を考慮に入れられないため、公衆網を通じたコール ルーティングにはより多くの問題が伴います。AAR は、VoPSTN 配置モデルと同様に、コール ルーティングを公衆網に依存します。いずれの場合も、ロケーションおよびサイト間の EM ユーザの移動は、ユーザの移動するすべてのサイトが同じ AAR グループに属する場合にだけサポートされます。詳細については、「エクステンション モビリティ」（P.9-110）を参照してください。

- Cisco エクステンション モビリティ サービスまたはこのサービスを実行中のノードの再起動は、自動ログアウト設定に影響を与えます。

  Cisco エクステンション モビリティ サービスを停止するまたは再起動する場合、システムは最大ログイン間隔が経過後のすでにログインしているユーザを自動ログアウトしません。これらの電話機は、手動でログアウトするか、毎日のデータベース クリーンアップ処理が実行されるのを待つ必要があります（通常は深夜）。

WebDialer では、エクステンション モビリティを使用してログインされた電話機だけを使用できます。詳細については、「WebDialer」（P.19-35）を参照してください。

クラスタ間のエクステンション モビリティ（EMCC）の設計上の考慮事項

EMCC を配置する場合、次の設計上の考慮事項が適用されます。

一般的な設計上の考慮事項

- EMCC では、企業内のすべてのクラスタにわたってユーザは一意である必要があります。LDAP 同期によって複数のクラスタの共通ユーザが保守されている場合は、ある種のフィルタリングを適用する必要があります。
- 使用を計画している機能との組み合せで、クラスタ間のネットワーク遅延を考慮します。Visiting 電話機がホーム クラスタに登録されると、機能は動作します。ただし、特定の配置のネットワーク遅延によっては、すべてのアプリケーションおよび機能がユーザ要件を満たすとはかぎりません。特定のネットワークに対して機能の操作性を判断するためにテストが必要な場合があります。

  たとえば、EMCC は Visiting 電話機の動的 CTI 制御をサポートします。ただし、アプリケーションを介してオフフックが発行され、電話機がオフフックになるまでに 1 秒かかる場合、内勤者はこれを許容できてもコール センター エージェントは許容できない場合があります。
- ログイン プロセス中に電話機ロード ファームウェアは強制されません。代わりに、クロス登録によって新しい電話機ファームウェアがダウンロードされないように、Visiting クラスタの電話機ロード情報が保守されます。
- ホーム クラスタのロケールが Visiting クラスタのロケールと異なる場合、電話機は Visiting クラスタの TFTP サーバから新しいロケールをダウンロードします。そのロケールを使用できない場合、電話機はロケールを変更せず、Visiting クラスタのロケールを保守します。
- 登録された Visiting 電話機に対してホーム クラスタで DLU は消費されません。
- EMCC ログインの合計数は、Bulk Administration Tool（BAT）の EMCC 挿入デバイスの合計数によって制御されます。
- EMCC は、非セキュア クラスタおよび混合モード クラスタをサポートします。ただし、参加するすべての EMCC クラスタは同じモードである必要があり、非セキュア電話機だけが EMCC 登録に対してサポートされます。
- EMCC は、RSVP ベースのコール アドミッション制御だけをサポートします。Unified CM のロケーションベースのコール アドミッション制御はサポートされません。
- RSVP Agent を除き、その他のすべてのメディア リソースは、EMCC ローミング デバイス プールに関連付けられたメディア リソース グループ リストに従って、ホーム クラスタから割り当てられます。
- オーディオおよびビデオ コーデックは、EMCC リージョン設定によって決まります。これらの設定は、EMCC 登録電話機の通常のリージョン設定よりも優先されます。すべての EMCC リージョン パラメータは、すべてのクラスタで同じ値を使用して設定する必要があります。異なる場合、そのクラスタの RSVP Agent は、リモート クラスタ更新操作によって使用不可になります。
- EMCC ローミング デバイス プールを正しく割り当てるには、EMCC 対応電話機に、デバイス設定またはデバイス プール経由で設定されたジオロケーションが必要です。

コール処理の設計上の考慮事項

- ユーザのディレクトリ番号の着信コールは常にホーム クラスタの音声ゲートウェイで受信されるため、着信コールでは RTP メディアは Visiting 電話機とホーム ゲートウェイ間を流れます。
- EMCC SIP トランクを介して送信されるコールは、ホーム クラスタの番号操作を通過します。コールされる番号には、Visiting クラスタのルート パターンと一致するために操作が必要な場合があります。

- ホーム クラスタの H.323 および SIP ゲートウェイの設定済みコーデック能力を確認します。たとえば、ホーム クラスタのゲートウェイが G.711 コールだけを受け入れるように設定されており、EMCC リージョンの帯域幅が 8 kbps（G.729）に設定されている場合、コールを完了するにはトランスコーダが必要です。あるいは、G.711 以外に G.729 を許可するように、H.323 または SIP ゲートウェイ ダイヤル ピアを設定できます。
- EMCC 緊急コールの発信側について、設計上の考慮事項を作成する必要があります。ダイヤル プラン設定によっては、Visiting クラスタのゲートウェイからの発番号は、通常はホーム クラスタに関連付けられる、ユーザの DID である場合があります。このことにより、EMCC SIP トランクまたはルート パターンで着信する、または Visiting ゲートウェイで発信する発信番号を変換する必要があります。
- EMCC が Cisco Emergency Responder とともに配置される場合、Emergency Responder は、1 つの Emergency Responder クラスタによって処理されるすべてのクラスタに配置される必要があります。Visiting クラスタが Emergency Responder とともに配置され、ホーム クラスタは Emergency Responder とともに配置されない場合、コールが Visiting クラスタに戻ったときに Emergency Responder は Visiting 電話機を識別できません。

Unified CM Assistant

Cisco Unified CM Assistant は、Unified CM に統合されたアプリケーションです。これを使用すると、1 人または複数のマネージャに代わってアシスタントが着信コールを処理できます。Unified CM Assistant Console デスクトップ アプリケーションまたは Unified CM Assistant Console 電話サービスをアシスタントの電話機で使用すると、アシスタントが手早くマネージャの状態を確認し、コールをどうするかを決定できます。自分の電話機のソフトキーおよびサービス メニューを使用するか、または PC インターフェイスを介してキーボード ショートカット、ドロップダウン メニューを使用するか、あるいはマネージャのプロキシ回線へのコールのドラッグ アンド ドロップすることによって、アシスタントはコールを処理できます。

ここでは、Unified CM Assistant 機能の設計について次の項目を説明します。

- 「Unified CM Assistant のアーキテクチャ」（P.19-20）
- 「Unified CM Assistant のハイ アベイラビリティ」（P.19-24）
- 「Unified CM Assistant のキャパシティ プランニング」（P.19-27）
- 「Unified CM Assistant の設計上の考慮事項」（P.19-29）
- 「Unified CM Assistant Console」（P.19-33）

Unified CM Assistant のアーキテクチャ

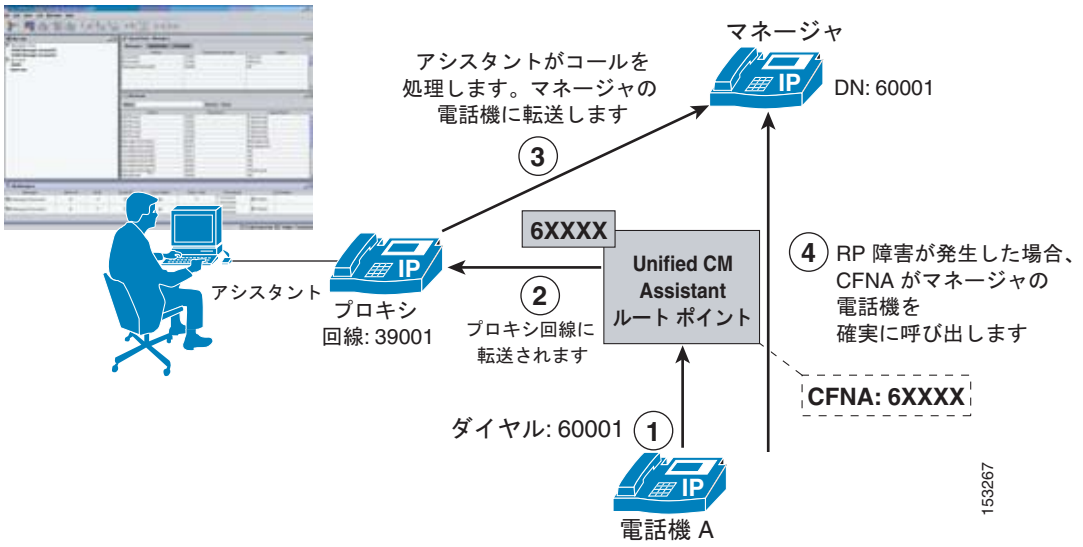
Unified CM Assistant アプリケーションは、プロキシ回線モードとシェアド ライン モードの 2 つのモードで動作できます。各モードの動作と機能は異なり、それぞれに長所と短所があります。どちらのモードも、1 つのクラスタ内で設定できます。ただし、同一のアシスタントでモードを混合させることはできません。1 人以上のマネージャにサポートを提供している 1 人のアシスタントは、シェアド ライン モードまたはプロキシ回線モードのいずれかでこれらのマネージャをサポートできます。

Unified CM Assistant のプロキシ回線モード

図 19-7 は、プロキシ回線モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、ディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。CTI/Unified CM Assistant Route Point（RP）は、6XXXX に設定された DN に基づいてこの

コールを代行受信します。次に、マネージャの DN に基づいて、コールはルート ポイントにより、アシスタントの電話機上のマネージャのプロキシ回線（DN：39001）に転送されます（ステップ 2）。次に、アシスタントはコールに応答または処理し、必要に応じてマネージャの電話機にコールを転送します（ステップ 3）。Unified CM Assistant アプリケーションの障害、または Unified CM Assistant RP の障害が発生した場合に、マネージャの DN へのコールがマネージャの電話機を直接呼び出すよう、RP の Call Forward No Answer（CFNA）の 6XXXX 設定による呼び出しメカニズムが存在します（ステップ 4）。

図 19-7　Unified CM Assistant のプロキシ回線モード

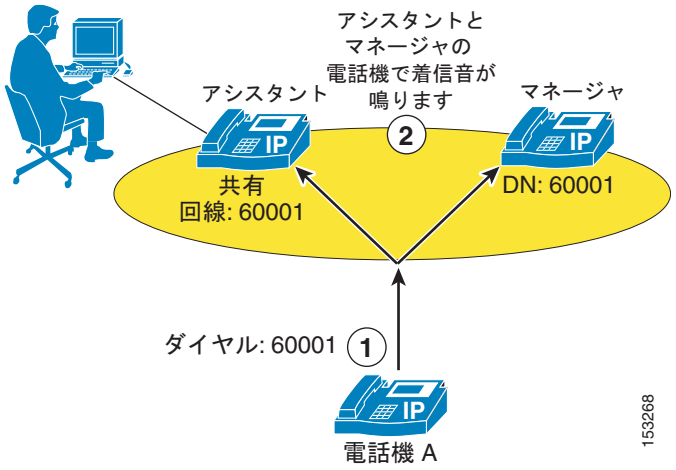


（注）　図 19-7 に示す CFNA による呼び出しメカニズムでは、Unified CM Assistant RP のディレクトリ番号設定ページの [Forward No Answer Internal] フィールドと [Forward No Answer External] フィールドの両方で、Unified CM Assistant RP ディレクトリ番号と同じ集約番号桁の設定が必要です。また、これらの各コール転送パラメータの Calling Search Space（CSS; コーリング サーチ スペース）フィールドは、Unified CM Assistant RP または Unified CM Assistant アプリケーションに障害が発生した場合にマネージャの電話機の DN に到達できるように、マネージャの電話機の DN が設定されたパーティションを含むコーリング サーチ スペースで設定する必要があります。

Unified CM Assistant のシェアド ライン モード

図 19-8 は、シェアド ライン モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、アシスタントの電話機のシェアド ラインであるディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。このコールは、アシスタントとマネージャの電話機の両方で着信音を鳴らします。ただし、マネージャが Do Not Disturb（DND）機能を呼び出した場合、着信音が鳴るのはアシスタントの電話機だけになります（ステップ 2）。

図 19-8　Unified CM Assistant のシェアド ライン モード



Unified CM Assistant のシェアド ライン モードでは、マネージャの電話機へのコールを代行受信するために Unified CM Assistant RP は必要ありません。ただし、マネージャの電話機および Unified CM Assistant Console デスクトップ アプリケーションの Do Not Disturb（DND）機能は、Cisco IP Manager Assistant および Cisco CTIManager サービスに依存します。さらに、Unified CM Assistant シェアド ライン モードでは、コール フィルタリング、コール代行受信、アシスタント選択、Assistant Watch などの機能は使用できません。

Unified CM Assistant のアーキテクチャ

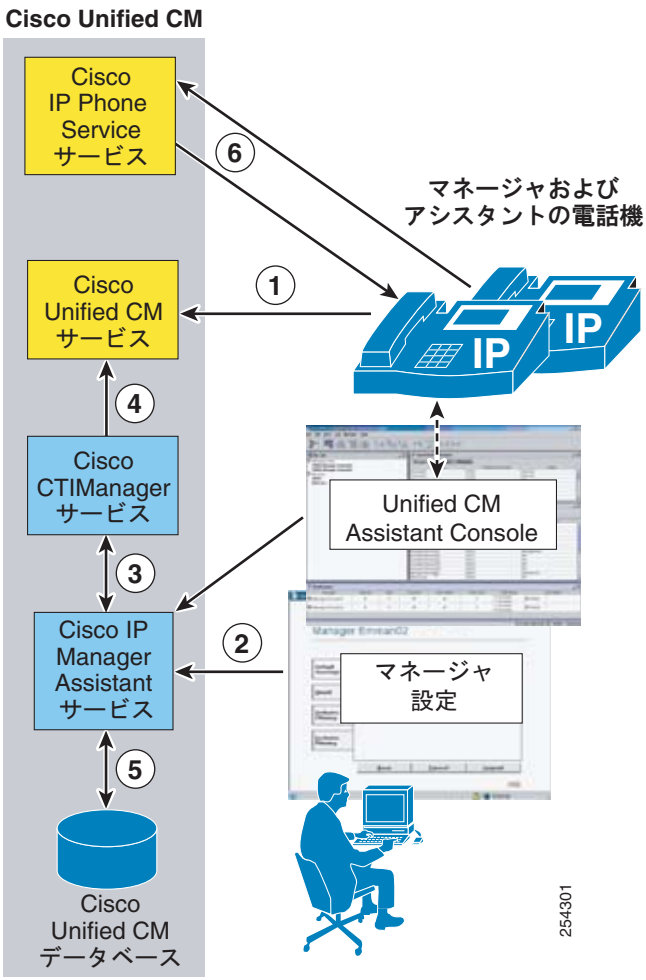
Unified CM Assistant アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 19-9 は、Unified CM Assistant のメッセージ フローとアーキテクチャを示しています。Unified CM Assistant のマネージャおよびアシスタント ユーザに対して Unified CM Assistant を設定すると、次の一連の対話とイベントが発生します。

1. マネージャとアシスタントの電話機は Cisco Unified CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 19-9 のステップ 1 を参照）。
2. Unified CM Assistant Console デスクトップ アプリケーションと Manager Configuration Web ベース アプリケーションは、どちらも Cisco IP Manager Assistant サービスと通信およびインターフェイスします（図 19-9 のステップ 2 を参照）。
3. 次に、Cisco IP Manager Assistant サービスは、回線モニタリング情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 19-9 のステップ 3 を参照）。
4. CTIManager サービスは、Unified CM Assistant 電話制御情報を Cisco CallManager Service に渡し、さらに Unified CM Assistant RP をも制御します（図 19-9 のステップ 4 を参照）。
5. それと並行して、Cisco IP Manager Assistant サービスは、Unified CM データベースとの間で、Unified CM Assistant アプリケーション情報の読み取りと書き込みを行います（図 19-9 のステップ 5 を参照）。
6. マネージャは、Services ボタンを押すことにより、Unified CM Assistant 電話サービスを呼び出して、その電話機が加入している（Unified CM Assistant 電話サービスを含む）すべてのサービスのリストを返す IP Phone Service サービスへのコールを生成できます（図 19-9 のステップ 6 を参照）。

Unified CM Assistant 電話サービスは Cisco IP Manager Assistant サービスで制御され、電話機を使用してマネージャによって加えられた設定の変更は、Cisco IP Manager Assistant サービスを通じて処理および伝達されます。

（注）　Services Provisioning エンタープライズ パラメータが内部に設定されている場合、ステップ 1 および 2 はバイパスされます。一方、Services Provisioning が外部 URL または両方に設定されている場合、ユーザが回線ボタンまたはスピード ダイヤル ボタンを押して、Cisco IP Manager Assistant サービスへの直接コールを生成できるように、Service URL ボタンはユーザの電話機で Unified CM Assistant 電話サービスの設定ができます。ステップ 1 および 2 もバイパスされます。

図 19-9　Unified CM Assistant のアーキテクチャ



（注）　図 19-9 は、同じノードですべてが実行されている IP Phone Service、Cisco CallManager、CTIManager、および Cisco IP Manager Assistant サービスを示していますが、この設定は必須ではありません。これらのサービスではクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Unified CM Assistant のハイ アベイラビリティ

Unified CM Assistant アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、Unified CM Assistant サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、アシスタントとマネージャの電話機、Unified CM Assistant ルート ポイント、Unified CM Assistant Console デスクトップ アプリケーション、および電話サービス に関連して検討し、さらにアシスタントとマネージャの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 19-9 に示すように、Unified CM Assistant 機能は、主に Cisco IP Manager Assistant サービスおよび Cisco CTIManager サービスに依存します。いずれの場合も、冗長性はプライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Unified CM Assistant サーバ（Cisco IP Manager サービスを実行しているノード）のアクティブおよびバックアップのペアは最大で 3 個まで定義できます。つまり、単一クラスタ内で合計 6 つの Unified CM Assistant サーバになります。アクティブおよびバックアップ Unified CM Assistant サーバ ペアは Cisco IPMA Server IP Address、Pool 2、Cisco IPMA Server IP Address、および Pool 3 Cisco IPMA Server IP Address サービス パラメータを使用して設定されます。これらのパラメータを設定することで、必要な Unified IP Assistant サービスに冗長性が与えられます。いずれかのプライマリ Unified CM Assistant に障害が発生した場合、バックアップまたはスタンバイ Unified CM Assistant サーバが Unified CM Assistant サービス要求を処理できます。Unified CM Assistant サーバの各ペアでは、任意の時点でアクティブになり、要求を処理する Unified CM Assistant サーバは 1 つだけです。その別の Unified CM Assistant サーバはスタンバイ状態になり、アクティブなサーバに障害が発生しない限り、要求を処理しません。

また、CTIManager (Primary) IP Address および CTIManager (Backup) IP Address サービス パラメータを使用して、2 つの CTIManager サーバまたはサービスを各 Unified CM Assistant サーバ用に定義できます。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。クラスタ ノードのすべての Unified IP Assistant および CTIManager サービスに障害が発生した場合は、Unified CM Assistant ルート ポイントおよび Unified CM Assistant Console デスクトップ アプリケーションがダウンし、その結果 Unified CM Assistant アプリケーション全体がダウンします。ただし、前にも説明したように、Unified CM Assistant に障害が発生した場合、CFNA による呼び出しメカニズムは引き続き動作し、マネージャへのコールは直接マネージャの電話にルーティングできます。

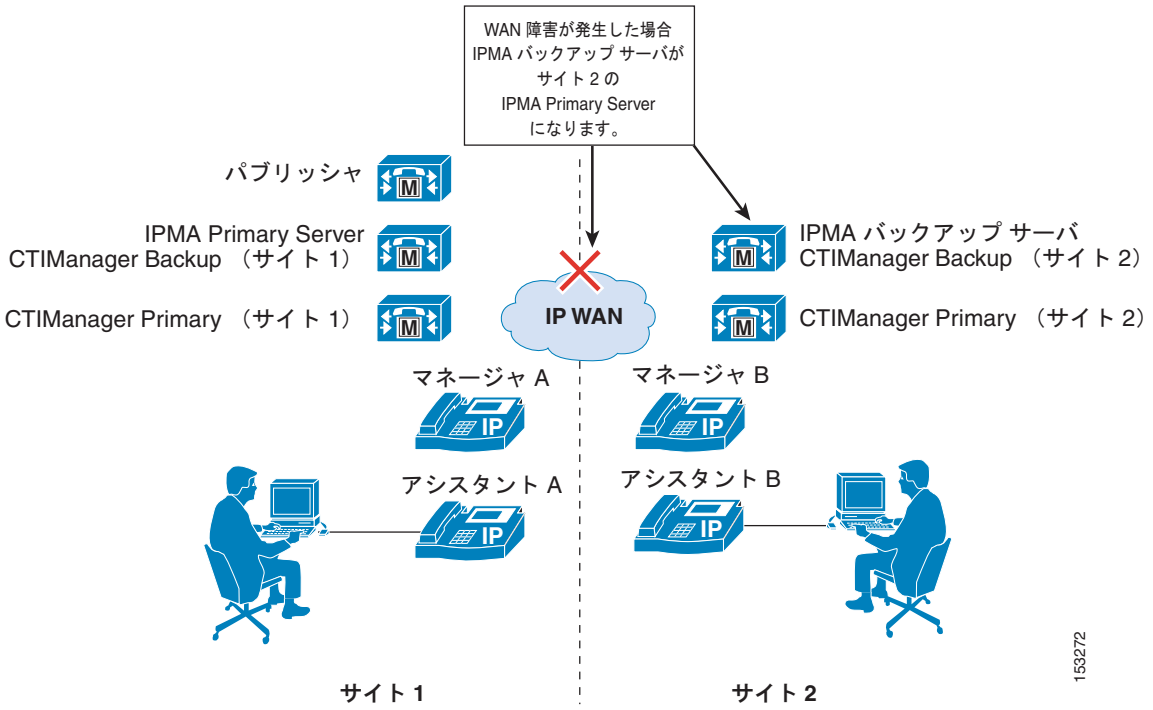
（注）　Unified IP Assistant シェアド ライン モードで設定した場合、Unified CM Assistant および CTIManager サービスが障害によって完全に停止しても、電話機は 1 本の回線を共有し続けるため、アシスタントは引き続きマネージャの代わりにコールを処理できます。ただし、Unified CM Assistant Console デスクトップ アプリケーションと DND の機能は、使用できなくなります。

図 19-10 は、WAN を通じたクラスタリングで、2 サイトの配置による Unified CM Assistant および CTIManager のプライマリ サーバとバックアップ サーバの冗長設定を示しています。最大限の冗長性を実現するため、サイト 1 のノードはプライマリ Unified CM Assistant サーバとして設定し、サイト 2 のノードはバックアップ Unified CM Assistant サーバとして設定します。WAN に障害が発生した場合、既存のプライマリ Unified CM Assistant サーバはサイト 2 から到達できなくなるため、サイト 2

のバックアップ Unified CM Assistant サーバがプライマリ Unified CM Assistant サーバになります。このように、Unified CM Assistant サーバは、WAN 障害を前提として、クラスタオーバー WAN 環境で冗長にできます。さらに、サイト 1 とサイト 2 の両方でプライマリおよびバックアップ CTIManager を設定すると、CTIManager は WAN の障害に対する冗長性を持ち、各サイトで CTIManager の障害に対して追加の冗長性が提供されます。

（注）　図 19-10 で説明するシナリオは、特別な状況を示しています。通常の動作時に、Unified CM Assistant サーバの任意ペアを同時にアクティブにすることはできません。Unified CM Assistant サーバのアクティブおよびバックアップ ペアがネットワークを通じて通信できる場合、一方のサーバはバックアップ モードとなり、要求を処理できません。

図 19-10　WAN を通じた 2 サイト クラスタリングによる Unified CM Assistant の冗長性



前に説明したように、パブリッシャは、Unified CM Assistant 情報を Unified CM データベースへ書き込みする時に単一の障害点となります。パブリッシャに障害が発生しても、Unified CM Assistant アプリケーションのすべての部分が引き続き動作します。ただし、Unified CM Assistant アプリケーション設定を変更できなくなります。パブリッシャが回復するまで、Unified CM Assistant Console デスクトップ アプリケーション、Manager Configuration Web ベース アプリケーション、電話機のソフトキー、または Unified CM Assistant 電話サービスを通じて設定を変更できません。この条件には、Do Not Disturb、DivertAll、Assistant Watch、コール フィルタリングなどの機能の有効化や無効化、およびコール フィルタとアシスタント選択設定の変更が含まれます。

デバイスと到達可能性の冗長性

デバイス レベルでの Unified CM Assistant の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、マネージャおよびアシスタントの電話機と Unified CM Assistant RP は、デバイス登録用のデバイス プールと Cisco Unified CM グループ設定の組み合せによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、Unified CM Assistant RP は呼制御機能に関して CTIManager にも依存するため、前の項で説明したプライマリおよびバックアップ CTIManager に依存する必要があります。
Unified CM Assistant Console デスクトップ アプリケーションも、冗長性と機能がコンポーネント サービスに依存します。Assistant Console デスクトップ アプリケーションは、マネージャの着信コールの処理を持続できるように、プライマリ Unified CM Assistant サーバからバックアップ サーバ（およびその反対）への自動フェールオーバーをサポートしています。この自動フェールオーバーに要する時間は、Cisco Unified IPMA Assistant Console Heartbeat Interval および
Cisco Unified IPMA Assistant Console Request Timeout のサービス パラメータを使用して制御できます。ハートビートまたはキープアライブの頻度は、Unified CM Assistant サーバの障害がデスクトップ アプリケーションですばやく検出されるように設定しますが、キープアライブをあまり頻繁に送信することで、ネットワークに悪影響を与えないように注意してください。多数の Assistant Console アプリケーションが使用されている場合、この考慮事項は特に重要です。

Unified CM Assistant Console 電話サービスは、Unified CM Assistant Console デスクトップ アプリケーションとは異なり、プライマリ Unified CM Assistant サーバに障害が発生した場合の冗長性には手動で調整する必要があります。プライマリ Unified CM Assistant サーバがダウンした場合、電話コンソールを使用しているアシスタントにはこの状態の表示が見えません。ただし、アシスタント電話では、ソフトキー を使用するときにメッセージ「Host not found Exception」を受信します。バックアップ Unified CM Assistant サーバで電話コンソールを引き続き使用するには、ユーザは IP Services メニューから再びログインして、セカンダリ Unified CM Assistant 電話サービスを手動で選択する必要があります。

マネージャおよびアシスタントの到達可能性に確実に冗長性を与えるフェールオーバー メカニズムは、他にもいくつかあります。第 1 に、（プロキシ回線モードで）Unified CM Assistant アプリケーションを通じてマネージャのアシスタントに送信されるコールは、設定した時間の経過後にそのコールへの応答がない場合、次の応答可能なマネージャのアシスタントに転送します。設定した時間の経過後に次のアシスタントがコールに応答しない場合、そのコールは次の応答可能なマネージャのアシスタントに再び転送され、それ以降も同様に転送が続けられます。このメカニズムは、Cisco IPMA RNA Forward Calls および Cisco IPMA RNA Timeout のサービス パラメータを使用して設定します。第 2 に、前述したように、クラスタ ノードのすべての Unified IP Assistant と CTI サービスに障害が発生した場合、Unified CM Assistant RP は使用できなくなります。ただし、Unified CM Assistant RP の CFNA 設定に基づいて、すべてのマネージャの DN に対するコールはマネージャの電話機に直接呼び出され、マネージャの到達可能性に十分な冗長性が与えられます。

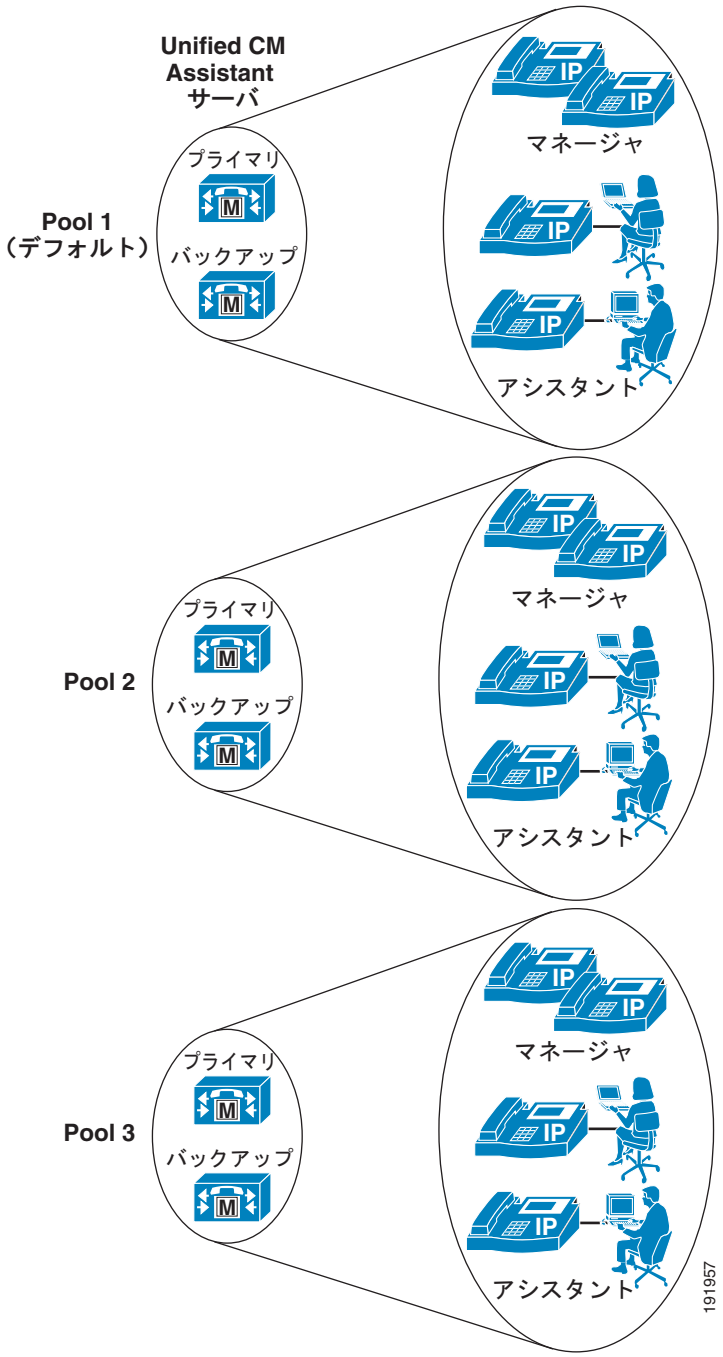
Unified CM Assistant のキャパシティ プランニング

Cisco Unified CM Assistant アプリケーションは、次のキャパシティをサポートしています。

- マネージャあたり最大 10 人のアシスタントを設定できる。
- 1 人のアシスタントに対して最大 33 人のマネージャを設定できる（マネージャ毎に 1 つの Unified CM Assistant 制御回線がある場合）。
- クラスタあたり最大 3500 人のアシスタントと 3500 人のマネージャを、Cisco MCS 7845 を使用して設定できる（合計 7000 人）。
- プライマリおよびバックアップ Unified CM Assistant サーバのペアをクラスタあたり最大 3 組配置できる。ただし、Enable Multiple Active Mode サービス パラメータが True に設定され、Unified CM Assistant サーバ の 2 番めおよび 3 番めのプールが設定されている場合。

Unified CM Assistant 最大でアシスタント 3500 人とマネージャ 3500 人（合計 7000 人）のキャパシティを実現するには、マルチの Unified CM Assistant サーバ プールを定義する必要があります。図 19-11 に示しているように、最大 3 個のプールを設定できます。各プールはプライマリおよびバックアップ Unified CM Assistant サーバおよびマネージャとアシスタントのグループで構成されています。Pool 1 の Unified CM Assistant サーバは Cisco IPMA Server（Primary/Backup）の IP Address サービス パラメータで設定し、Pool 2 のサーバは Pool2 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト パラメータで設定し、および Pool 3 のサーバは Pool3 で Cisco IPMA Server（Primary/Backup）の IP Address アドバンスト パラメータで設定します。

図 19-11　Unified CM Assistant Server Pools 環境下のマルチ アクティブ モード



Cisco Unified CM Assistant アプリケーションは、回線モニタリングおよび電話制御のために CTIManager と対話します。Unified CM Assistant 用のまたはマネージャ電話用の各回線（インターコム回線を含む）が CTI 回線を CTIManager と共に必要になります。また、各 Unified CM Assistant ルート ポイントは、CTI 回線インスタンスが CTIManager と共に必要になります。

Unified CM Assistant を設定する場合、必要な CTI 回線または接続の数について、CTI 回線または接続に対する全体的なクラスタ制限と合わせて考慮する必要があります（クラスタごとの CTI 接続制限

の詳細については、「CTI のキャパシティ プランニング」（P.8-40）を参照してください）。追加の CTI 回線が別のアプリケーションに必要になる場合、これらの CTI 回線によって Unified CM Assistant のキャパシティが制限される場合があります。

Unified CM Assistant の設計上の考慮事項

Unified CM Assistant には、重複および共有内線番号に関して次の制限があり、ディレクトリ番号のプロビジョニングを計画する場合に注意する必要があります。

- プロキシ回線モードの Unified CM Assistant では、アシスタントの電話機のプロキシ回線番号は、異なるパーティション間でも一意にする必要があります。
- プロキシ回線モードの Unified CM Assistant では、2 人のマネージャは異なるパーティション間でも、同じ Unified CM Assistant 制御回線番号（DN）を持つことができません。

Multiple Active Mode を有効にして複数の Unified CM Assistant サーバ プールを使用する場合は、Unified CM Assistant サーバ プールの間でマネージャおよびアシスタントが均等に分散されるようにして、適切なサーバ プール（1 から 3）がエンド ユーザの [Manager Configuration] ページの [Assistant Pool] フィールドで選択されることを確認します。マネージャに連携したアシスタントは、そのマネージャが設定されたプールに自動的に割り当てられます。

Unified CM Assistant は、CTI Manager に対する安全でない接続と安全な接続（トランスポート レイヤ セキュリティ）の両方をサポートします。

Unified CM Assistant のエクステンション モビリティの考慮事項

Unified CM Assistant のマネージャは、Extension Mobility（EM; エクステンション モビリティ）を使用して、プロキシ回線モードとシェアド ライン モードの両方でそれぞれの電話機にログインできます。ただし、そのマネージャは、エンド ユーザ ディレクトリの [Cisco Unified CM Assistant Manager] 設定ページで、Mobile Manager として設定する必要があります。Unified CM Assistant と組み合せて EM を使用する場合、ユーザが EM を使用して複数の電話機にログインできないようにする必要があります。この動作は、EM サービス パラメータの Multiple Login Behavior を使用して有効または無効にできます。クラスタ内で同じユーザによる複数の EM ログインが必要な場合、EM を使用する Unified CM Assistant のマネージャに、複数の電話機にログインしないよう指示する必要があります。マネージャが EM で 2 つの異なる電話機にログインすることを許可すると、2 人のマネージャは異なるパーティション間でも同じ Unified CM Assistant 制御回線番号（DN）を持つことができないという、前述の制限に違反することになります。

（注） Unified CM のアシスタントは、Mobile Assistant の概念がないため、EM を使用してそれぞれの電話機にログインできません。

Unified CM Assistant のダイヤル プランの考慮事項

ダイヤル プラン設定は、プロキシ回線モードで設定される Unified CM Assistant では非常に重要です。マネージャの DN に対するコールが Unified CM Assistant RP で代行受信され、アシスタントの電話機に転送されることを保証するには、Unified CM Assistant RP およびアシスタントの電話機上のマネージャのプロキシ回線を除いて、すべてのデバイスからマネージャの DN に到達できないように、コーリング サーチ スペースおよびパーティションを設定する必要があります。

図 19-12 は、ダイヤル プラン コンポーネント内の各種デバイスのコーリング サーチ スペース、パーティション、および設定に対する最小要件を持つ、プロキシ回線モードの Unified CM Assistant ダイヤル プランの例を示しています。プロキシ回線モードでは 3 個のパーティションが必要です。図 19-12 の例では、次のパーティションになります。

- すべての Unified CM Assistant RP DN を含む Assistant_Route_Point パーティション
- すべてのアシスタントとその他のユーザの電話機 DN を含む Assistant_Everyone パーティション
- すべてのマネージャの電話機の DN を含む Assistant_Manager パーティション

また、2 つのコーリング サーチ スペースが必要です。図 19-12 の例では、次のコーリング サーチ スペースになります。

- Assistant_Route_Point パーティションおよび Assistant_Everyone パーティションを含む ASSISTANT_EVERYONE_CSS コーリング サーチ スペース
- Assistant_Manager パーティションおよび Assistant_Everyone パーティションを含む MANAGER_EVERYONE_CSS コーリング サーチ スペース

これは、この例でのダイヤル プランの範囲です。ただし、コール ルーティングが必要に応じて動作するように、適切なコーリング サーチ スペースでさまざまな電話機および Unified CM Assistant RP DN または回線を適切に設定することも重要です。この場合、すべてのユーザの回線、アシスタントのプライマリ（またはパーソナル）回線、およびマネージャの電話回線は、これらの回線すべてが Assistant_Everyone パーティションおよび Assistant_Route_Point パーティションのすべての DN に到達できるように、ASSISTANT_EVERYONE_CSS コーリング サーチ スペースで設定します。テレフォニー ネットワーク内のデバイスで設定されるインターコムなどの回線は、この同じコーリング サーチ スペースで設定します。すべてのマネージャのプロキシ回線およびすべての Assistant_RP 回線は、これらの回線すべてが Assistant_Manager パーティションのマネージャ DN および Assistant_Everyone パーティションに属するすべての DN に到達できるように、MANAGER_EVERYONE_CSS コーリング サーチ スペースで設定します。この方法により、ダイヤル プランでは、アシスタントの電話機の Assistant_RP 回線およびマネージャのプロキシ回線だけが、マネージャの電話機 DN に直接到達できるように確保します。

図 19-12　Unified CM Assistant のプロキシ回線モードのダイヤル プランの例

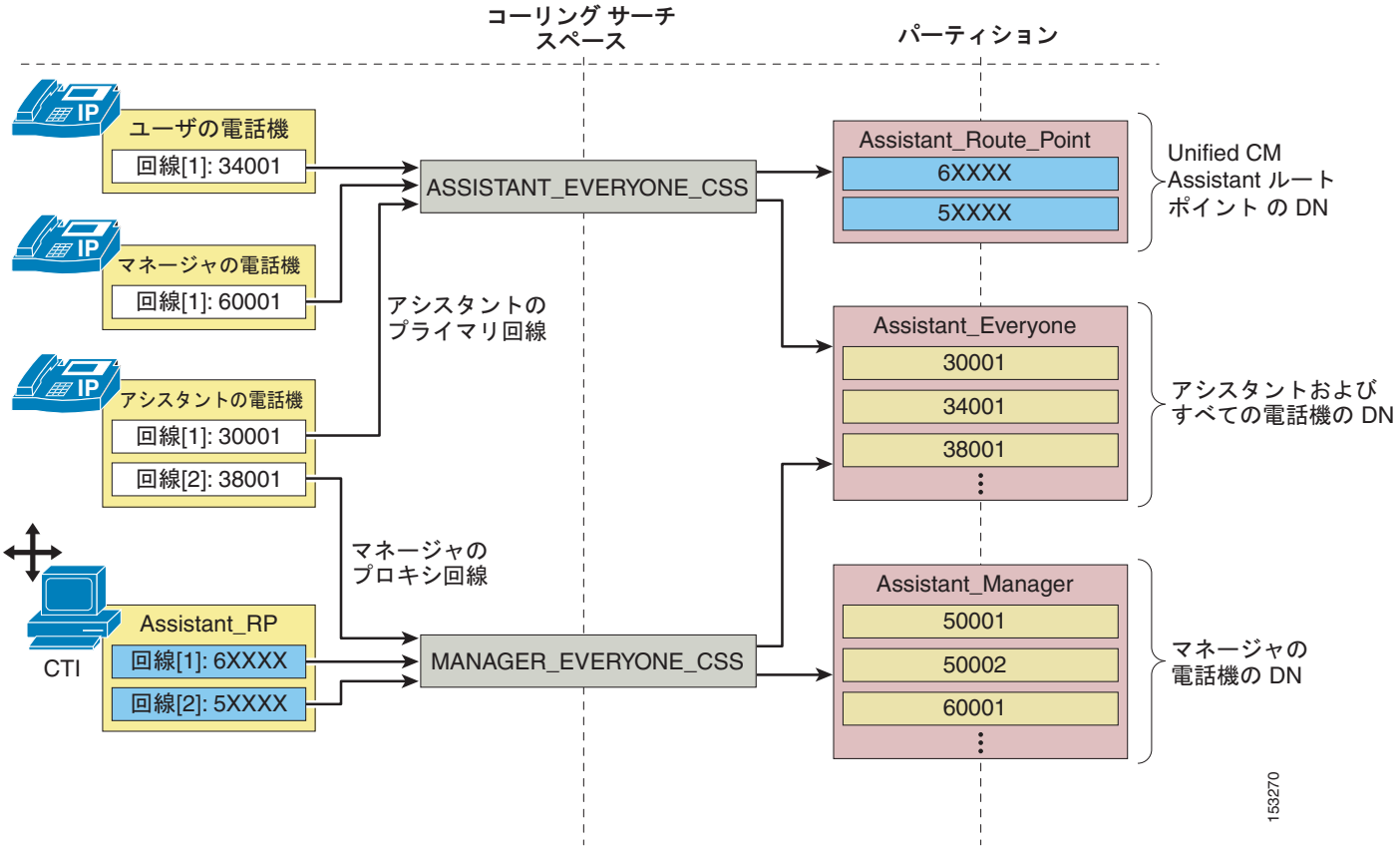


図 19-12 の例では、プロキシ回線モードでの Unified CM Assistant に関するダイヤル プランの最小要件を示しています。ただし、実際のテレフォニー ネットワークには、ほとんどの場合、Unified CM Assistant のコーリング サーチ スペースおよびパーティションとの統合が必要な追加または既存のダイヤル プラン要件があります。図 19-13 は、このような統合ダイヤル プランを示しています。この例では、前述したダイヤル プランは、2 つの追加のパーティションと 1 つの追加のコーリング サーチ スペースを処理する必要があります。図 19-13 では On Cluster パーティションが追加され、追加の電話機 DN もいくつか含まれています。On Cluster パーティションは、既存のデバイスがこれらの追加 DN に到達できるように、既存の Unified CM Assistant コーリング サーチ スペースの両方（ASSISTANT_EVERYONE_CSS および MANAGER_EVERYONE_CSS）に追加されています。UNRESTRICTED_CSS コーリング サーチ スペースも、既存のダイヤル プランに追加されています。このコーリング サーチ スペースは Assistant_Route_Point、Assistant_Everyone、および新たに追加した On Cluster パーティションで設定します。また、PSTN という別の新しいパーティションが追加されています。これには、共通ルート リスト（RL）、ルート グループ（RG）、およびボイス ゲートウェイ メカニズムを通じて、公衆網にコールをルーティングするために使用されるルート パターンのセットが含まれています。この PSTN パーティションは、UNRESTRICTED_CSS コーリング サーチ スペースの一部として設定します。

電話機およびデバイス回線のコーリング サーチ スペースの設定は、新しく追加したパーティションおよびコーリング サーチ スペースを組み込むために調整できます。ただし、Assistant_RP およびアシスタントの電話機のマネージャ プロキシ回線は、MANAGER_EVERYONE_CSS コーリング サーチ スペースに割り当てたままにする必要があります。この例で、マネージャには公衆網への無制限アクセス

が与えられる可能性があるため、マネージャの電話回線は、最初に設定された ASSISTANT_EVERYONE_CSS コーリング サーチ スペースから、新しい UNRESTRICTED_CSS に移動されています。

図 19-13　Unified CM Assistant のプロキシ回線モードのダイヤル プラン統合の例

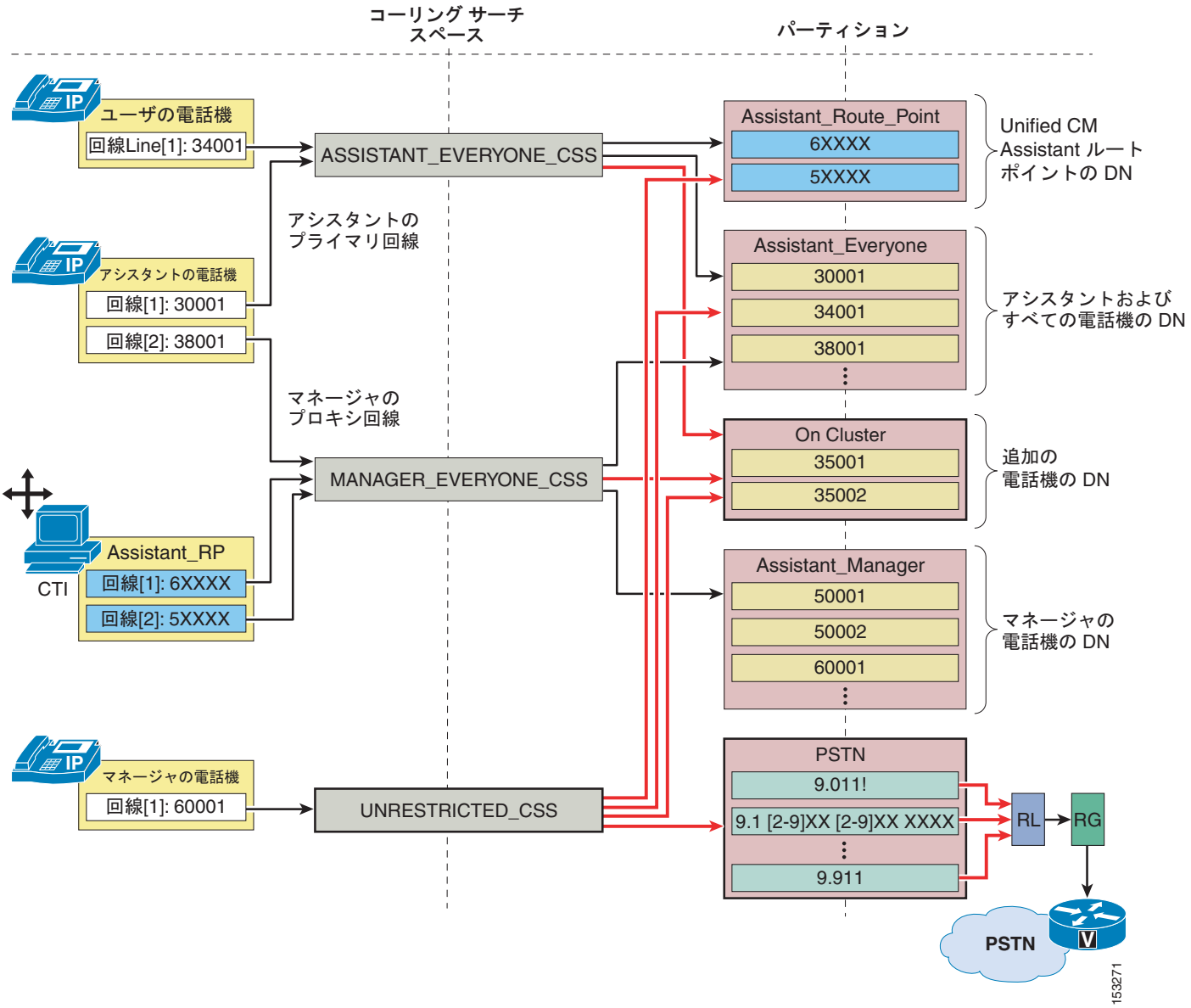


図 19-13 に示すように、追加のパーティションとコーリング サーチ スペースを新規または既存の Unified CM Assistant ダイヤル プランに統合することはできますが、基になるプロキシ回線モードのメカニズムが影響を受けないように注意する必要があります。

Unified CM Assistant シェアド ライン モードでは、特別なダイヤル プランのプロビジョニングは必要ありません。注意の必要な Unified CM Assistant RP またはプロキシ回線が存在しないため、マネージャとアシスタントの電話機は、ネットワーク内の他の電話機と同様にコーリング サーチ スペースお

よびパーティションで設定できます。シェアド ライン モードに関する唯一の要件は、シェアド ラインの機能を実現できるように、マネージャとアシスタントの DN が同じパーティションに属する必要があることです。

Unified CM Assistant Console

Unified CM Assistant Console デスクトップ アプリケーションまたは Unified CM Assistant Console 電話サービスは、アシスタントがマネージャの代わりにコールを処理するために必要です。このデスクトップ アプリケーションは、コールを処理するためのグラフィカル インターフェイスをアシスタントに提供しますが、電話サービスはコールを処理するためのメニュー方式インターフェイスを提供します。デスクトップ アプリケーションと IP 電話サービスの両方では、アシスタントがマネージャの電話機の設定および環境の設定ができて、回線ステータスおよび可用性をモニタできます。また、このデスクトップ アプリケーションは、クリックコール スピード ダイヤルおよびディレクトリ エントリなど別の機能を備えています。この別の機能も従来のソフトキーおよびメニュー アプローチを使用してアシスタントの電話機で行うことができます。

Unified CM Assistant Console のインストール

Unified CM Assistant Console デスクトップ アプリケーションは、次の URL からインストールできます。

https://<*Server_IP-Address*>:8443/plugins/CiscoUnifiedCallManagerAssistantConsole.exe

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

Unified CM Assistant Console 電話サービスは、いかなるインストールも必要がありません。アシスタントの電話機をコンソールとして使用可能にするには、アシスタントの電話機を Unified CM Assistant 電話サービスにサブスクライブします（これは、マネージャの電話機もサブスクライブする必要があることと同じサービスです）。

Unified CM Assistant Console の QoS

インストール後に、マネージャに代わってコールを処理するには、アシスタントがユーザ ID とパスワード（Cisco Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログインし、[Go Online] アイコンまたはメニュー項目をクリックして、ステータスを「online」に切り替える必要があります。ユーザがログインし、オンライン状態になると、デスクトップ アプリケーションは TCP ポート 2912 で Unified CM Assistant サーバと通信します。このアプリケーションは、トラフィックを受信する場合に一時的な TCP ポートを選択します。Cisco Unified CM 上の Unified CM Assistant サーバは、呼制御（コール フローの生成と処理）のためにデスクトップ アプリケーションとインターフェイスするので、TCP ポート 2912 で Cisco Unified CM から受信されたトラフィックは、Cisco Unified CM によって 24 の Differentiated Services Code Point（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。この方法により、Unified CM Assistant 電話制御トラフィックは、その他のすべてのコール シグナリング トラフィックと同様に、ネットワークを通じてキューに入れることができます。

対称的なマーキングとキューを保証するため、Cisco Unified CM の TCP ポート 2912 を宛先とする Unified CM Assistant Console アプリケーション トラフィックも、DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Cisco Unified CM および Unified CM Assistant サーバに向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。Unified CM Assistant Console アプリケーションは、すべてのトラフィックをベストエフォートとしてマーキングします。つまり、スイッチ ポート レベル（または、可能な限りコンソール PC に近いネットワーク パスに沿った場所で）Access Control List（ACL; アクセス コントロール リス

ト）を適用することで、アプリケーション PC から送信され、TCP ポート 2912 の Cisco Unified CM を宛先とするトラフィックを、DSCP 0（PHB Best Effort）から DSCP 24（PHB CS3）に再マーキングする必要があります。

Unified CM Assistant Console のディレクトリ ウィンドウ

Assistant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、アシスタントは Cisco Unified CM Directory エンド ユーザを検索できます。ディレクトリ ウィンドウの [Name] フィールドに入力する検索文字列は、Unified CM Assistant サーバに送信され、Cisco Unified CM データベースに対して検索が直接実行されます。次に、Unified CM Assistant サーバによって、検索照会への応答がデスクトップ アプリケーションに返されます。

デスクトップ アプリケーションのディレクトリ検索によって生じる追加のトラフィックはわずかですが、1 つ以上の Unified CM Assistant コンソール アプリケーションがリモート サイトで実行されている集中型のコール処理配置では、このトラフィックが問題になることがあります。1 つのエントリが得られるディレクトリ検索では、Unified CM Assistant サーバからデスクトップ アプリケーションへの約 1 キロビットのトラフィックが発生します。1 回の検索あたり最大 25 のエントリを取得できるため、デスクトップ アプリケーションで実行される検索ごとに最大約 25 キロビットのトラフィックが生成されることがあります。ただし、Unified CM Assistant サーバからの低速 WAN リンクを通じて、複数の Unified CM Assistant Console デスクトップ アプリケーションでディレクトリ検索が実行されると、輻輳、遅延、およびキューの発生する可能性が高くなります。また、ディレクトリ検索トラフィックは、デスクトップに対するその他すべての Unified CM Assistant トラフィックと同様に、TCP ポート 2912 の Cisco Unified CM から発生します。つまり、ディレクトリ検索トラフィックも DSCP 24（PHB CS3）としてマーキングされるため、コール シグナリング トラフィックと同様にキューに入れられます。このため、ディレクトリ検索によって、呼制御トラフィックの輻輳、オーバーラン、または遅延が生じる可能性があります。

（注）　ディレクトリ検索で 25 を超えるエントリが生成される場合、アシスタントには、ダイアログボックスを介して警告メッセージ「Your search returned more than 25 entries.Please refine your search.」が表示されます。

ネットワーク輻輳の可能性を考慮に入れて、管理者は Unified CM Assistant Console ユーザに次の操作の実行を推奨することを推奨します。

- ディレクトリ ウィンドウ検索機能の使用を制限する。
- 返されるエントリの数を減らすため、この機能を使用するときは、[Name] フィールドにできる限り多くの情報を入力し、ワイルドカードやブランクでの検索は実行しない。

これらの推奨事項は、次のいずれかの条件が該当する場合は特に重要です。

- クラスタ内に多数の Unified CM Assistant Assistants が存在する。
- Cisco Unified CM または Unified CM Assistant サーバ（あるいはその両方）から低速 WAN リンクによって分離されている多数のアシスタントが存在する。

Unified CM Assistant Phone Console の QoS

Unified CM Assistant Phone Console 電話サービスを使用してマネージャに代わってコールを処理するには、アシスタントがユーザ ID と PIN（Unified CM の End-user ディレクトリで設定されている）を入力してアプリケーションにログインする必要があります。ユーザがログインしている状態になると、電話コンソール サービスは HTTPS および SCCP を使用して Unified CM と通信します。Unified CM Assistant コール生成およびコール処理の呼制御トラフィックは、SCCP を使用して電話と Unified CM の間で送信されます。デフォルトでは、このトラフィックは 24 の Differentiated Services Code Point

（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。こうして、コール シグナリング トラフィックと同様にネットワークを通じてキューに入れられ確保します。したがって、追加の QoS の設定またはマーキングの必要はありません。

WebDialer

WebDialer は Cisco Unified CM のクリックコール アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できます。管理者が CTI リンクを管理したり、JTAPI または TAPI アプリケーションを作成したりするために必要なものはありません。Cisco WebDialer には、独自のユーザ インターフェイスと認証メカニズムを提供するための、簡単な Web アプリケーションと HTTP または Simple Objects Access Protocol（SOAP）が用意されているからです。Cisco Unified Communications Widget の**クリックコール** アプリケーションは SOAP インターフェイスを使用し、現在は次の Web サイトでダウンロードできます（ログイン認証が必要です）。

http://tools.cisco.com/support/downloads/go/Redirect.x?mdfid=278875240

ここでは、WebDialer 機能の設計について次の項目を説明します。

- 「WebDialer のアーキテクチャ」（P.19-35）
- 「WebDialer のハイ アベイラビリティ」（P.19-41）
- 「WebDialer のキャパシティ プランニング」（P.19-42）
- 「WebDialer の設計上の考慮事項」（P.19-43）

WebDialer のアーキテクチャ

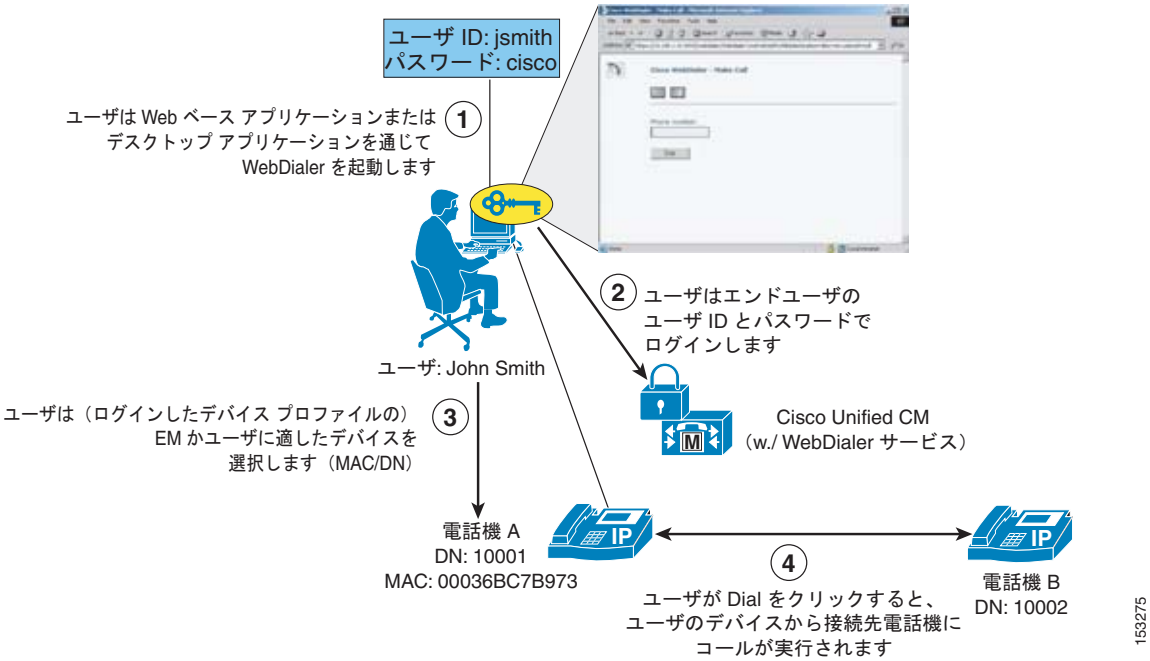
WebDialer アプリケーションには、WebDialer サーブレットと Redirector サーブレットの 2 つのサーブレットが含まれています。サブスクライバ サーバで Cisco WebDialer Web サービスがアクティブである場合、両方のサーブレットが有効になります。これらのサーブレットは関連していますが、それぞれ異なる機能を提供し、同時に実行するように設定できます。

WebDialer サーブレット

図 19-14 は、単純な WebDialer の例を示しています。この例で、ユーザ John Smith は、Unified Communications Widget のクリックコールなどの Web ベース アプリケーションまたはデスクトップ アプリケーションから WebDialer を起動します（ステップ 1）。WebDialer は、ログイン クレデンシャル要求で応答します。ユーザは、Unified CM エンド ユーザ ディレクトリで設定される有効なユーザ ID とパスワードで応答する必要があります。この場合、John Smith は userID = jsmith および password = cisco を送信します（ステップ 2）。次に、このログインに基づいて、WebDialer は [Cisco WebDialer Preferences] 設定ページで応答し、ユーザは、[User permanent device] または [Use Extension Mobility] のいずれかを示す必要があります（ユーザが EM デバイス プロファイルを持つと想定して）。この場合、ユーザ John Smith は、[User permanent device] を選択し、設定ページのドロップダウン メニューからその電話機に対して適切な MAC アドレス（SEP00036BC7B973）とディレクトリ番号（10001）を選択します（ステップ 3）。最後に、コールする電話番号を要求する画面が表示され（この値はすでに表示されていることがあります）、ユーザは [Dial] をクリックする必要があります。この場合、John Smith が 10002 と入力し、[Dial] をクリックすると、その電話機から番号 10002 の電話機 B へのコールが自動的に生成されます（ステップ 4）。

（注）　ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。Cookie がブラウザでクリアされるか、または WebDialer サーバの再起動によってクリアされた場合は、再ログインが要求されます。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータ で設定できます。これは、WebDialer サービス パラメータ で設定された通り所定の時間が経過した後、自動的に期限切れになります。

図 19-14　WebDialer サーブレットの動作



Redirector サーブレット

Redirector サーブレットは、マルチクラスタまたは分散型のコール処理環境において、WebDialer 機能を提供します。この機能を使用すると、すべての Unified CM クラスタ間で単一の企業全体の Web ベース WebDialer アプリケーションを使用できます。図 19-15 は、WebDialer アプリケーションの一部として Redirector サーブレットの基本的な動作を示しています。この例で、この企業には 3 個の Unified CM クラスタとして、New York、Chicago、および San Francisco があります。3 個のクラスタはすべて、単一の WebDialer アプリケーションで設定されます。San Francisco クラスタは、Redirector として指定されます。企業全体の Redirector として San Francisco の WebDialer を指定するには、各クラスタ WebDialer サーバに独自の IP アドレス、および San Francisco の WebDialer IP アドレスで指定されたサービス パラメータ [List of WebDialer] が必要です。

（注）　Cisco Unified CM 7.1(2) 以降のリリースでは、[List of WebDialers] も [Application Server] メニューから設定できます。詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html にある『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

San Francisco の WebDialer サーバには、独自の IP アドレスと、企業内のその他の WebDialer サーバすべてのアドレスが設定されます。この例に基づいて、各 WebDialer サーバの [List of WebDialers] サービス パラメータ フィールドは、次のように設定されます。

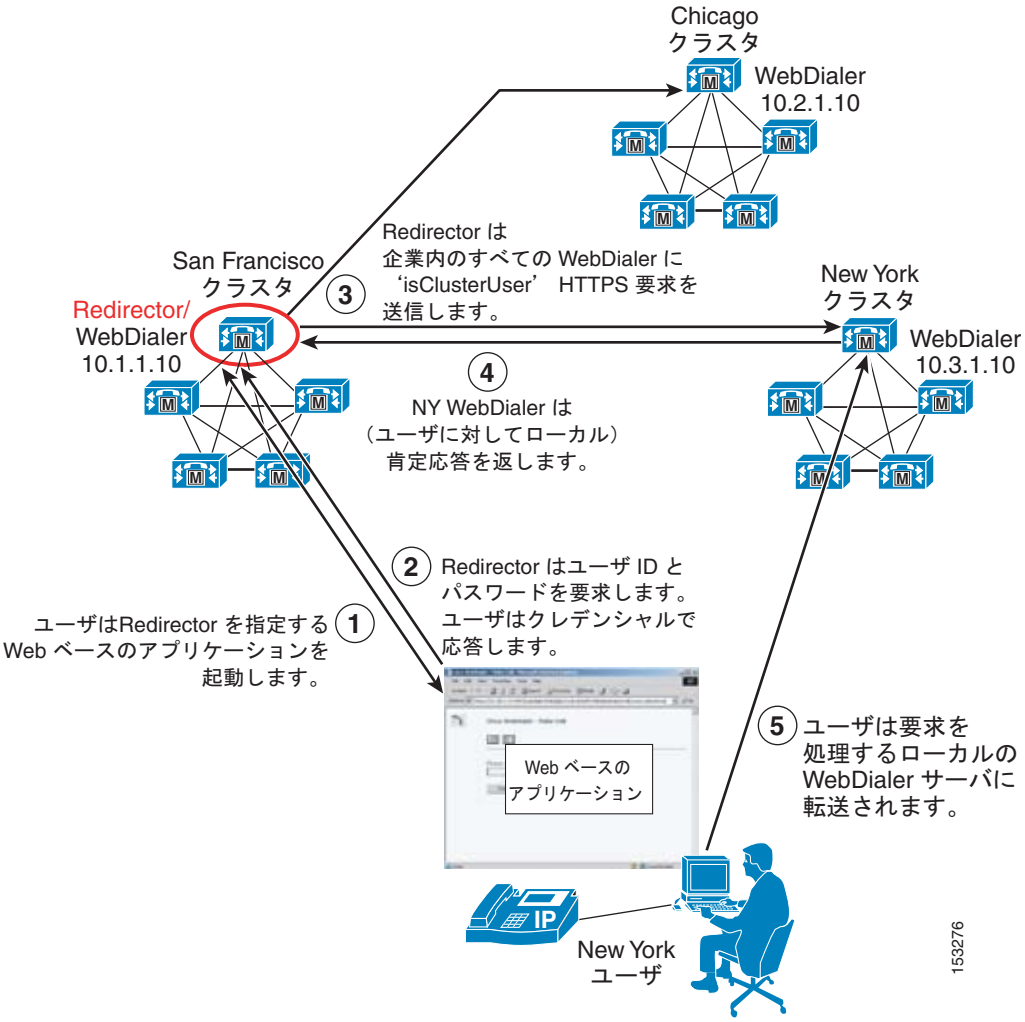
- New York の WebDialer：List of WebDialers: 10.1.1.10:8443 10.3.1.10:8443
- Chicago の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.10:8443
- San Francisco の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.10:8443 10.3.1.10:8443

企業全体の Web ベース アプリケーションは San Francisco の Redirector を指し、New York のユーザから起動されます（図 19-15 のステップ 1 を参照）。次に、Redirector はユーザのログインを要求し、New York ユーザは自分のユーザ ID とパスワードで応答します（図 19-15 のステップ 2 を参照）。

（注）　ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。一方、ユーザ Web ブラウザ クッキーは期限を WebDialer サービス パラメータ で設定できます。これは、WebDialer サービス パラメータ で設定された通り所定の時間が経過した後、自動的に期限切れになります。

次に、Redirector は、（List of WebDialers サービス パラメータの設定に従って）企業内のすべての WebDialer に isClusterUser HTTPS 要求を同時に送信します。この例で、要求は Chicago および New York の WebDialer サーバに送信されます（図 19-15 のステップ 3 を参照）。New York ユーザは New York クラスタに対してローカルであるため、New York の WebDialer は肯定応答を返します（図 19-15 のステップ 4 を参照）。最後に、New York ユーザはアプリケーション要求を処理するローカル WebDialer サーバに転送されます（図 19-15 のステップ 5 を参照）。この転送はユーザに通知されません。ただし、ブラウザのアドレス バーの URL は、ユーザが Redirector から WebDialer サーバに転送されたときに変更されます。

図 19-15　Redirector サーブレットの動作



（注）　Redirector アプリケーションは、Unified CM データベースでのユーザ認証の必要な企業全体のアプリケーションであるため、すべての Unified CM クラスタですべてのエンド ユーザのユーザ ID を一意にすることを強く推奨します。一意でない場合、Redirector アプリケーションが isClusterUser 要求に対する複数の肯定応答を受信する可能性があります。この場合、Redirector アプリケーションによって、ユーザは自分のローカル WebDialer サーバを手動で選択するように求められます。このため、ユーザは自分のローカル サーバを知っている必要があります。正しくないサーバを選択した場合、WebDialer 要求は失敗します。

WebDialer のアーキテクチャ

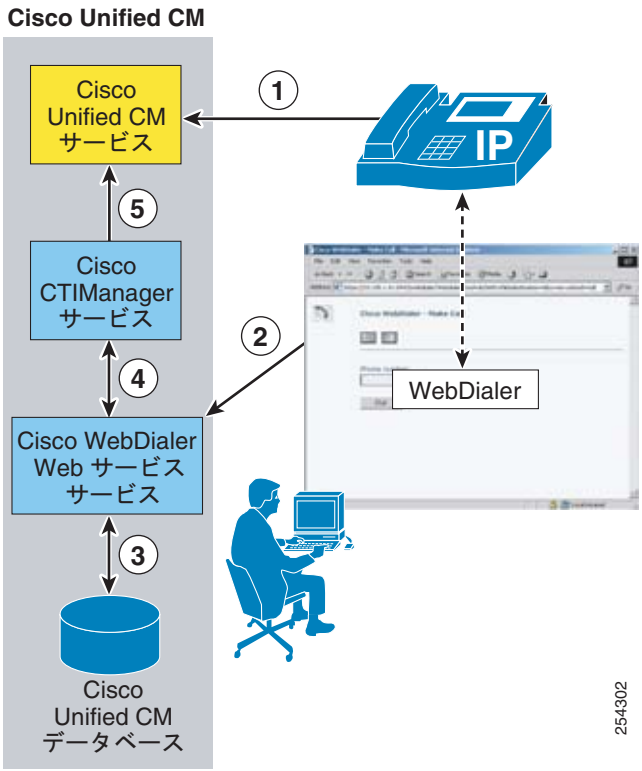
WebDialer アプリケーションのアーキテクチャは、その機能と同様に、そのアーキテクチャについても理解することが重要です。図 19-16 は、WebDialer のメッセージ フローとアーキテクチャを示しています。次の一連の対話とイベントが発生します。

1. WebDialer ユーザの電話機は、Cisco CallManager サービスを通じて登録し、コールの発信と受信を行います（図 19-16 のステップ 1 を参照）。
2. ユーザの PC 上の WebDialer アプリケーションは、次のいずれかのインターフェイスを通じて Cisco WebDialer Web Service と通信します（図 19-16 のステップ 2 を参照）。
   - HTML over HTTPS

     このインターフェイスは、HTTPS プロトコルに基づいて Web ベースのアプリケーションで使用されます。これは、Redirector サーブレットへのアクセスを提供する唯一のインターフェイスです。
   - Simple Object Access Protocol（SOAP）over HTTPS

     このインターフェイスは、SOAP インターフェイスに基づいてデスクトップ アプリケーションで使用されます。
3. WebDialer Web サービスは、Unified CM データベースからユーザおよび電話の情報を読み取ります（図 19-16 のステップ 3 を参照）。
4. 次に、WebDialer Web サービスは、回線と電話の制御情報を交換するために、CTIManager サービスと対話します（図 19-16 のステップ 4 を参照）。
5. CTIManager サービスは、WebDialer 電話制御情報を Cisco CallManager サービスに渡します（図 19-16 のステップ 5 を参照）。

図 19-16　WebDialer のアーキテクチャ



（注）　図 19-16 は、すべて同じノードで実行されている Cisco Unified CallManager、CTIManager、および WebDialer Web Service サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

WebDialer の URL

Web ベースのアプリケーションから HTML-over-HTTPS インターフェイスを通じて WebDialer アプリケーションにアクセスするには、次の URL を使用します。

- WebDialer サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Webdialer?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行しているクラスタ内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

- Redirector サーブレット

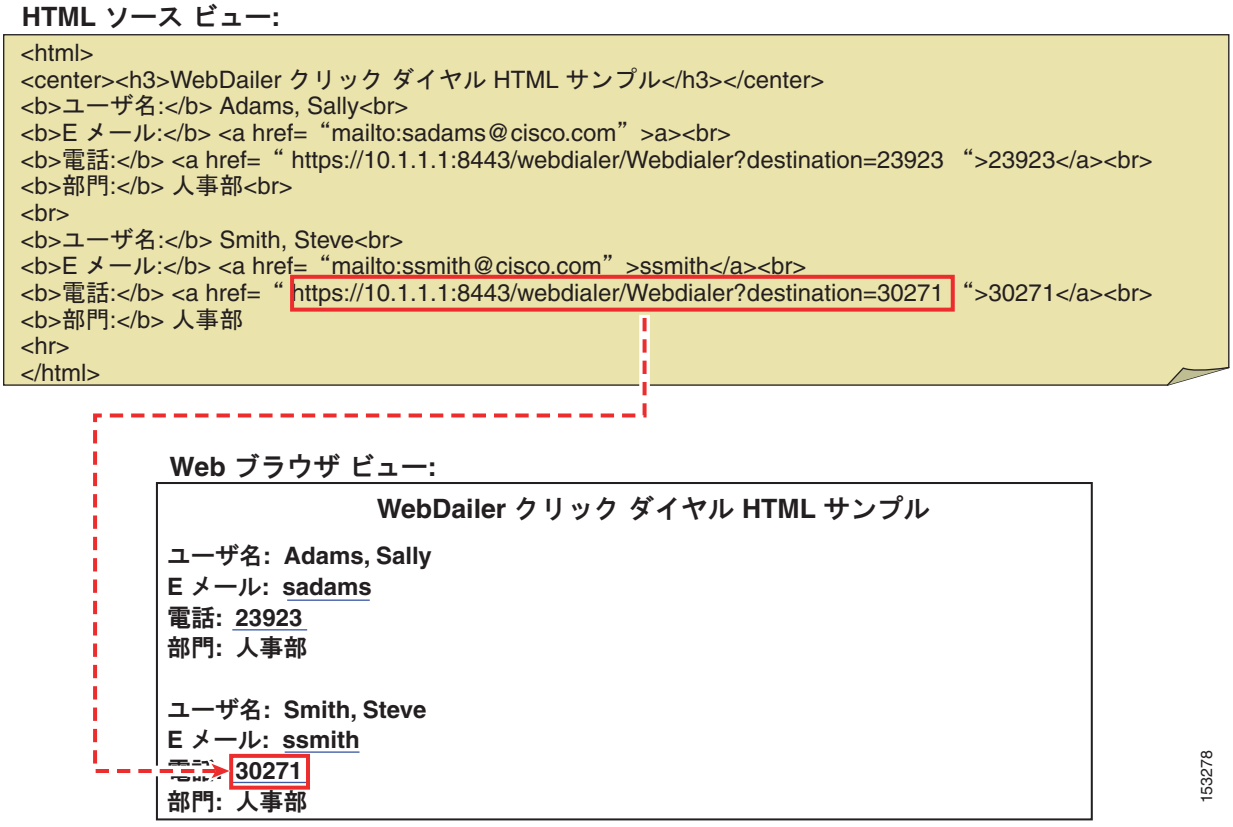
  https://<*Server-IP_Addr*>:8443/webdialer/Redirector?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行している企業内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

図 19-17 は、Cisco WebDialer アプリケーションをコールするクリックコール Web ベース アプリケーションで使用される、HTML ソース コードの例を示しています。この例で、HTML ソース ビューの URL https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 は、Web ブラウザ ビュー内のユー

ザ Steve Smith 用の「Phone: 30721」リンクに対応しています。ユーザがこのリンクをクリックすると、WebDialer アプリケーションが起動し、ログイン後に Dial をクリックすると、そのユーザの電話機から Steve Smith の電話機へのコールが生成されます。URL を https://10.1.1.1:8443/webdialer/Redirector?destination=30271 に変更すると、Redirector を使用するクリックコール アプリケーションで同じコードを使用できます。

図 19-17　WebDialer URL の HTML の例



デスクトップ アプリケーションのクリックコールで使用される SOAP-over-HTTPS ソース コードの情報および例については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Developers Guide*』の WebDialer API Programming 資料を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_programming_reference_guides_list.html

WebDialer のハイ アベイラビリティ

WebDialer アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、冗長性を、WebDialer サービスおよび CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、ユーザの電話機および WebDialer ユーザ インターフェイスに関連して検討する必要があります。

サービスとコンポーネントの冗長性

図 19-16 に示すように、WebDialer 機能は、主に Cisco WebDialer Web Service および Cisco CTIManager サービスに依存します。WebDialer サービスの場合は、List of WebDialers サービス パラメータに複数の WebDialer サーバの IP アドレスをリストし、クラスタ内の複数のノードでサービスを有効にすることで、冗長性を実現します。CTIManager の場合、冗長性は、プライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Primary Cisco CTIManager および Backup Cisco CTIManager のサービス パラメータを使用すると、クラスタ内に 2 つの CTIManager サーバまたはサービスを定義できます。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。Web ベース（またはデスクトップ）アプリケーションが指している WebDialer サーバに障害が発生し、クラスタ ノード上のプライマリおよびバックアップ CTIManager サービスにも障害が発生した場合、WebDialer アプリケーションはダウンします。WebDialer サービスは Unified CM パブリッシャに依存しません。

デバイスと到達可能性の冗長性

デバイス レベルでの WebDialer の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、ユーザの電話機は、デバイス登録用のデバイス プールと Unified CM グループ設定の組み合せによって提供される組み込み冗長性に依存します。

複数の WebDialer サービスは冗長性を提供するために複数の Unified CM サブスクライバを実行できます。しかしながら、多くのアプリケーションは複数の IP アドレスを処理するようには備わっていません。企業では、複数の WebDialer サーバのプレゼンスをマスクして Server Load Balancer（SLB; サーバ ロード バランサ）使用することを推奨します。SLB 機能は、仮想 IP アドレスまたは DNS-resolvable hostname を実現します。この DNS-resolvable hostname は、WebDialer および Redirector サーバの実 IP アドレスのフロントエンドになるものです。Cisco Application Control Engine（ACE）または Cisco IOS SLB 機能など多くの SLB デバイスは、複数の WebDialer サーバおよび障害イベント発生時に自動的な転送要求のステータスをモニタする設定ができます。SLB 機能は、追加のクリックコール キャパシティを必要とする場合、ロード バランサ WebDialer 要求も設定できます。代替えとして、DNS Service（SRV）レコードも冗長性の提供に使用できます。

企業の配置では、リンク コストもまた重要な考慮事項です。Cisco ACE Global Site Selector（GSS）アプライアンスは、リンク コストおよびロケーションをロード バランシング アルゴリズム追加することで、その他の機能の 1 つとして、SLB 機能のキャパシティ を拡張します。ACE および GSS の詳細については、http://www.cisco.com を参照してください。

WebDialer のキャパシティ プランニング

WebDialer および Redirector サービスは Unified CM クラスタ内で複数のサブスクライバ ノードを実行でき、次のキャパシティ がサポートされています。

- 各 WebDialer サービスは、ノードごとに 1 秒あたり最大 2 コール要求（1 時間あたり 7,200 コール）まで処理できます。
- 各 Redirector サービスは、1 秒あたり最大 8 コール要求まで処理できます。

次の一般式が WebDialer の 1 秒あたり のコール数の決定に使用できます。

（WebDialer のユーザ数）X（（平均 BHCA）/（3600 秒/時間））

この計算を行う場合、特に WebDialer サービス使用し、開始しているユーザあたり BHCA の数を適切に推定することが重要です。次に、見本の組織でこれら WebDialer デザインの計算を使用する例を示します。

例 19-1　WebDialer のコール数 1 秒あたりの計算

会社 XYZ は、WebDialer サービスを使用してクリックコール アプリケーションを稼動させることを考えています。その事前のトラフィック分析結果は次の資料の通りです。

- 10,000 人をクリックコール機能で有効にする。
- 各ユーザの平均 6 BHCA
- すべてのコールの 50% が発信で、50% が着信
- 計画では、すべての発信のうち、WebDialer サーバを使用して開始する発信を 30% と見積もる。

（注） これらの値は、WebDialer 配置のサイジングの演習を示すために使用した例です。ユーザのダイヤル特性は、組織から組織へ 広範にわたって変化します。

10,000 のユーザで各 6 BHCA では、合計 60,000 BHCA に相当します。ただし、WebDialer 配置のサイジングの計算は、発信コールのみの割合を占めます。このサイジングの例で最初の情報では、合計 BHCA の 50%が発信です。これは、WebDialer を使用する有効なクリックコールが、すべてのユーザのうち、合計で 30,000 placed BHCA という結果になります。

この発信数のうち、WebDialer サービスを使用して開始されるところの百分率（%）は、組織から組織で変化します。この例の組織では、ユーザが利用するいくつかのクリックコール アプリケーションは、WebDialer を使用して開始する発信の 30% と計画されています。

WebDialer を使用の場合（30,000 placed BHCA）X 0.30 = 9,000 placed BHCA

9,000 BHCA の負荷をサポートするのに必要な WebDialer サーバの数を判別するには、この値を煩雑する時間に維持する必要のある平均の Busy Hour Call Attempt（BHCA）1 秒あたりに変換します。

（9,000 call attempts / 時間）X（時間 /3600 秒）= 2.5 cps

各 WebDialer サービスは最大で 2 cps をサポートできます。したがって、この例では、WebDialer サービスを実行するため 2 つのノードを設定する必要があります。これは、将来の WebDialer 拡張使用に利用できます。障害が発生時に WebDialer キャパシティを維持するため、冗長性を提供する追加のバックアップ WebDialer サーバを設置する必要があります。

Cisco WebDialer アプリケーションは、電話制御のために CTIManager と対話することに留意してください。有効にすると、各 WebDialer サービスは単一持続性 CTI 接続を CTIManager に開きます。また、各 WebDialer の個々の MakeCall（または EndCall）要求は一時的な CTI 接続を生成します。WebDialer コール レートの処理に必要な CTI 接続の数も、クラスタごとの CTI 接続制限に対して適用されます（クラスタごとの CTI 接続制限の詳細については、「CTI のキャパシティ プランニング」（P.8-40）を参照してください）。

WebDialer の設計上の考慮事項

次のガイドラインと制限は、Unified CM テレフォニー環境内の WebDialer の配置と動作に関連して適用されます。

- 管理者は、すべての WebDialer ユーザが Unified CM エンド ユーザ ディレクトリの電話機またはデバイス プロファイルに関連付けられることを確認します。
  - 電話機が関連付けられていない状態でユーザが [Cisco WebDialer Preferences] 画面の [Use permanent device] を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

「No supported device configured for user」

- デバイス プロファイルが関連付けられていない状態で（またはプロファイルを使用してログインしないで）ユーザが [Cisco WebDialer Preferences] 画面の [Use Extension Mobility] を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

  「Call to <*dialed_ number*> failed: User not logged in on any device」

- List of WebDialers サービス パラメータを設定するときは、WebDialer IP アドレスと同時にポート番号 8443 を指定する必要があります。
- クライアント識別コード（CMC）または強制承認コード（FAC）を使用している場合、WebDialer ユーザはトーンが聞こえたときに、電話機のキーパッドを使用して適切なコードを入力する必要があります。トーンが聞こえたときに適切なコードを入力しないと、コールの失敗を示すリオーダー トーンが聞こえます。
- Cisco WebDialer は、Cisco Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）でサポートされている Skinning Client Control Protocol（SCCP）と Session Initiation Protocol（SIP）が動作するシスコ製 IP 電話をサポートします。
- Cisco Unified Personal Communicator は、デスクフォン モードで実行しているときに限り WebDialer をサポートします。Cisco Unified Personal Communicator がデスクフォン モードである場合、WebDialer によってサポートされる電話機モデルである限り、WebDialer を使用してデスク電話にクリックコール機能を備えることができます。ソフトフォン モードの Cisco Unified Personal Communicator は、WebDialer をサポートしません。

アテンダント コンソール

アテンダント コンソールの統合によって、受付係は、組織内でその目的のために特別に設計されたデスクトップ アプリケーションからコールに応答したり、コールを転送または送信したりできます。アテンダント コンソールからは社内ディレクトリにアクセスでき、場合によっては、特定のユーザの回線状態をモニタできます。Cisco Unified Communications ポートフォリオには、次の 3 つのタイプの Cisco Unified Attendant Console が用意されています。

- Cisco Unified Department Attendant Console
- Cisco Unified Business Attendant Console
- Cisco Unified Enterprise Attendant Console

Cisco Unified Department、Business、および Enterprise Attendant Console には、コンソール担当者の Windows PC にインストールするクライアント アテンダント コンソール アプリケーションが用意されています。また、Unified CM とは別の物理サーバにインストールされたアテンダント コンソール サーバ アプリケーションも必要です。アテンダント コンソール アプリケーションはアテンダント コンソール サーバ アプリケーションと通信し、アテンダント コンソール サーバ アプリケーションは Secure Socket Layer（SSL）接続で CTI および AVVID XML Layer（AXL）を介して安全に Unified CM と通信します。複数のアテンダント コンソールを 1 つのアテンダント コンソール サーバに接続できます。アテンダント コンソールの Department、Business、および Enterprise バージョンは、サポートされるオペレータ クライアントの数やサポートされるディレクトリ エントリの数など、各種の機能の制限がそれぞれ異なります。

ここでは、アテンダント コンソールの設計について次の項目を説明します。

- 「アテンダント コンソールのアーキテクチャ」（P.19-45）
- 「アテンダント コンソールのハイ アベイラビリティ」（P.19-47）
- 「アテンダント コンソールのキャパシティ プランニング」（P.19-47）
- 「アテンダント コンソールの設計上の考慮事項」（P.19-48）

アテンダント コンソールのアーキテクチャ

図 19-18 は、Cisco Unified Department、Business、または Enterprise Attendant Console 統合のアーキテクチャの概要を示しています。ソリューションの機能と動作を理解することにより、アーキテクチャ自体の理解も深まります。次の一連の手順（図 19-18 を参照）は、アテンダント コンソールへの一般的なコールに関係するイベントを示しています。

1. コールが Unified CM に入ります。着信番号は CTI ルート ポイントに設定されたディレクトリ番号と一致します。
2. CTI ルート ポイントは、アテンダント コンソール サーバ アプリケーションによって CTI が制御され、サーバに設定されているキュー Direct Dial In（DDI）に関連付けられます。
3. アテンダント コンソール サーバ アプリケーションは、コールを直接 Computer Telephony（CT）ゲートウェイ デバイスのいずれかに内部的にリダイレクトします。このプロセスの一環として、アテンダント コンソール サーバ アプリケーションは、コールを CTI ポートにリダイレクトする CTI リダイレクト メッセージを CTI Manager サービスに送信します。

（注）　CTI リダイレクト メッセージでは、コールは接続されません。コールへの応答はなく、メディア接続もありません。

4. アテンダント コンソール サーバ アプリケーションはここで、コールを CT ゲートウェイ デバイスに関連付け、CTI ポートでそのコールを制御します。
5. この時点で、コールは、キュー DDI に関連付けられたシステム内のアテンダント コンソール クライアント アプリケーションに送信されます。
6. コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコールに応答することを選択すると、別の CTI リダイレクト メッセージが CTI Manager サービスに送信され、それによってコールが CTI ポートから応答するコンソール担当者の電話機に転送されます。コールは、コンソール担当者の電話機の設定に応じて、その電話機のハンドセットまたはヘッドセットに自動的に接続します。コンソール担当者の電話機および発信側のゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。
7. 別の内線番号への転送が必要である場合、コンソール担当者はアテンダント コンソール クライアント アプリケーションを介して転送を開始し、アテンダント コンソール サーバ アプリケーションに転送を伝達します。
8. アテンダント コンソール サーバ アプリケーションはそのコールを内部的にサービス キューに関連付け、CTI リダイレクト メッセージを CTI Manager サービスに送信します。これによって、コールはコンソール担当者の電話機からアテンダント コンソール サーバ アプリケーションによって制御される CTI ポートにリダイレクトされます。

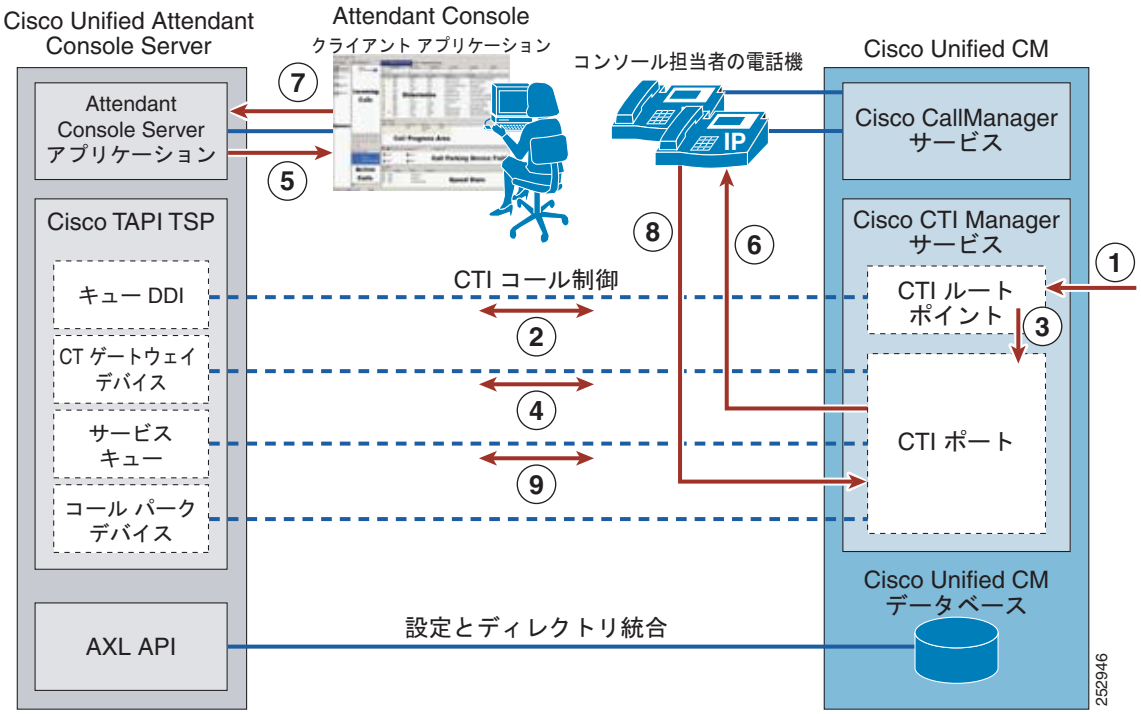
（注）　コール転送はコンソール担当者の電話機から発信される場合もありますが、その場合はアテンダント コンソール サーバ アプリケーションがコール フローから外れ、拡張機能（転送再コール機能など）は利用できなくなります。

9. この段階で、サービス キューは転送を実行する前にコールに実際に応答するので（短い接続があります）、アテンダント コンソール サーバ アプリケーションにインストールされた Cisco TAPI Wave ドライバが起動します。この CTI ポートおよびコール開始ゲートウェイまたは電話機のリージョンとロケーションの設定によって、メディアに使用されるコーデックが決定します。設定されている CTI ポートの Music On Hold（MoH; 保留音）オーディオ ソースも、発信者に聞こえる MoH に影響します。転送はこのように実行されるので、応答がない場合、アテンダント コンソール クライアント アプリケーションが引き続きコールを制御します。最終的な相手がコールを受信すると、アテンダント コンソール サーバ アプリケーションはコール フローから外れます。

（注）　アテンダント コンソール サーバ アプリケーションにインストールされる Cisco TAPI Wave ドライバは、G.711 コーデックだけをサポートします。サービス キューおよびコール パーク デバイスに対応する CTI ポートを設定する場合は、これらの CTI ポートに、G.711 の使用を指示する他のデバイスとのリージョンが設定されるようにシステムを設計するか、そうでなければトランスコーディング メディア リソースを装備します。

（注）　Cisco TAPI Wave ドライバによる G.711 a-law コーデックのサポートは、Cisco Unified CM 7.1(2) および Cisco TSP 7.1(3.3) 以降のリリースで導入されました。

図 19-18　Cisco Unified Department、Business、および Enterprise Attendant Console のアーキテクチャ



アテンダント コンソール サーバ アプリケーションのコール パーク機能では、Unified CM の固有のコール パーク機能は使用されません。代わりに、コール パーク デバイスを使用する独自のコール パーク機能が使用されます。コール パーク デバイスは、図 19-18 のステップ 7 ～ 9 にあるように、サービス キューとほとんど同様に機能します。転送と同様に、コール パーク デバイスを利用することで、コールのパーク中にアテンダント コンソール サーバ アプリケーションがコールを制御できるようになります。Cisco TAPI Wave Driver のコーデック制限（G.711 だけをサポート）は、コール パーク デバイスがかかわるコールにも影響します。

アテンダント コンソールのハイ アベイラビリティ

CTI と AXL 通信の両方について、統合の両側に冗長性を備えることを検討する必要があります。

CTI に関しては、アテンダント コンソール サーバ アプリケーションは Cisco Telephony Service Provider（TSP）プラグイン（Unified CM からダウンロード）を使用して、CTI Manager サービスと通信します。Cisco TSP では、プライマリとバックアップの CTI Manager サービスを設定できます。プライマリの CTI Manager サービスがオフラインになった場合の復元性を高めるため、クラスタ内の少なくとも 2 つの Unified CM サブスクライバ ノードで CTI Manager サービスを有効にすることを推奨します。現在、アテンダント コンソール サーバ アプリケーションに対する復元性の機能はありません。したがって、アテンダント コンソール サーバに障害が発生した場合の復元性を得るには、キュー DDI に関連付けられたすべての CTI ルート ポイントに Call Forward No Answer（CFNA）の宛先を設定します。アテンダント コンソール サーバ アプリケーションがオフラインになると、コールは自動的に CFNA の設定に従います。たとえば、宛先を 1 台の IP 電話に関連付けられたハント パイロット番号または Directory Number（DN; ディレクトリ番号）にできます。

AXL 通信を有効にするには、Unified CM ノードで Cisco AXL Web Service をアクティブにします。複数の Unified CM ノードで Cisco AXL Web Service を有効にできますが、アテンダント コンソール サーバ アプリケーションには Unified CM 接続用に 1 つのエントリしか設定できません。障害が発生した場合、管理者は Cisco AXL Web Service を実行するバックアップ用の Unified CM ノードにこのエントリをアップデートできます。

また、Unified CM には、Unified Department、Business、および Enterprise Attendant Console ソリューションとの統合用に一連の CTI ルート ポイントおよび CTI ポートが用意されています。これらのデバイスにはデバイス プールがあり、そのため Unified CM グループに割り当てられて、登録を維持する役割を果たす Unified CM コール処理ノードの優先順位別リストが示されます。Unified CM グループ内のプライマリの Unified CM がオフラインである場合、CTI ルート ポイントと CTI ポートはセカンダリの Unified CM ノードを登録できるので、CTI ルート ポイントおよびポート自体のハイ アベイラビリティが実現します。

アテンダント コンソールのキャパシティ プランニング

さまざまな Cisco Unified Department、Business、および Enterprise Attendant Console モデルおよびそれぞれのキャパシティの比較については、次の Web サイトで入手可能な『*Cisco Unified Business/Department/Enterprise Attendant Console Design Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps7282/products_implementation_design_guides_list.html

Unified CM クラスタを正しくサイジングするには、Unified CM クラスタのスケーラビリティに影響する可能性がある相互依存変数が多数存在するため、シスコ代理店またはシスコのシステム エンジニアが Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst）を使用して、多数の CTI リソースと大量のコールを包含するすべての設計を検証する必要があります。サイジング ツールを使用すると、Attendant Console 設計基準を満たすために必要なサーバまたはクラスタの正確な台数を決定できます。

各種の Unified Department、Business、および Enterprise Attendant Console のパフォーマンスとキャパシティについては、次の Web サイトで入手できる製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7282/tsd_products_support_series_home.html

アテンダント コンソールの設計上の考慮事項

次の設計上のガイドラインと制限は、Unified CM テレフォニー環境内の Cisco Unified Department、Business、および Enterprise Attendant Console の配置および動作に関して適用されます。

- 次の一般的な設計指針は、アテンダント コンソール サーバ アプリケーション コンポーネントに適用します。
  - キュー DDI

    1 つの一意なキュー DDI が、特にアテンダント コンソールにルーティングされる、システム内の一意の着信ディレクトリ番号ごとに必要です。
  - CT ゲートウェイ デバイス

    キュー DDI に入るすべての着信コールは、直接 CT ゲートウェイ デバイスにリダイレクトされます。CT ゲートウェイ デバイスが所定の時間に予想される最大着信コール数を処理するのに十分な台数になるよう、システムを設計してください。
  - サービス キュー

    コンソール担当者がコールを転送するか、コールを保留にするたびに、サービス キューが必要になります。システム内のすべてのコンソール担当者が所定の時間に転送する、または保留にするコールの最大数を維持できるだけの十分なサービス キューが用意されるように、システムを設計する必要があります。コンソール担当者ごとに 3 つか 4 つのサービス キューを用意することが一般的なガイドラインですが、シナリオによってはさらに多くのキューが必要になる場合もあります。
  - コール パーク デバイス

    コンソール担当者がアテンダント コンソール クライアント アプリケーションを介してコール パーク機能を起動するたびに、コール パーク デバイスが必要になります。この機能では、Unified CM の固有のコール パーク機能は使用されません。所定の時間にシステム内のすべてのコンソール担当者がパークするコールの最大数を処理できるだけの十分なコール パーク デバイスが用意されるように、システムを設計してください。
- アテンダント コンソール サーバ アプリケーションに設定されたすべてのキュー DDI、CT ゲートウェイ デバイス、サービス キュー、およびコール パーク デバイスによって、Unified CM 内の CTI ルート ポイントまたは CTI ポートが作成されます。また、Unified Department、Business、または Enterprise Attendant Console の統合を処理するために必要な CTI 接続の数も、クラスタごとの CTI 接続制限までカウントされます（クラスタごとの CTI 接続制限の詳細については、「CTI のキャパシティ プランニング」（P.8-40）を参照してください）。
- アテンダント コンソール サーバ アプリケーションは、エンド ユーザ デバイスの Busy Lamp Field（BLF; ビジー ランプ フィールド）モニタリングを可能にしますが、このアプリケーションでは、BLF スピード ダイヤル機能を実現する Unified CM 内の同一機能は使用されないことに注意してください。代わりに、アテンダント コンソール サーバ アプリケーションは、CTI を介して Unified CM と通信することで、モニタ対象デバイスの回線状態情報を取得します。アテンダント コンソール サーバ アプリケーションがエンド ユーザ デバイスをモニタする場合は、BLF のモニタ対象デバイスの台数が特定のレベル（デフォルトで 2,000）に到達するまで、CTI 経由でモニタが継続されます。この上限に到達すると、BLF プラグインが、新しく要求されたデバイスをモニタ対象デバイスのリストに追加するために、そのリストからデバイスを削除し始めるため、アテンダント コンソール サーバから CTI 経由で開始されるデバイスの台数が上限（デフォルトで 2000）を超えることはありません。CTI 経由でモニタされるこれらのデバイスは、Unified CM 上の CTI 上限も考慮されます。

- アテンダント コンソール サーバ アプリケーションにインストールされる Cisco TAPI Wave ドライバは、G.711 コーデックだけをサポートします。サービス キューおよびコール パーク デバイスに対応する CTI ポートを設定する場合は、これらの CTI ポートに、G.711 の使用を指示する他のデバイスとのリージョンが設定されるようにシステムを設計するか、そうでなければトランスコーディング メディア リソースを装備します。
- アテンダント コンソール サーバ アプリケーションは、エンド ユーザ デバイスの Busy Lamp Field（BLF; ビジー ランプ フィールド）モニタリングを可能にしますが、このアプリケーションでは、BLF スピード ダイヤル機能を実現する Unified CM 内の同一機能は使用されないことに注意してください。代わりに、アテンダント コンソール サーバ アプリケーションは、CTI を介して Unified CM と通信することで、モニタ対象デバイスの回線状態情報を取得します。
- Quality of Service（QoS）に関しては、アテンダント コンソール サーバ アプリケーション、アテンダント コンソール クライアント アプリケーション、および Cisco TSP はすべて Best Effort としてマークされたトラフィック（DSCP=0）を送信します。このトラフィックが WAN または通常輻輳するリンクを経由する場合は、ネットワークを介して優先的に処理されるようにパケットにマーキングする必要があります。これらのアプリケーションに関連付けられた TCP ポート番号の完全なリストについては、次の Web サイトで適切なログイン認証によって入手可能な Unified Department、Business、または Enterprise Attendant Console の設計ガイドを参照してください。

  http://www.cisco.com/go/ac
- アテンダント コンソール サーバ アプリケーションは、パーティションを認識しません。したがって、複数のパーティションに同じディレクトリ番号（DN）が存在する場合、モニタ対象のデバイスの DN に誤りが生じる可能性があります。
- Cisco Unified Department、Business、および Enterprise Attendant Console は、Cisco Unified Presence Server にも統合できます。このタイプの統合の詳細については、次の Web サイトで入手できる Unified Department、Business、または Enterprise Attendant Console の適切なアドミニストレーション ガイドを参照してください。

  http://www.cisco.com/en/US/products/ps7282/prod_maintenance_guides_list.html
- Cisco Unified Department、Business、および Enterprise Attendant Console の設計ガイドラインについては、次の Web サイトで入手可能なマニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps7282/products_implementation_design_guides_list.html

PART 4

Unified Communications アプリケーションとサービス

CHAPTER 20

Cisco Unified Communications アプリケーションおよびサービスの概要

ネットワーク、コール ルーティング、および呼制御のインフラストラクチャを Cisco Unified Communications システム用に配置すると、追加のアプリケーションおよびサービスをそのインフラストラクチャの最上位に追加または階層化できます。既存の Cisco Unified Communications インフラストラクチャに配置できるアプリケーションおよびサービスは多数存在します。通常は、次のアプリケーションおよびサービスを配置します。

- 音声メッセージング：ボイスメール サービスおよびメッセージ待機インジケータを提供します。
- リッチ メディア会議：音声会議とビデオ会議、および Web ベースのアプリケーションとドキュメント共有を提供します。
- プレゼンス サービス：ユーザ デバイスおよびクライアントでのユーザの応答可能性を確認します。
- モビリティ サービス：企業外部のユーザに対して、企業レベルのユニファイド コミュニケーション機能を提供します。
- コンタクト センター：大規模コールのコール処理、キューイング、およびモニタリングを行います。
- コラボレーション クライアント サービス：複数のユニファイド コミュニケーション サービスを統合し、さまざまなアプリケーションを活用できるようにします。

本 SRND のこの章では、上記のアプリケーションおよびサービスについて説明します。各章では、アプリケーションまたはサービスの概要を示したあと、アーキテクチャ、ハイ アベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。各章では、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

SRND のこの部分に含まれる章は、次のとおりです。

- 「シスコの音声メッセージング」（P.21-1）

  この章では、音声メッセージングについて説明します。音声メッセージングは、ほとんどのユニファイド コミュニケーション配置において一般的に普及しているアプリケーションです。音声メッセージングを使用して、発信者はメッセージを送信し、システムのサブスクライバはメッセージを取得できます。この章では、音声メッセージング アプリケーションに関するメッセージング配置モデル、音声メッセージングの機能、ボイスメール ネットワーキング、および設計と配置のベスト プラクティスについて説明します。

- 「Cisco コラボレーティブ会議」（P.22-1）

  この章では、リッチ メディア会議について説明します。ユニファイド コミュニケーション システムのユーザは、リッチ メディア会議を使用して、音声会議、ビデオ会議、および Web コラボレーション会議に対するスケジュール、管理、および参加を実行できます。この章では、コンポーネン

ト、配置モデル、ビデオ機能、H.323 と SIP の呼制御の統合、キャパシティと冗長性、さまざまな推奨ソリューションと設計のベスト プラクティスなど、リッチ メディア会議のさまざまな側面について検討します。

- 「Cisco Unified Presence」（P.23-1）

  この章では、プレゼンス サービスについて説明します。生産性はユーザの応答可能性ベースのアプリケーションによって向上できるため、ほとんどのユニファイド コミュニケーション配置において、プレゼンス サービスの重要性が高まっています。この章では、プレゼンスを定義し、プレゼンスのさまざまなコンポーネントと機能、プロトコル、配置モデル、冗長性、キャパシティ、および一般的な設計ガイドラインについて説明します。

- 「Cisco Collaboration クライアントおよびアプリケーション」（P.24-1）

  この章では、従来のハードウェアベースの電話機と機能豊富な PC ベースのクライアント間のギャップを急速に埋めている、コラボレーション クライアントとアプリケーションについて説明します。この章では、さまざまなコラボレーション クライアント、その機能、およびさまざまな統合方式以外に、サードパーティ製の各種コラボレーション アプリケーションとの統合について説明します。

- 「モバイル ユニファイド コミュニケーション」（P.25-1）

  この章では、モビリティ アプリケーションについて説明します。モビリティ アプリケーションは、モバイル従業員の増加、およびユニファイド コミュニケーション機能およびサービスに関する企業の境界があいまいになっていることからその重要性は非常に高く、モビリティ アプリケーションとサービスに対する需要が高まる結果となっています。この章では、モビリティのソリューション アーキテクチャ、機能、および設計と配置が及ぼす影響について説明します。

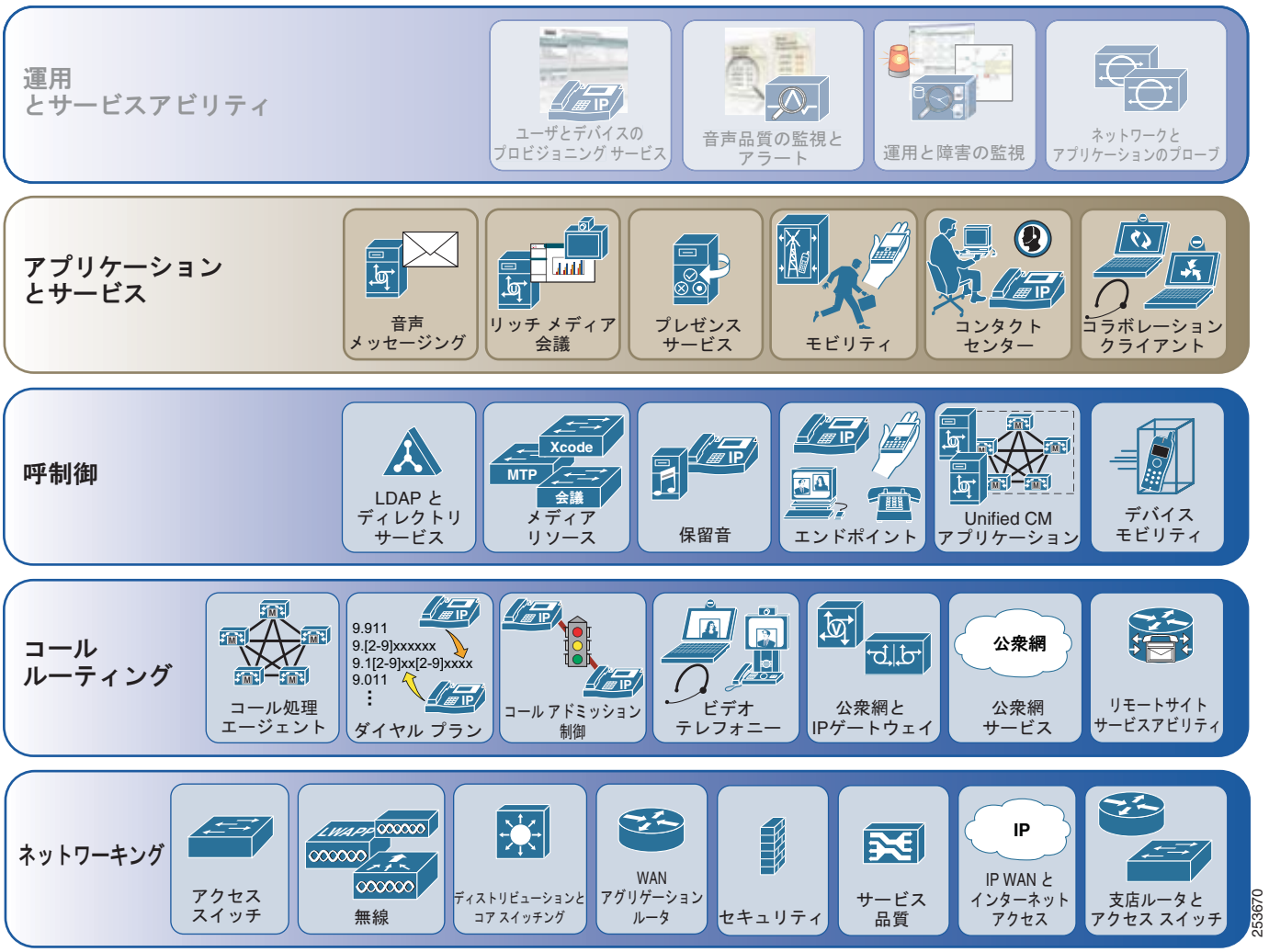
- 「Cisco Unified Contact Center」（P.26-1）

  この章では、大容量コール センター アプリケーションを必要とする大規模なユニファイド コミュニケーション配置にとって重要かつ不可欠な部分である、コンタクト センター ソリューションについて説明します。この章では、コール センター ソリューションのアーキテクチャ、機能、および設計と配置が及ぼす影響について説明します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムの場合と同様に、ユニファイド コミュニケーション アプリケーションとサービスは、基盤となるネットワーク インフラストラクチャとシステム インフラストラクチャの最上位で階層化する必要があります。図 20-1 は、Cisco Unified Communications システム アーキテクチャ全体におけるユニファイド コミュニケーション アプリケーションとサービスの論理的ロケーションを示しています。

図 20-1　Cisco Unified Communications アプリケーションとサービスのアーキテクチャ



ユニファイド コミュニケーション アプリケーションとサービス（音声メッセージング、リッチ メディア会議、プレゼンス、モビリティ、コンタクト センター、コラボレーション クライアントなど）は、ネットワーク接続から基本的なユニファイド コミュニケーション機能（呼制御、付加サービス、ダイヤル プラン、コール アドミッション制御、ゲートウェイ サービスなど）までのすべてに関して、基盤となるユニファイド コミュニケーションのコール ルーティングと呼制御インフラストラクチャ、およびネットワーク インフラストラクチャに依存します。たとえば、音声メッセージング アプリケーションとリッチ メディア会議アプリケーションでは、ネットワーク インフラストラクチャを利用して、キャンパス サイト、支店サイト、およびインターネット上のユーザに到達します。また、これらのアプリケーションは、コール ルーティングと呼制御インフラストラクチャによって提供される、ユニファイド コミュニケーションの音声とビデオのエンドポイント、コール ルーティング、公衆網接続、

およびメディア リソースを使用します。アプリケーションとサービスは、これらのインフラストラクチャ レイヤおよび基本的なユニファイド コミュニケーション サービスに依存しているだけでなく、多くの場合、完全に機能するために相互依存もしています。

ハイ アベイラビリティ

ネットワーク、コール ルーティング、および呼制御の各インフラストラクチャの場合と同様に、重要なユニファイド コミュニケーション アプリケーションとサービスでは、ネットワークやアプリケーションに障害が発生した場合でも必要な機能を引き続き使用できるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。多くのユニファイド コミュニケーション アプリケーションが他のアプリケーションやサービスに依存しているため、場合によっては、単一のサーバまたは機能の障害が、複数のサービスに影響を及ぼすことがあります。たとえば、コンタクト センター配置のさまざまなアプリケーション サービス コンポーネントが適切に機能できる場合でも、この配置において、コール センター アプリケーションへのコールのルーティングが呼制御サーバに依存していると、すべての呼制御サーバに障害が発生したとき、コンタクト センターが事実上使用できなくなる場合があります。

音声メッセージングやリッチ メディア会議などのアプリケーションとサービスの場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続やアプリケーション サーバの障害が原因で機能が一時的に失われ、その結果、発信者がメッセージを残すことができない、ユーザがメッセージを取得できない、ユーザが会議をスケジュールできない、およびユーザが会議に参加できない、などの状況が発生することが含まれます。また、音声メッセージングとリッチ メディア会議アプリケーションの発信者とユーザのフェールオーバーに関する考慮事項には、特定の障害が発生した場合に、エンド ユーザがサービスに引き続きアクセスできるように、冗長なリソースによって一部の機能を処理できるようにするというシナリオが含まれます。

また、ハイ アベイラビリティの考慮事項は、プレゼンスやモビリティなどのサービスに関する考慮事項でもあります。ネットワーク接続の中断またはサーバの障害が発生すると、通常、機能が低下し、場合によっては、機能が完全に失われます。プレゼンス サービスの場合、このことは、一部またはすべてのデバイスおよびクライアントで、プレゼンスや可用性の更新を送受信できなくなることを意味することがあります。モビリティ サービスの場合、ハイ アベイラビリティの考慮事項には、2 ステージ ダイヤリングまたは Dial-via-office などの特定の機能の喪失の可能性、またはシングル ナンバー リーチなどの機能の低下（会社の電話または携帯電話のいずれかだけが鳴る結果となる）が含まれます。さらに、一部の障害シナリオでは、完全な機能を再度使用するために、会社の電話およびモバイル クライアントを再登録し、再接続や最認証を行うことが必要となります。

コンタクト センターの配置の場合、数多くのサーバとコンポーネントに対して、ハイ アベイラビリティを考慮する必要があります。通常、独立した単一サーバまたは単一コンポーネントの障害は、そのサーバまたはコンポーネントに冗長性がある限り、機能や機能性を失うことなく対処できます。これ以外の場合には、複数のサーバまたはコンポーネントの損失によって、通常、一部の機能や機能性が失われます。ただし、すべての呼制御サーバなどの特定のコンポーネントが完全に失われた場合は、より深刻な機能の喪失が発生することがあります。

コラボレーション クライアントおよびアプリケーションについて考慮する場合は、ハイ アベイラビリティが特に重要となります。特定のコラボレーション機能や機能性が障害シナリオで使用できなくなるだけでなく、場合によっては、プレゼンス対応クライアントがネットワークに接続できなくなり、登録およびコールの発信や受信などの基本的な機能でさえ使用できなくなる可能性があります。また、クライアントやデバイスが、サービスを再度提供するために、再接続および再認証する必要がある場合もあります。

キャパシティ プランニング

ネットワーク、コール ルーティング、および呼制御インフラストラクチャは、個々のコンポーネントとシステム全体のキャパシティおよびスケーラビリティを理解したうえで、設計および展開する必要があります。同様に、ユニファイド コミュニケーション アプリケーションとサービスの配置は、キャパシティとスケーラビリティの考慮事項に注意して設計する必要があります。さまざまなユニファイド コミュニケーション アプリケーションを配置する場合は、アプリケーション自体のスケーラビリティの考慮が重要となるだけでなく、基盤となるインフラストラクチャのスケーラビリティについても考慮する必要があります。ネットワーク インフラストラクチャは、使用可能な帯域幅を持ち、アプリケーションによって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティングと呼制御のインフラストラクチャでは、ユーザとデバイスの設定および登録以外に、プロトコルと接続に関するアプリケーション統合の負荷を処理できる必要があります。たとえば、モビリティ、プレゼンス、コンタクト センターなどのアプリケーションとサービスでは、ユーザ、デバイス、および機能に関して、これらの個々のアプリケーションに対するキャパシティの暗黙的要件がありますが、Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）などの接続とプロトコルを処理する基盤インフラストラクチャのスケーラビリティも、同様に重要となります。モビリティ、プレゼンス、またはコンタクト センター アプリケーションが、多数の CTI 接続をサポートできる一方で、基盤となる呼制御およびコール ルーティングのインフラストラクチャが、これらのアプリケーションとサービスによって追加された CTI 負荷を処理するために使用できるキャパシティを持っていない場合があります。

音声メッセージングやリッチ メディア会議などのアプリケーションとサービスの場合、キャパシティ プランニングの考慮事項には、メールボックスまたはユーザの数、メールボックス サイズ、音声ポートとビデオ ポート、MCU セッションなどが含まれます。基盤となるネットワーク、コール ルーティング、および呼制御の各インフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、アプリケーション サーバや MCU を増やしたり、サーバや MCU ハードウェアを大容量モデルにアップグレードすることで、キャパシティを追加できます。

また、キャパシティ プランニングの考慮事項は、プレゼンスやモビリティなどのサービスに関する考慮事項でもあります。スケーラビリティで考慮する必要があるのは、設定済みまたはサポート対象のユーザとデバイスの数などの事項だけでなく、これらのアプリケーションとその他との統合および接続の数も含まれます。2 ステージ ダイヤリングおよび Dial-via-office コールの量は、呼制御機能および公衆網ゲートウェイ機能の両方の観点から、モビリティ アプリケーションにとって特別な考慮事項になります。一方、プレゼンス サービスの場合、スケーラビリティに関する重要な考慮事項には、プレゼンス ステータスの変更の頻度、およびネットワークへのこれらの変更の伝達以外に、テキストまたはインスタント メッセージの量が含まれます。通常、追加のアプリケーション サーバまたはハードウェアのアップグレードによって、これらのアプリケーションおよびサービスのキャパシティは増加しますが、基盤となるコール ルーティング インフラストラクチャと呼制御インフラストラクチャが、増加したすべての負荷を処理できる必要があります。

コンタクト センターの配置は、スケーラビリティの考慮事項という点では、他のアプリケーションおよびサービスと変わりません。当然、コールを処理するエージェントとエージェント デバイスの数は、ユーザとデバイスの設定および登録において重要となります。ただし、コンタクト センターの配置のキャパシティという観点となると、主要な考慮事項は、コンタクト センターでは一般的な多数の Busy Hour Call Attempts（BHCA; 最繁時呼数）、および呼制御インフラストラクチャとルーティング インフラストラクチャへの CTI 統合の数です。

コラボレーション クライアントおよびアプリケーションのキャパシティ プランニングを考慮する場合は、デバイスの登録および設定が、スケーラビリティの考慮事項として最も重要となります。ただし、プレゼンスやメッセージングなどのバックエンド アプリケーションとサービスには、スケーラビリティに関する他の暗黙的要件があります。また、さまざまなクライアントをサードパーティ製のアプリケーションおよびインフラストラクチャとともに配置または統合する場合は、これらのサードパーティ製の配置でサポートされているキャパシティを考慮することも必要となります。

CHAPTER 21

シスコの音声メッセージング

この章では、Cisco Unified Communications システムで利用可能な音声メッセージング ソリューションについて説明します。この章では、シスコの音声メッセージング製品である Cisco Unity、Cisco Unity Connection、および Cisco Unity Express を取り上げ、これらの製品を Cisco Unified Communications Manager（Unified CM）と共に配置するための設計ガイドラインとベスト プラクティスを説明します。また、この章では、業界標準プロトコルを使用した、サードパーティ製ボイスメール システムとの統合についても説明します。

このガイドでは、Unified CM に関するメッセージング配置のシナリオが中心ですが、特に、集中型 Unified CM 配置の Survivable Remote Site Telephony（SRST）フォールバック サポートで使用される場合には、適宜、Cisco Unified Communications Manager Express（Unified CME）についても説明します。

この章では、次のトピックについて取り上げます。

この章ではまず、Cisco メッセージング ソリューションのポートフォリオの各製品について簡単に説明した後、企業向け Unified Communications ソリューションにおける各製品の位置付けに関する簡単な概要を示します。次に、メッセージング配置モデルを基盤として、ボイスメール統合を説明します。ここではまず、さまざまなメッセージング配置モデルを定義した後、さまざまな Unified CM コール処理配置モデルにおける各メッセージング配置モデルの位置付けを説明します。さらに、さまざまな冗長性オプションの設計、および Survivable Remote Site Voicemail について説明します。この項では、Cisco Unity と Unity Connection を一緒に説明します。Cisco Unity Express については、別に専用の項を設けて、それがサポートする配置モデルを説明します。シスコの音声メッセージング製品ポートフォリオ内で利用可能な相互運用のための主要な設計ガイドラインについて説明します。新しい概念である仮想化、および仮想システム設計時に考慮する必要がある重要な設計上の要素について説明します。この項では、トランスコーディングや Cisco Unified Communications Manager とのさまざまな統合を含む、多くのシステム レベルの設計上の考慮事項およびベスト プラクティスについて説明します。さらに、この章では、サポートされている業界標準プロトコルを使用したサードパーティ製ボイスメール統合の詳細について説明します。

この章では、基本設計に関する説明を行います。また、Unified CM を使用して Unified Communications システムに音声メッセージング製品をどのように組み込むかに重点を置いて説明します。各製品の詳細な設計ガイドラインおよびサードパーティ製のメッセージングとテレフォニー システムの相互運用性に関する情報については、次に示す製品別の設計ガイドを参照してください。

- Cisco Unity Connection 設計ガイド

  http://www.cisco.com/en/US/products/ps6509/products_implementation_design_guides_list.html
- Cisco Unity 設計ガイド

  http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_implementation_design_guides_list.html

この章の新規情報

表 21-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 21-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
仮想化	「Cisco Unity と Unity Connection の仮想化」（P.21-34）	2011 年 7 月 29 日
Cisco Unity Connection での E.164 サポート	「Cisco Unity Connection による E.164 番号サポート」（P.21-40）	2011 年 6 月 2 日
Cisco Unity Connection での IPv6 サポート	「Cisco Unity Connection による IPv6 サポート」（P.21-45）	2010 年 11 月 15 日
Cisco Unity Connection 用の単一受信トレイ	「Cisco Unity Connection による単一受信トレイ」（P.21-45）	2010 年 11 月 15 日
Cisco Unity と Unity Connection の冗長性	「メッセージングの冗長性」（P.21-18）	2010 年 4 月 2 日
Enhanced Message Waiting Indicator（eMWI; 拡張メッセージ待機インジケータ）	「拡張メッセージ待機インジケータ（eMWI）」（P.21-41）	2010 年 4 月 2 日
Survivable Remote Site Voicemail（SRSV）	「Survivable Remote Site Voicemail」（P.21-10）	2010 年 4 月 2 日
仮想化	「Cisco Unity と Unity Connection の仮想化」（P.21-34）	2010 年 4 月 2 日
ボイスメールの相互運用性	「ボイスメールの相互運用性」（P.21-32）	2010 年 4 月 2 日

音声メッセージング ポートフォリオ

Cisco Unified Communications のメッセージング ポートフォリオは、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express の 3 つの主なメッセージング製品で構成されます。それぞれの製品が対応する要件は異なりますが、互いに他の製品と重なり合う機能とスケーラビリティを備えています。Voice Mail Networking を使用することで連携して動作することもできます。また、Cisco Unified Messaging Gateway を利用して、非常にスケーラブルな形でこれを実現することも可能です。これについては、この章で後ほど説明します。

これらの製品を検討する場合、それらに搭載されたメッセージング オプションを理解し、特定の配置要件に適したオプションを判断するためには、製品が該当するメッセージング タイプを考慮することが役立ちます。次の定義は、このようなメッセージング タイプの説明に役立ちます。

- *ボイスメール専用*とは、いずれのメッセージング クライアント経由でもボイスメールにアクセスできないテレフォニー ボイスメール統合を指します。
- *ユニファイド メッセージング*とは、テレフォニー アクセス、およびメッセージ クライアントを介したボイスメールへのアクセスを備えたボイスメールを指します。
- *ユニファイド メッセージング*とは、テレフォニー アクセス、およびメッセージング クライアントを介したボイスメール、電子メール、FAX へのアクセスを備えたボイスメールを指します。

表 21-2 は、これらのタイプのメッセージングをサポートするシスコ製品を示します。

表 21-2　各製品でサポートされるメッセージング環境

メッセージング タイプ	Cisco Unity	Cisco Unity Connection	Cisco Unity Express
ボイスメール専用	あり	あり	あり
ユニファイド メッセージング	あり	あり	あり
ユニファイド メッセージング	あり	あり	なし

（注）　Cisco Unity Connection を使用したユニファイド メッセージングの詳細については、「Cisco Unity Connection による単一受信トレイ」（P.21-45）を参照してください。

上のメッセージング タイプと定義に基づき、次の 3 つのメッセージング製品のオプションが用意されています。

- Cisco Unity

  このソリューション オプションは、大企業の組織が抱えるニーズにも対応可能な拡張性を持っており、Microsoft Exchange（Exchange 2007/2010 を含む）に統合可能な強力な音声メッセージング、ユニファイド メッセージング、ユニファイド メッセージングのオプションを提供します。

- Cisco Unity Connection

  このオプションは、20,000 ユーザ以下の中規模企業用に、ユニファイド メッセージング、音声認識、およびコール転送ルールを 1 つのシステムに組み合せて管理しやすくしたものです。また、デジタル ネットワーク システムに最大 10 のノードをネットワーク接続できます（必要であれば、さらに 2 つのデジタル ネットワークを結合して最大 20 ノードをサポートできます）。Cisco Unity Connection は、1 つのデジタル ネットワークで最大 100,000 ユーザまたは連絡先をサポートできます。500 ユーザ以下の組織では、Cisco Unity Connection をシングル サーバ ソリューションとして、Cisco Unified Communications Manager Business Edition 3000 および 5000 で使用できます。Cisco Unified Communications Manager Business Edition の詳細については、「コール処理の設計上の考慮事項」（P.8-34）を参照してください。

- Cisco Unity Express

  このオプションは、中小規模企業および 500 ユーザ以下の支店用に、特定の Cisco サービス統合型ルータで、コスト効率の高い音声メッセージングおよびユニファイド メッセージング、自動応答、および Interactive Voice Response（IVR; 音声自動応答装置）の各機能を提供します。

製品機能の完全な比較については、http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_data_sheets_list.html で入手可能な『*Cisco Messaging Products: Feature Comparison*』を参照してください。

表 21-3 に、スケーラビリティについての簡単な製品間の比較を示します。

表 21-3　音声メッセージング ソリューションのスケーラビリティ

ソリューション	単一のサーバ（またはフェールオーバー配置やクラスタ配置）でサポートされるユーザ			デジタル ネットワーキング ソリューションでサポートされる最大ユーザ数[1]	
	500	15,000	20,000	100,000	250,000
Cisco Unity Express	○	×	×	○	○
Cisco Unified CMBE	○	×	×	×	×
Cisco Unity Connection（ユニファイド メッセージング）	○	○	○	○	×
Cisco Unity（ユニファイド メッセージングおよび音声メッセージング）	○	○	×	○	○

1. Cisco Unified Messaging Gateway を使用してさまざまな製品をネットワーク接続すると、サポートされるユーザ数が大幅に増加します。サポートされるユーザ数は、ネットワーク接続されたノード数および Unified Messaging Gateway でサポートされる最大ユーザ数に直接関連します。Cisco Unified Messaging Gateway のスケーラビリティの詳細については、http://www.cisco.com/en/US/products/ps8605/products_data_sheets_list.html で入手可能な『Cisco Unified Messaging Gateway data sheet』を参照してください。

（注） Voice Profile for Internet Mail（VPIM）プロトコルおよびデジタル ネットワーキングのいずれを使用してもサポートされる最大ユーザ数が大幅に増加しますが、デジタル ネットワーキングでは、追加のサーバ検出機能およびディレクトリ同期化機能が提供されます。

スケーラビリティの詳細については、「Cisco Unified Messaging Gateway によるボイスメール ネットワーキング」（P.21-4）を参照してください。

Cisco Unified Messaging Gateway によるボイスメール ネットワーキング

Cisco Unified Messaging Gateway（UMG）は、インテリジェント ボイス メッセージング ルーティング、システム ディレクトリの管理、メッセージング形式、およびスケーラブルなボイス メッセージング フレームワークを提供することによって、エンドツーエンドのネットワーク接続されたボイス メッセージング ソリューションを可能にします。Cisco UMG は、Cisco Unity、Cisco Unity Express、Cisco Unity Connection、および Avaya Interchange をサポートします。

この章では、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express と Cisco Unified CallManager の統合について、設計上の側面を中心に説明します。Cisco Unified CM には、Session Initiation Protocol（SIP; セッション開始プロトコル）トランクの機能が搭載されているため、SIP プロキシ サーバを配置することなく、直接 Cisco Unity および Unity Connection と統合できます。

以前のリリースの Cisco Unity、Unity Connection、Unity Express、および Unified CM または Unified CM Express の詳細については、http://www.cisco.com で入手可能な資料を参照してください。

上で説明したように、この章で扱う設計に関するトピックは、ボイスメールのみの設定、ユニファイド メッセージング設定、およびユニファイド メッセージング設定に適用されます。加えて、この章では、Microsoft Exchange（2003、2007、または 2010）および Microsoft Windows（2003）を使用した Cisco Unity または Cisco Unity Connection の配置の設計面についても説明します。また、Microsoft

Active Directory（AD）2008 のサポートも Cisco Unity 7.*x* 以降のリリースで追加されました。この章では、Microsoft NT 4.0 や Exchange 5.5 による配置、および Microsoft NT 4.0 や Exchange 5.5 からのアップグレードにおける設計については説明しません。Cisco Unity Connection および Unity Express は外部メッセージ ストアに依存しません。Cisco Unity Connection 8.*x* は、Exchange 統合をサポートしますが、Cisco Unity と異なり、Exchange 統合に依存しません。

（注）　Microsoft Exchange 2010 および Active Directory 2008 R2 をサポートする Cisco Unity の正確なバージョンについては、Cisco Unity のリリース ノート（http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_release_notes_list.html）を参照してください。

シスコ以外のメッセージング システムとの統合など、Cisco Unity または Cisco Unity Connection に関するその他の設計情報については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。

Cisco Unity Express に関するその他の設計情報については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

シスコ以外のメッセージング システムとの統合など、Cisco Unified Messaging Gateway に関するその他の設計情報については、http://www.cisco.com で入手可能な Cisco Unified Messaging Gateway の製品マニュアルを参照してください。

メッセージング配置モデル

この章では、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express について、さまざまなメッセージング配置モデルの概要を示します。Cisco Unity、Unity Connection、およびさまざまなメッセージング コンポーネントに固有の配置モデルや設計上の考慮事項の詳細については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。Cisco Unity Express については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

Cisco Unity と Unity Connection は、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 集中型メッセージングを使用するマルチサイト配置
- 分散型メッセージングを使用するマルチサイト配置

Cisco Unity Express もまた、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング
- 分散型メッセージングを使用するマルチサイト配置
- Cisco Unified CME により分散型メッセージングを使用するマルチサイト配置

（注）　Cisco Unity Express は、最大 10 の Unified CME を持つ集中型音声メッセージングをサポートします。詳細については、http://www.cisco.com で Cisco Unified Communications Manager Express の資料を参照してください。

Cisco Unified CM と Unified CME のコール処理配置モデルは、Cisco Unity、Unity Connection、および Unity Express のメッセージング配置モデルに依存しませんが、互いに対して考慮が必要な暗黙的要件があります。

3 つのメッセージング配置モデルに加えて、Cisco Unity はメッセージング冗長性もサポートしています（「メッセージングの冗長性」（P.21-18）を参照）。アクティブ/アクティブ設定では、Cisco Unity Connection のメッセージング冗長性も利用できます。詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

すべてのメッセージング配置モデルが、ボイスメール、ユニファイド メッセージング、およびユニファイド メッセージングのインストールをサポートしています。

単一サイト メッセージング

このモデルでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトのアベイラビリティの高い同じ LAN 上に置かれます。サイトは、単一サイトである場合も、高速 Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）を介して相互接続されたキャンパス サイトである場合もあります。メッセージング システムのクライアントもすべて、単一（またはキャンパス）サイトに置かれます。このモデルの際立った特徴は、リモート クライアントが存在しないことです。

集中型メッセージング

このモデルでは、単一サイト モデルと同様に、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトに置かれます。サイトは、1 つの物理的なサイトである場合も、高速 MAN を介して相互接続されたキャンパス サイトである場合もあります。ただし、単一サイト モデルとは異なり、メッセージング クライアントをローカルとリモートの両方に置くことができます。

メッセージング クライアントはメッセージング システムのローカルで使用されることもリモートで使用されることもあるため、ViewMail for Outlook（VMO）を使用する場合、および Telephone Record and Playback（TRaP; 電話での録音および再生）機能とメッセージ ストリーミング機能を Cisco Unity で使用する場合は、これらの Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）クライアントには設計上特別に考慮する必要がある事項があります。リモート クライアントは、TRaP を使用すべきではありません。また、リモート クライアントは、再生前にメッセージをダウンロードするように設定する必要があります。ローカル クライアントとリモート クライアントで機能や操作が異なるとユーザが混乱するおそれがあるため、音声ポートで TRaP を無効にし、クライアントがローカルであるかリモートであるかに関係なく、メッセージをダウンロードするように設定し、TRaP を使用しないように GUI クライアントを設定する必要があります。このことは、Cisco Unity IMAP クライアントの ViewMail for Outlook（VMO）に対して当てはまります。これらの設計上の考慮事項は、Cisco Unity に固有の事項です。

Cisco Unity Telephone User Interface（TUI; 電話ユーザ インターフェイス）は、ローカル クライアントとリモート クライアントの両方に対して同様に動作します。

分散型メッセージング

分散型メッセージング モデルは、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング システムで構成されます。複数のロケーションを持つことができ、各ロケーションに独自のメッセージング システムとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのクライアント アクセスが各メッセージング システムに対してローカルであり、メッセージング システムは、すべてのロケーションにまたがるメッセージング バックボーンを共有します。分散型メッセージング システムからのメッセージ送信は、フルメッシュ タイプまたはハブアンドスポーク タ

イプのメッセージ ルーティング インフラストラクチャによって、メッセージング バックボーンを介して行われます。WAN によって、メッセージング インフラストラクチャ コンポーネントを、サービス提供先のメッセージング システムから切り離すことはできません。

分散型メッセージングは、基本的に、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング モデルです。このルールの例外は、PBX-IP Media Gateway（PIMG）統合と T1-IP Media Gateway（TIMG）統合です。PIMG 統合と TIMG 統合は、設計に関するこのドキュメントでは説明しません。PIMG または TIMG の詳細については、http://www.cisco.com で入手できる Cisco Unity の統合ガイドを参照してください。

分散型メッセージング モデルは、ローカルおよびリモートの GUI クライアント、TRaP、およびメッセージのダウンロードに関して、集中型メッセージングと同じ設計基準を持っています。

メッセージングと Unified CM 配置モデルの組み合せ

ここでは、さまざまなメッセージング配置モデルを Unified CM コール処理配置モデルに統合する場合の設計上の考慮事項について説明します。表 21-4 では、Cisco Unity、Unity Connection、および Unity Express によってサポートされるメッセージング配置モデルとコール処理配置モデルのさまざまな組み合せを示します。

表 21-4　サポートされているメッセージングと Unified CM コール処理配置モデルの組み合せ

モデル タイプ	Cisco Unity	Cisco Unity Connection	Cisco Unity Express
単一サイト メッセージングと単一サイト コール処理	あり	あり	あり
集中型メッセージングと集中型コール処理	あり	あり	なし[1]
分散型メッセージングと集中型コール処理	あり	あり	あり
集中型メッセージングと分散型コール処理	あり	あり	なし[1]
分散型メッセージングと分散型コール処理	あり	あり	あり
集中型メッセージングと WAN を介したクラスタリング	あり	あり	なし
分散型メッセージングと WAN を介したクラスタリング	あり	あり	あり

1. Unified CME による集中型ボイスメール メッセージングが Cisco Unity Express 3.2 以降サポートされていますが、これは Unified CM コール処理配置モデルには適用されません。

この項では、次のトピックについて取り上げます。

- Cisco Unity と Unity Connection メッセージングおよび Unified CM の 配置モデル
- Cisco Unity Express の配置モデル

各トピックではメッセージングと Unified CM の配置モデルの組み合せを定義した後、そのモデルに適用可能なシスコのボイスメール メッセージング製品と、そのモデルの組み合せに関する設計上の考慮事項について説明します。ここでは、各製品のすべての組み合せを取り上げるわけではありません。いくつかの例を示し、各製品のベスト プラクティスと設計上の考慮事項を説明します。ここでの説明は、基本となるメッセージング配置モデルと Unified CM とのインタラクションの理解を促すためのものであり、すべての可能性を詳細に説明することは意図していません。

サイト分類の詳細、およびメッセージング配置モデルとコール処理配置モデルのサポートされている組み合せの詳細な分析については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』および『*Design Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity と Unity Connection メッセージングおよび Unified CM の配置モデル

ここでは、Cisco Unity と Unity Connection によってサポートされるメッセージング配置モデルとコール処理配置モデルのさまざまな組み合せを示します。

集中型メッセージングと集中型コール処理

集中型メッセージングでは、ボイス メッセージング サーバを Unified CM クラスタと同じサイトに置くことができます。集中型コール処理では、サブスクライバがクラスタおよびメッセージング サーバに対して、リモートとローカルのどちらにも存在できます（図 21-1 を参照）。リモート ユーザが中央のサイトのリソース（音声ポート、IP Phone、Tail-End Hop-Off（TEHO; テールエンド ホップオフ）の場合の公衆網ゲートウェイなど）にアクセスする場合、そのコールはゲートキーパー コール アドミッション制御にとって透過的になります。したがって、Unified CM でリージョンとロケーションを設定して、コール アドミッション制御を提供する必要があります（「帯域幅の管理」（P.21-35）を参照）。IP Phone または MGCP ゲートウェイにリージョン間コールを発信する場合、IP 電話は設定済みのリージョン間コーデックを自動的に選択します。Cisco Unity メッセージング配置では、WAN を通過する（リージョン間）コールのために、音声ポートが Unified CM トランスコーディング リソースを使用するように、ネイティブ トランスコーディングを無効にする必要があります。Cisco Unity でこの機能を無効にする方法の詳細については、「ネイティブ トランスコーディング動作」（P.21-36）を参照してください。

図 21-1　集中型メッセージングと集中型コール処理

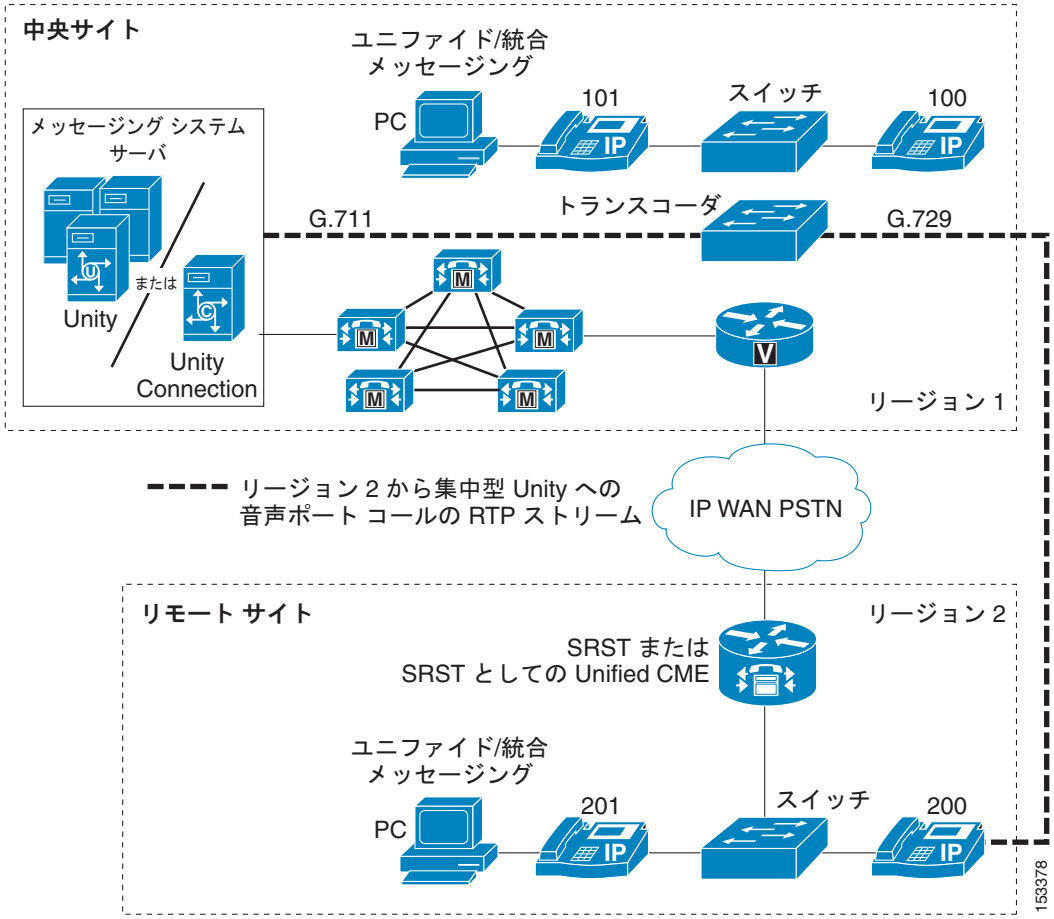


図 21-1 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

図 21-1 で示しているように、内線番号 200 からリージョン 1 のボイスメール ポートにコールが発信されると、エンドポイントではリージョン間の G.729 コーデックが使用されますが、RTP ストリームがトランスコードされ、音声ポート上では G.711 が使用されます。この例では、Cisco Unity サーバ上のネイティブ トランスコーディングが無効になっています。Unified CM トランスコーディング リソースは、ボイスメール システムと同じサイトに置く必要があります。

AAR によってルーティングされるボイスメール コールで RDNIS が送信されないことによる影響

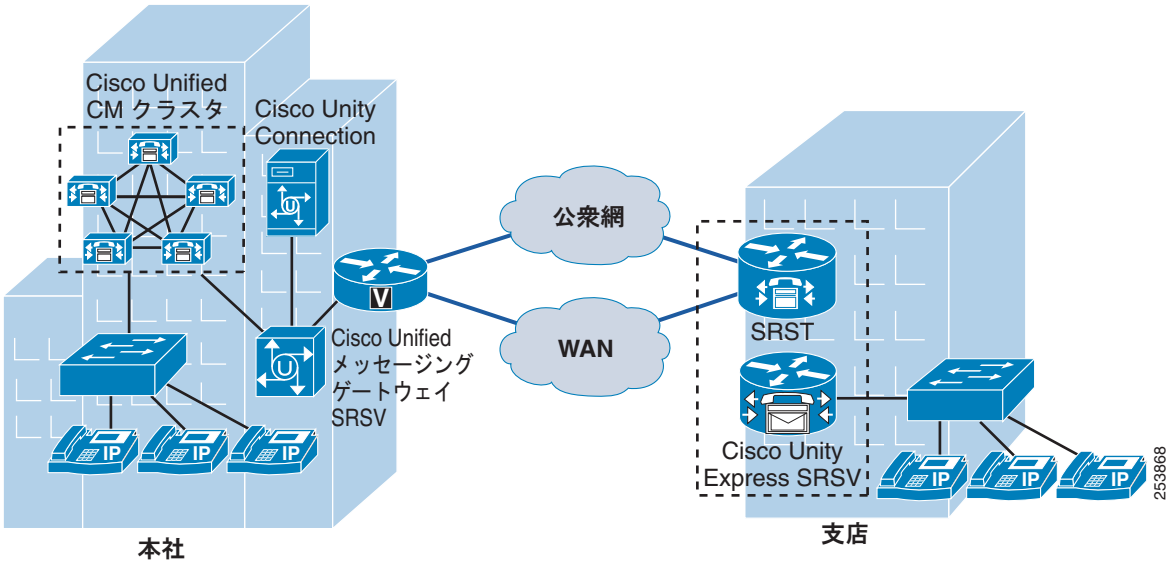
集中メッセージング環境では、WAN がオーバーサブスクリプションの状態になった場合に、Unified CM の機能である Automated Alternate Routing（AAR; 自動代替ルーティング）が、公衆網を介してコールを中央サイトのメッセージング ストアにルーティングできます。ただし、公衆網を介してコールが再ルーティングされる場合、Redirected Dialed Number Information Service（RDNIS）が損なわれることがあります。Cisco Unity または Unity Connection がメッセージング クライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が外線を介して再ルーティングするボイスメール コールに影響が及ぼされることがあります。RDNIS 情報が正しくない場合、コールはダイヤル先のユーザのボイスメール ボックスに到達せず、自動アテンダント プロンプトを受信します。発信者は、到達を試みているユーザの内線番号を再入力するように要求されることがあります。この動作は、主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通

信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合せて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

Survivable Remote Site Voicemail

Survivable Remote Site Voicemail（SRSV）では、集中型メッセージングと集中型コール処理配置において、バックアップ ボイスメール サービスが提供されます。SRSV では、サイト間の接続が利用できない場合に、支店ロケーションにある Cisco Unity Express を利用して、本社にある Cisco Unity Connection に代わるバックアップ ボイスメール サービスを提供します（図 21-2 を参照）。通常の動作において、本社の Cisco Unified Messaging Gateway は設定（SRST 電話機、ユーザ、メールボックスの情報など）を Cisco Unified CM および Cisco Unity Connection から取得し、設定されたスケジュールに基づいて Cisco Unity Express SRSV のメールボックスをプロビジョニングおよび更新します。Cisco Unity Express SRSV は、SRST がアクティブである場合にだけアクティブとなり、それ以外の場合にはアイドルとなります。サイト間のネットワーク接続が復元されると、Cisco Unity Express SRSV から Cisco Unity Connection にすべてのメッセージ（新規メッセージ、保存されたメッセージ、削除されたメッセージなど）がアップロードされます。

図 21-2　一般的な Survivable Remote Site Voicemail 配置



（注）　Survivable Remote Site Telephony（SRST）および Cisco Unity Express SRSV は 1 つの論理ユニットであり、SRST ルータに Cisco Unity Express SRSV がインストールされます。

SRSV では、次のアクティビティを行う場合に WAN リンクの帯域幅が使用されます。

- Unified CM および Cisco Unity Connection から Cisco Unity Express SRSV への設定のアップロード
- WAN リンクが復元された場合の Cisco Unity Express SRSV から Cisco Unity Connection への音声メッセージのアップロード

既存の音声ネットワークへの SRSV トラフィックの影響を最小限に抑えるために、SRSV トラフィック（設定および音声メッセージのアップロード）をベストエフォートとして分類します。SRSV ソフトウェアでは、どのネットワーク パケットもマーキングされません。音声トラフィックやその他の優先順位の高いトラフィックを優先するために、ネットワーク エッジ ルータで SRSV トラフィックを IP Precedence 0（DSCP 0 または PHB BE）とマークすることを推奨します。さらに影響を少なくするために、設定のアップロードはピーク時以外の時間（夜間や週末など）にスケジュールすることを推奨します。スケジュールは、Unified Messaging Gateway SRSV Web インターフェイスで設定できます。

SRSV を配置する場合、次のルールが適用されます。

- Unified Messaging Gateway SRSV では、最大で 1,000 の Cisco Unity Express SRSV ノードがサポートされます。
- SRSV では、Cisco Unified CM Business Edition はサポートされません。
- Cisco Unity Express SRSV は、SRST ルータ、または SRST モードで実行されている Unified CME にインストールします。
- 支店内に複数の SRST ルータを配置することはできますが、各ルータに独自の Cisco Unity Express SRSV が必要です。また、各ルータには 1 つの Cisco Unity Express SRSV だけを設定できます。
- 音声メッセージのアップロードでハイ アベイラビリティを確保するには、冗長な Unified Messaging Gateway SRSV を配置します。Unified Messaging Gateway SRSV では、設定のアップロードにおけるハイ アベイラビリティはサポートされていません。
- Unified Messaging Gateway SRSV と Cisco Unity Express SRSV との間の接続でセキュリティを確保するには、Secure Socket Layer（SSL）プロトコルを使用します。
- SRSV では、Cisco Unity はサポートされていません。

SRSV の詳細については、http://www.cisco.com で入手可能なマニュアルを参照してください。

分散型メッセージングと集中型コール処理

分散型メッセージングは、テレフォニー環境内に複数のメッセージング システムが分散されており、各メッセージング システムがローカル メッセージング クライアントだけにサービスを提供することを意味します。このモデルは集中型メッセージングとは異なります。集中型メッセージングでは、メッセージング システムに対してローカルなクライアントとリモートのクライアントの両方が存在します。

図 21-3 では、集中型コール処理を使用する分散型メッセージング モデルを示しています。他のマルチサイト コール処理モデルと同様に、WAN 帯域幅を管理するためにリージョンとロケーションを使用する必要があります。このモデルでは、Cisco Unity でネイティブ トランスコーディングを無効にする必要もあります。

SRST モードの Cisco Unified Communications Manager Express（Unified CME）は、IP 電話および Cisco Unity または Unity Connection ボイスメール ポートの両方のコール処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 21-3 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップのコール処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity または Unity Connection サーバへのアクセスと MWI のサポートを提供します。SRST モードの Unified CME の詳細については、http://www.cisco.com で入手可能な Unified CME の製品マニュアルを参照してください。

図 21-3　分散型メッセージングと集中型コール処理

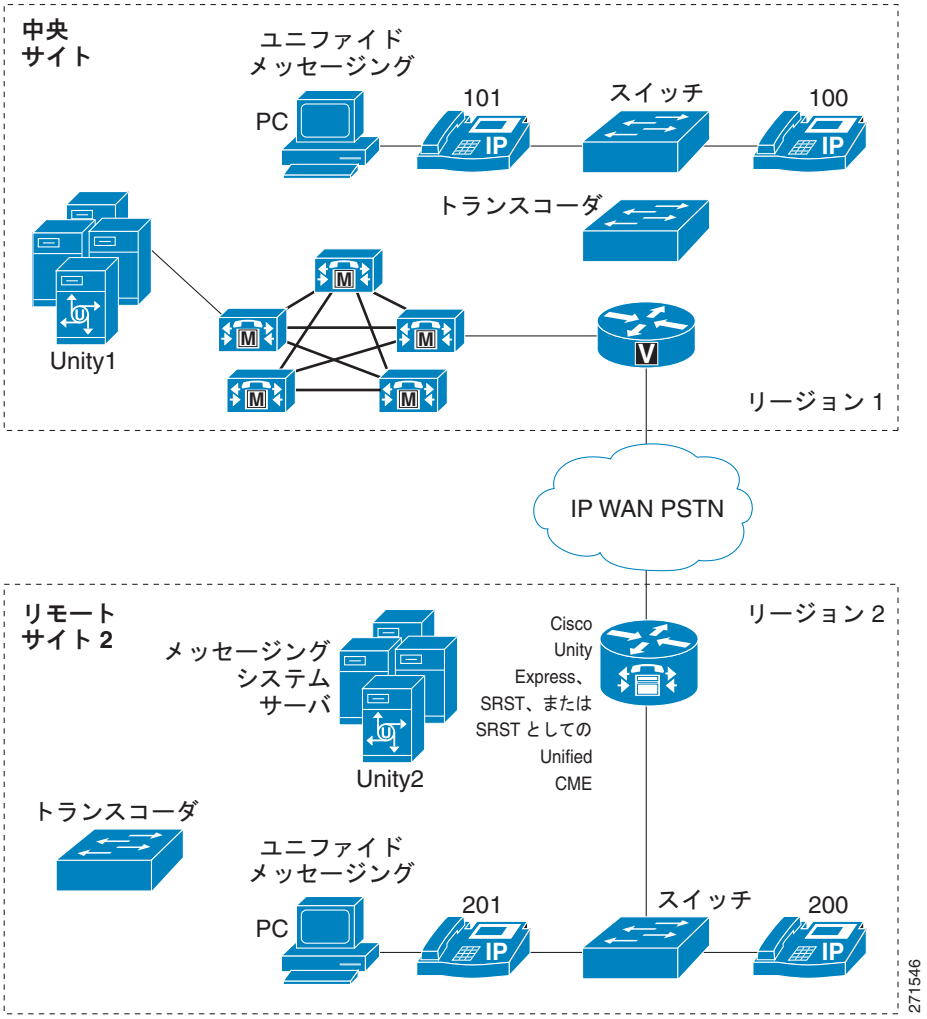


図 21-3 の構成では、トランスコーダ リソースが各 Cisco Unity メッセージ システム サイトに対してローカルである必要があります。リージョン 1 と 2 は、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

Unified CM サーバに設定されているコーリング サーチ スペースとデバイス プールによって、両方の Cisco Unity または Unity Connection サーバの音声メッセージング ポートに、適切なリージョンとロケーションが割り当てられる必要があります。さらに、テレフォニー ユーザをボイスメール ポートの特定のグループに関連付けるために、Unified CM ボイスメール プロファイルを設定する必要があります。コーリング サーチ スペース、デバイス プール、およびボイスメール プロファイルを設定する方法の詳細については、http://www.cisco.com で入手可能な、該当するバージョンの『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

メッセージング システムは相互に「ネットワーク接続」され、内部ユーザと外部ユーザの両方に単一のメッセージング システムを提供します。分散 Unity サーバ向けの Cisco Unity ネットワーク機能については、次の Web サイトで入手可能な『*Networking in Cisco Unity Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html

Cisco Unity Connection では、デジタル ネットワーキングがサポートされており、複数の Cisco Unity Connection システムを相互にネットワーク接続できます。デジタル ネットワーク システムでは、最大で 10 のノード（単一ノードまたはアクティブ/アクティブ ペア）を接続できます。また、必要に応じて 2 つのデジタル ネットワークを結合して、最大で 20 のノードをサポートできます。デジタル ネットワークでは、ディレクトリの最大 100,000 のエンティティがサポートされます。Cisco Unity Connection は、Microsoft Active Directory などの企業ディレクトリに統合して、ユーザを同期化し、デジタル ネットワーキングを同時に使用できます。この設定では、各 Cisco Unity Connection サーバまたはサーバ ペアが、企業ディレクトリから最大 20,000 ユーザを同期化できます。Cisco Unity Connection でのデジタル ネットワーキングまたはディレクトリ統合の詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

Cisco Unity と Unity Connection および SRST モードの Unified CME

SRST モードの Unified CME を使用すると、Cisco Unity サーバと Unity Connection サーバの両方をリモート サイトに置き、中央サイトの Unified CM に登録して、リモート ロケーションにある Unified CME にフォールバックできます。WAN リンクがダウンし、電話機が SRST モードの Unified CME にフェールオーバーすると、Cisco Unity と Unity Connection のボイスメール ポートも SRST モードの Unified CME にフェールオーバーします。これにより、リモートサイトのユーザが、WAN の障害時に、MWI 機能も含めてボイスメールにアクセスできるようになります。

このシナリオには、次の各項目が必要です。

- Cisco Unified CME 4.0 以降
- Cisco Unity 4.0(5) 以降と TSP バージョン 8.1(3) 以降
- Cisco Unity Connection 2.*x* 以降

（注）　Unified CM から SRST モードの Unified CME へ、またはその逆方向にフェールオーバーが発生した場合、Cisco Unity または Unity Connection サーバから MWI を再同期する必要があります。

メッセージング配置モデルの組み合せ

複数のメッセージング モデルを同じ配置で組み合せることができます。ただし、その配置は、上記の項で示したすべてのガイドラインに従う必要があります。図 21-4 では、集中型メッセージングと分散型メッセージングの両方が同時に採用されるユーザ環境を示しています。

図 21-4　結合された配置モデル

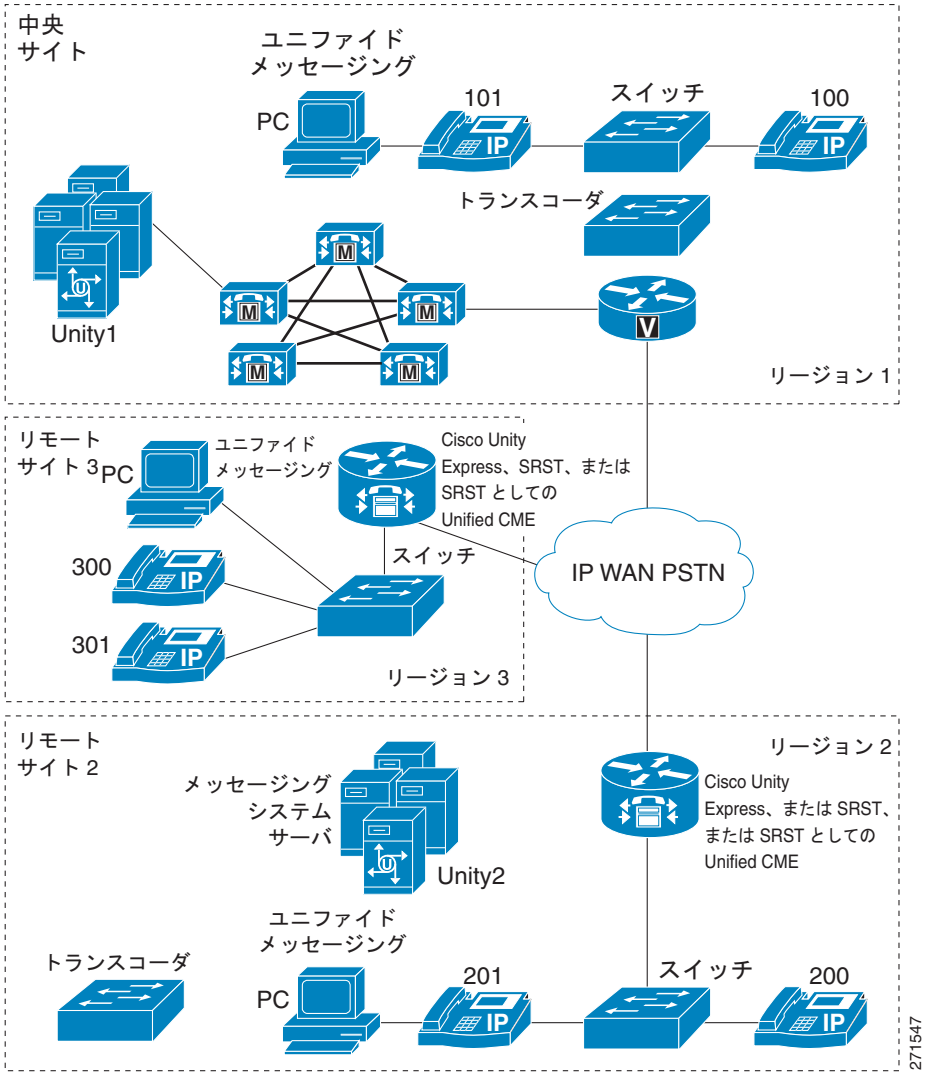


図 21-4 では、2 つのメッセージング モデルの組み合せを示しています。リージョン 1 と 3 は集中型メッセージングと集中型コール処理を使用し、リージョン 2 は分散型メッセージングと集中型コール処理を使用しています。すべてのリージョンが、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 21-4 では、中央サイトとサイト 3 の間で、集中型メッセージングと集中型コール シグナリングが使用されています。中央サイトのメッセージング システムは、中央サイトとサイト 3 の両方のクライアントにメッセージング サービスを提供します。サイト 2 は、集中型コール処理を使用する分散型メッセージング モデルを使用しています。サイト 2 に置かれているメッセージング システム（Unity2）は、サイト 2 の中にいるユーザだけにメッセージング サービスを提供します。この配置では、両方のモデ

ルが、この章に記載されているそれぞれの設計上のガイドラインに従っています。トランスコーディング リソースは各メッセージング システム サイトに対してローカルに置かれ、サイト 2 のユーザが中央サイトのユーザにメッセージを残す場合のように、（メッセージング システムに対して）リモートのサイトからメッセージング サービスにアクセスするクライアントをサポートします。

また、SRST モードの Cisco Unified Communications Manager Express（Unified CME）は、IP 電話および Cisco Unity または Unity Connection ボイスメール ポートの両方のコール処理バックアップに使用されます。このフォールバック サポートは、リモート サイト（たとえば、図 21-4 のリージョン 2）に配置され、WAN 障害などのために電話機と Unified CM との接続が失われた場合に、バックアップのコール処理を提供します。またリモート サイトのユーザに対し、WAN 障害時に、ローカルの Cisco Unity または Unity Connection サーバへのアクセスと MWI のサポートを提供します。SRST モードの Unified CME の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

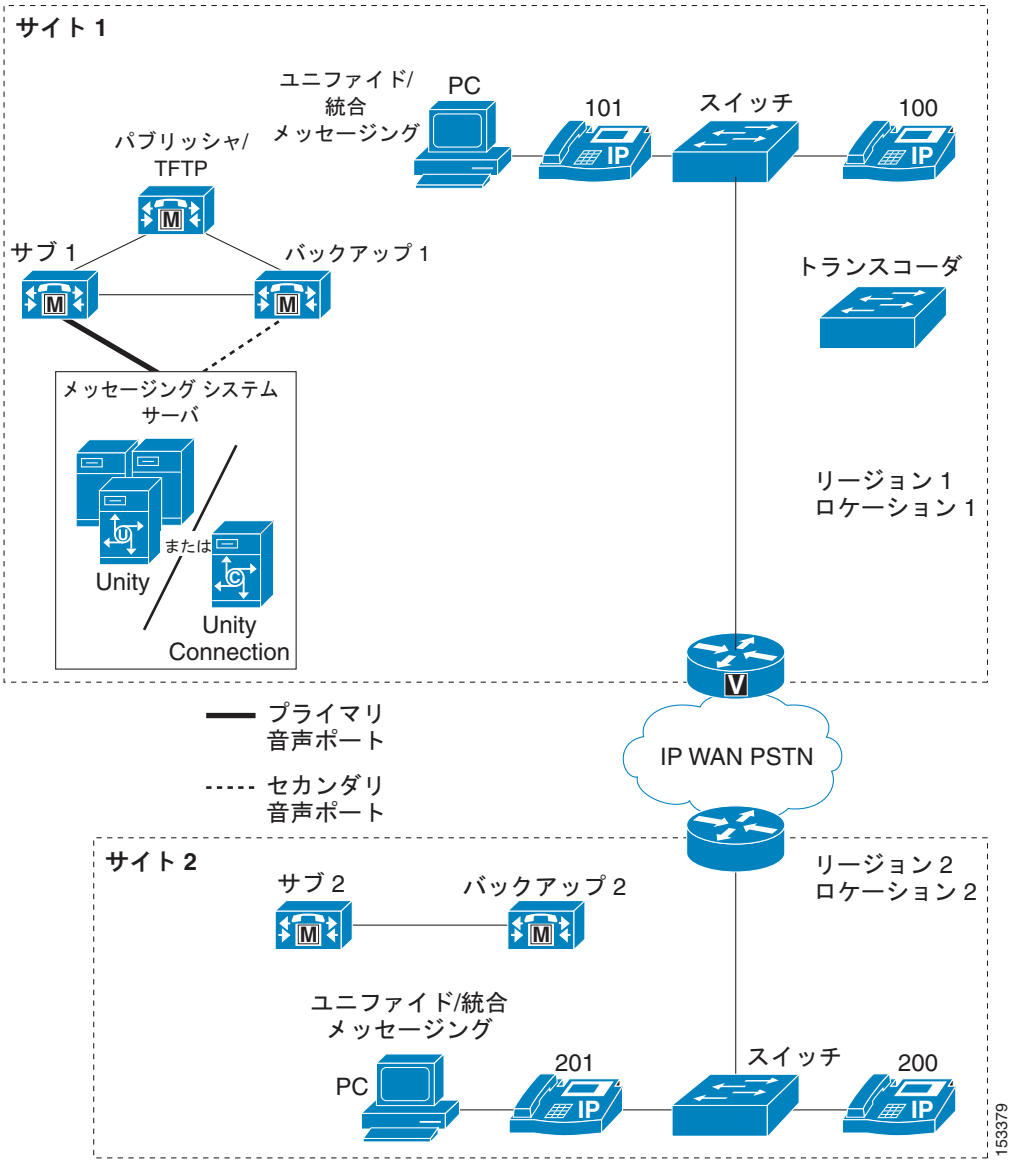
集中型メッセージングと WAN を介したクラスタリング

ここでは、集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介した Unified CM クラスタリングを一緒に配置する場合の Cisco Unity の設計上の問題について説明します。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、すべてのリモート メッセージング サイトがボイスメール機能を失います（図 21-5 を参照）。

WAN を介したクラスタリングは、ローカル フェールオーバーをサポートしています。ローカル フェールオーバーでは、各サイトが、物理的にそのサイトに置かれているバックアップ サブスクライバ サーバを持ちます。ここでは、Cisco Unity 集中型メッセージングと、WAN を介したクラスタリングのローカル フェールオーバーを一緒に配置する方法を中心に説明します。

詳細については、「IP WAN を介したクラスタリング」（P.5-46）の項を参照してください。

図 21-5　Cisco Unity 集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタリング



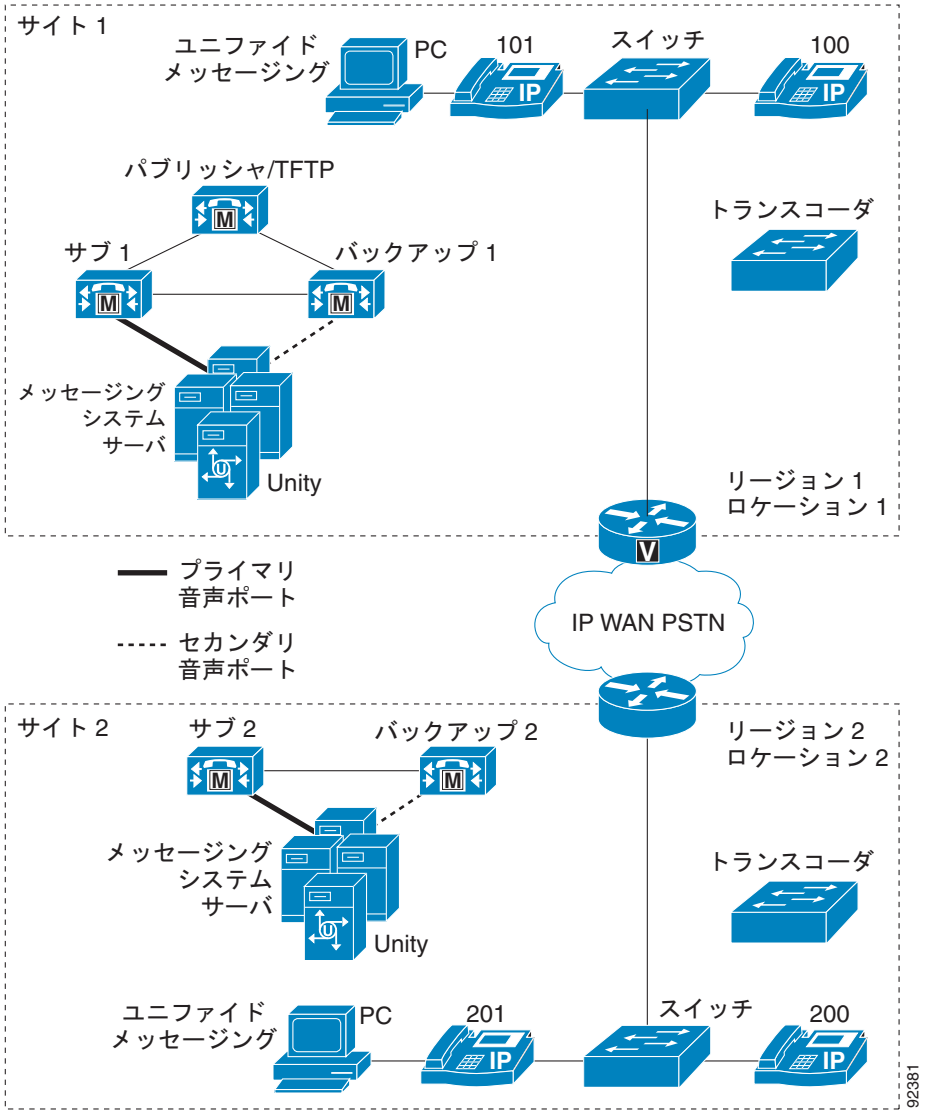
クラスタリングされたサーバ間の最小帯域幅の要求については、「ローカル フェールオーバー配置モデル」（P.5-51）の項を参照してください。

Unified CM による WAN 経由のクラスタリングでは、Cisco Unity と同様、最大 8 サイトがサポートされます。ボイスメール ポートは、Cisco Unity メッセージング システムが置かれているサイトだけに設定されます（図 21-5 を参照）。ボイスメール ポートは、WAN を介してリモート サイトに登録されません。他のサイトのメッセージング クライアントは、プライマリ サイトのすべてのボイスメール リソースにアクセスします。WAN に障害が発生すると、リモート サイトは集中型メッセージング システムにアクセスできなくなるため、WAN を介してリモート サイトに音声ポートを設定してもメリットがありません。ユニファイド メッセージングの場合、帯域幅を考慮して、ボイスメール ポートで TRaP を無効にし、すべてのメッセージング クライアントがそのローカル PC にボイスメール メッセージをダウンロードするようにする必要があります。

分散型メッセージングと WAN を介したクラスタリング

Cisco Unity メッセージング サーバも配置されたローカル フェールオーバー サイトでは、集中型メッセージング モデルと同様に、音声ポートがローカル Unified CM サブスクライバ サーバに登録されます。音声ポートの設定については、「Unified CM クラスタとの音声ポート統合」（P.21-42）および「専用 Unified CM バックアップ サーバを使用する音声ポート統合」（P.21-44）を参照してください。

図 21-6　Cisco Unity 分散型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタリング



WAN を介したクラスタリングを含む単純分散型メッセージング実装では、クラスタ内の各サイトに、独自の Cisco Unity メッセージング サーバとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのサイトにローカル Cisco Unity メッセージング システムが置かれるわけではなく、一部のサイトで、ローカル メッセージング クライアントがリモート メッセージング サーバを使用する場合、その配置は分散型メッセージングと集中型メッセージングの組み合せモデルとなります

（「メッセージング配置モデルの組み合せ」（P.21-14）を参照）。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、集中型メッセージングを使用するすべてのリモート サイトがボイスメール機能を失います。

ローカル メッセージング サーバを持たない各サイトは、そのすべてのメッセージング クライアントに対して単一のメッセージング サーバを使用する必要がありますが、そのようなサイトのすべてが同じメッセージング サーバを使用する必要はありません。たとえば、サイト 1 とサイト 2 のそれぞれがローカル メッセージング サーバを持っているとします。その場合、サイト 3 のすべてのクライアントがサイト 2 のメッセージング サーバを使用し（そのメッセージング サーバに登録し）、サイト 4 のすべてのクライアントがサイト 1 のメッセージング サーバを使用するようにできます。ローカル Cisco Unity メッセージング サーバを持つサイトには、トランスコーダ リソースが必要です。

他の分散型コール処理配置と同様に、これらのサイト間のコールはゲートキーパー コール アドミッション制御にとって透過的です。したがって、Unified CM でリージョンとロケーションを設定してコール アドミッション制御を提供する必要があります（「帯域幅の管理」（P.21-35）を参照）。

分散配置された Cisco Unity サーバは、デジタルでネットワーク接続することもできます。このトピックの詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Networking Guide*』を参照してください。配置される特定のメッセージング ストアに固有の Networking Guide が用意されています。

メッセージングの冗長性

ここでは、Cisco Unity と Cisco Unity Connection に関するメッセージングの冗長性について説明します。Cisco Unity Express は、メッセージングの冗長性をサポートしていません。

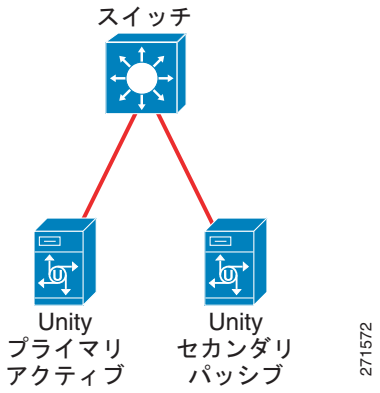
Cisco Unity

Cisco Unity は、2 種類の冗長性をサポートしています。1 つめは単純に Unity フェールオーバー（ローカル メッセージング フェールオーバー）と呼ばれ、システム障害のフェールオーバーが提供されます。2 つめは、スタンバイ冗長性と呼ばれ、地理的な複数の場所にわたるディザスタ リカバリ機能を提供します。Cisco Unity フェールオーバーとスタンバイ冗長性の比較については、『*Cisco Unity Design Guide*』を参照してください。

Cisco Unity フェールオーバーは、プライマリとセカンダリの 2 台のサーバがアクティブ / パッシブ冗長ペアとして設定されます。プライマリ サーバはアクティブの状態でコールを受け付け、セカンダリは非アクティブでコールを受け付けません。プライマリ サーバでサブスクライバや設定に関するデータを変更されると、その変更内容がセカンダリ サーバに自動的に複製されます。何らかの理由でプライマリ サーバが機能しなくなった場合、セカンダリ サーバが自動的にアクティブ サーバになりコールの受け付けを開始します。その間、プライマリ サーバは一時的に非アクティブになります。

図 21-7 に示しているように、ローカル メッセージング フェールオーバーを実装できます。ローカル フェールオーバーでは、プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。

図 21-7　Cisco Unity メッセージングのローカル フェールオーバー



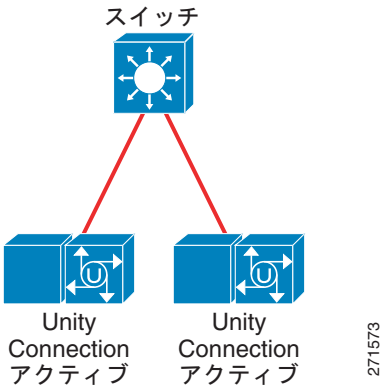
Cisco Unity Standby Redundancy はまた、地理的な複数の場所にわたるディザスタ リカバリ機能も提供します。この場合もプライマリとセカンダリの 2 台のサーバを使用しますが、それらは通常、別の都市にある異なるデータセンターにインストールされます。プライマリ サーバがインストールされたデータセンターが自然災害やその他の大規模災害に遭遇した場合、ディザスタ リカバリ設備にいる（またはリモートでアクセスできる）誰かが、セカンダリ サーバを手動でアクティブ化すると、セカンダリ サーバがコールの受付を開始します。スタンバイ冗長性またはフェールオーバー（ローカル メッセージング フェールオーバー）の要件に関する詳細については、http://www.cisco.com で入手できる適切なバージョンの『*System Requirements for Cisco Unity*』を参照してください。

Cisco Unity Connection

Cisco Unity Connection は、プライマリとセカンダリの 2 台のサーバをアクティブ/アクティブのサーバ ペアに設定したアクティブ/アクティブ冗長モデルで、メッセージング冗長性とロード バランシングをサポートします。アクティブ/アクティブ冗長モデルでは、プライマリとセカンダリの両方のサーバが、コールおよび HTTP 要求と IMAP 要求をアクティブに受け付けます。詳細については、http://www.cisco.com で入手できる『*Design Guide for Cisco Unity Connection*』を参照してください。

図 21-8 は、Cisco Unity Connection のアクティブ/アクティブ メッセージング冗長性を示します。

図 21-8　Cisco Unity Connection メッセージングの冗長性



Cisco Unity と Cisco Unity Connection の SIP トランクの実装には、いずれもメッセージング冗長機能のためのコール分岐（転送）が必要です。現在、Unified CM が SIP トランクのコールの分岐（転送）をサポートしていないため、Unified CM で SIP トランクが使用されている場合、Cisco Unity フェールオーバーは利用できません。ただし、アクティブ/アクティブ冗長性の Cisco Unity Connection サーバ

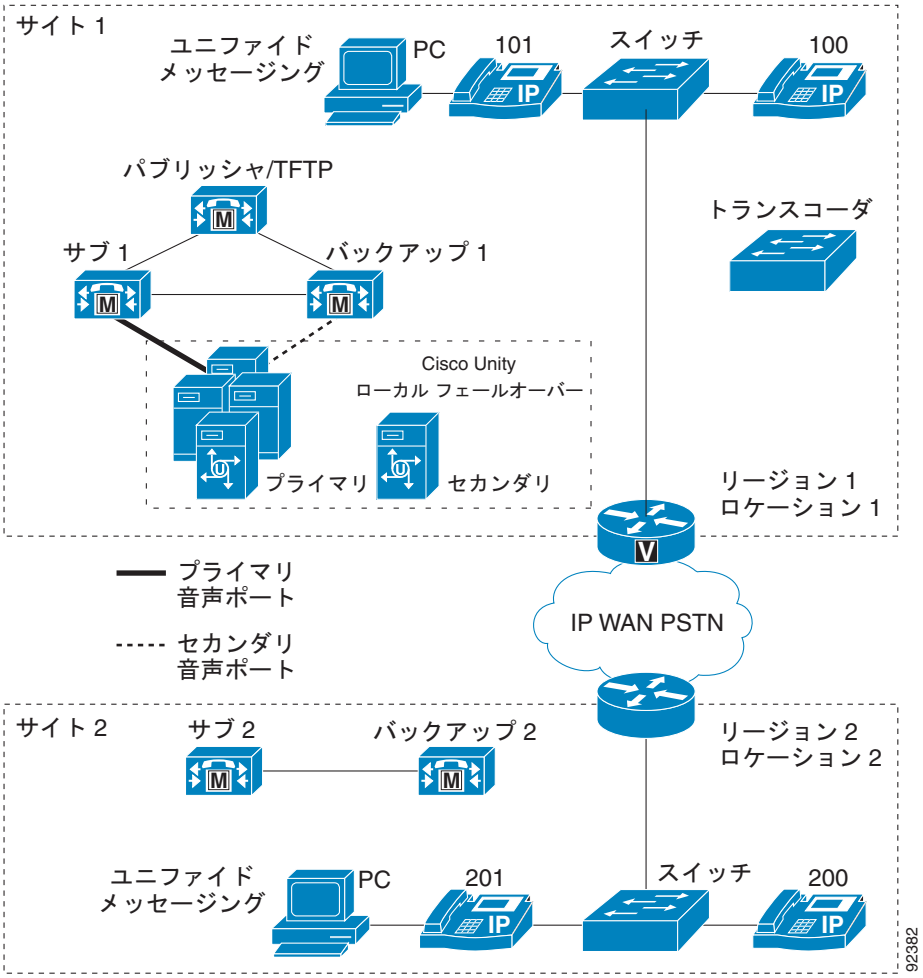
ペアで SIP トランクを使用している場合は、2 つの異なる SIP トランクをサーバ ペアの各サーバに 1 つずつ設定し、それらを同じルート リストに関連付けられた同じルート グループに追加することを推奨します。この設定では、Unified CM から 2 台のサーバに対するロード バランシング コールが可能です。

Cisco Unity フェールオーバーと WAN を介したクラスタリング

Cisco Unity ローカル フェールオーバーと WAN を介したクラスタリングを配置する場合は、「集中型メッセージングと WAN を介したクラスタリング」（P.21-15）および「分散型メッセージングと WAN を介したクラスタリング」（P.21-17）で説明している設計プラクティスを適用します。正常な動作時、プライマリ Cisco Unity サーバからの音声ポートは WAN を通過しません。

図 21-9 では、Cisco Unity ローカル フェールオーバーを示しています。プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が物理的に同じサイトに置かれていることに注意してください。Cisco Unity フェールオーバーは、Unified CM の WAN を介したクラスタリングで使用可能な最大数までリモート サイトをサポートします。

図 21-9　　Cisco Unity ローカル フェールオーバーと WAN を介したクラスタリング



Cisco Unity フェールオーバーの設定については、http://www.cisco.com で入手できる『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

離れたデータセンターに配置された Cisco Unity のフェールオーバー

すでに述べたように、WAN 経由のハイ アベイラビリティを運用するために Cisco Unity フェールオーバーを設定できますが、この配置にはいくつかの要件があります。たとえば、地理的に離れた複数のデータセンターでの完全な冗長性が重要な場合、この設定でインストール操作を成功させるために、満たすべき特定の要件があります。図 21-10 に、地理的に離れたデータセンターにおける Cisco Unity のフェールオーバーを示します。

図 21-10　地理的に離れたデータセンターにおける Cisco Unity のフェールオーバー

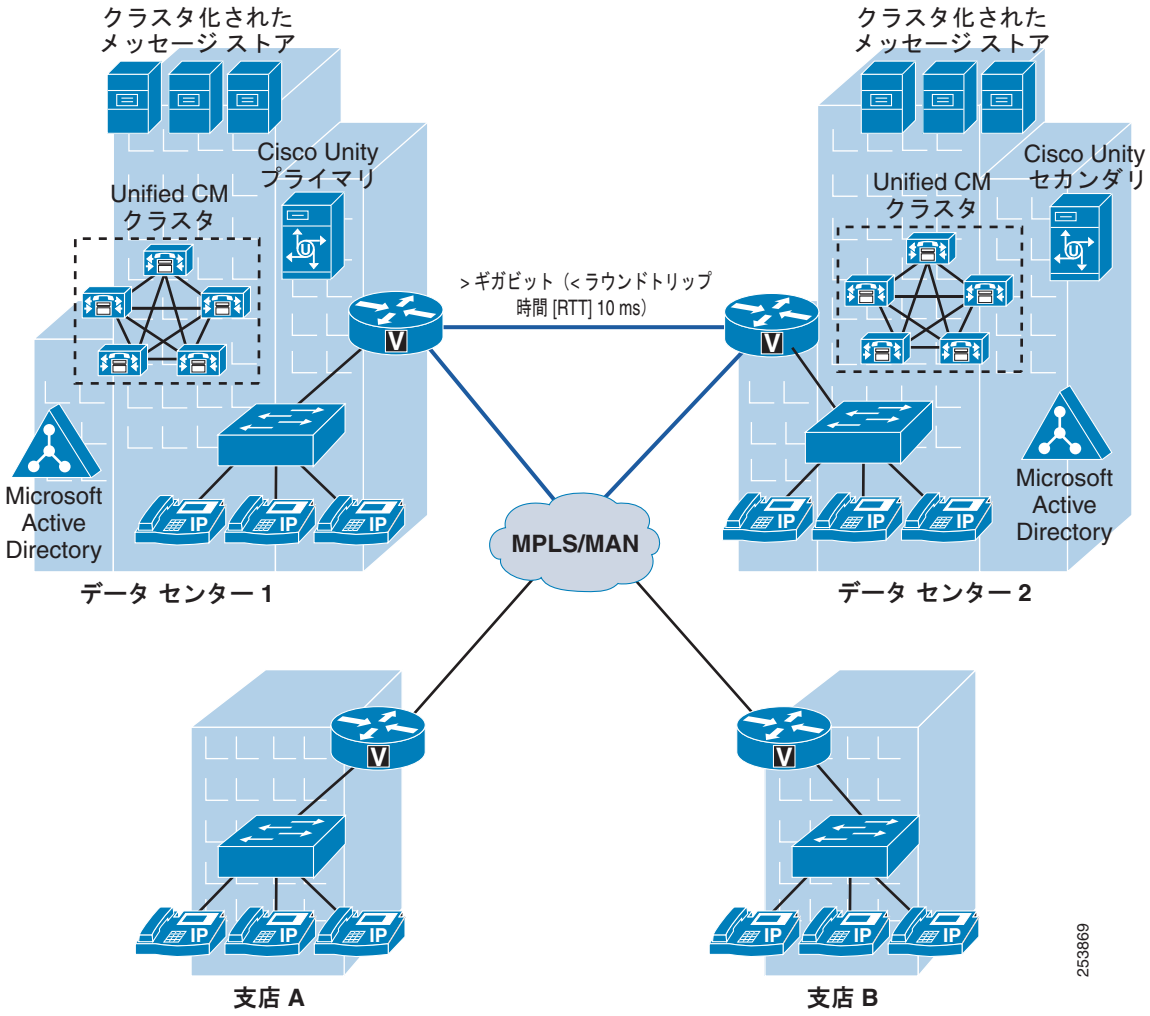


図 21-10 に示す設定には、次の要件が適用されます。

- プライマリとセカンダリの Cisco Unity サーバ間の最大 Round Trip Time（RTT; ラウンドトリップ時間）は 10 ms
- 最低 1 ギガビットの帯域幅
- Cisco Unity サーバおよび各メッセージング サーバとの間の最大 RTT は 10 ms
- Cisco Unity サーバおよびドメイン コントローラまたはグローバル カタログ サーバは同じ場所に設置

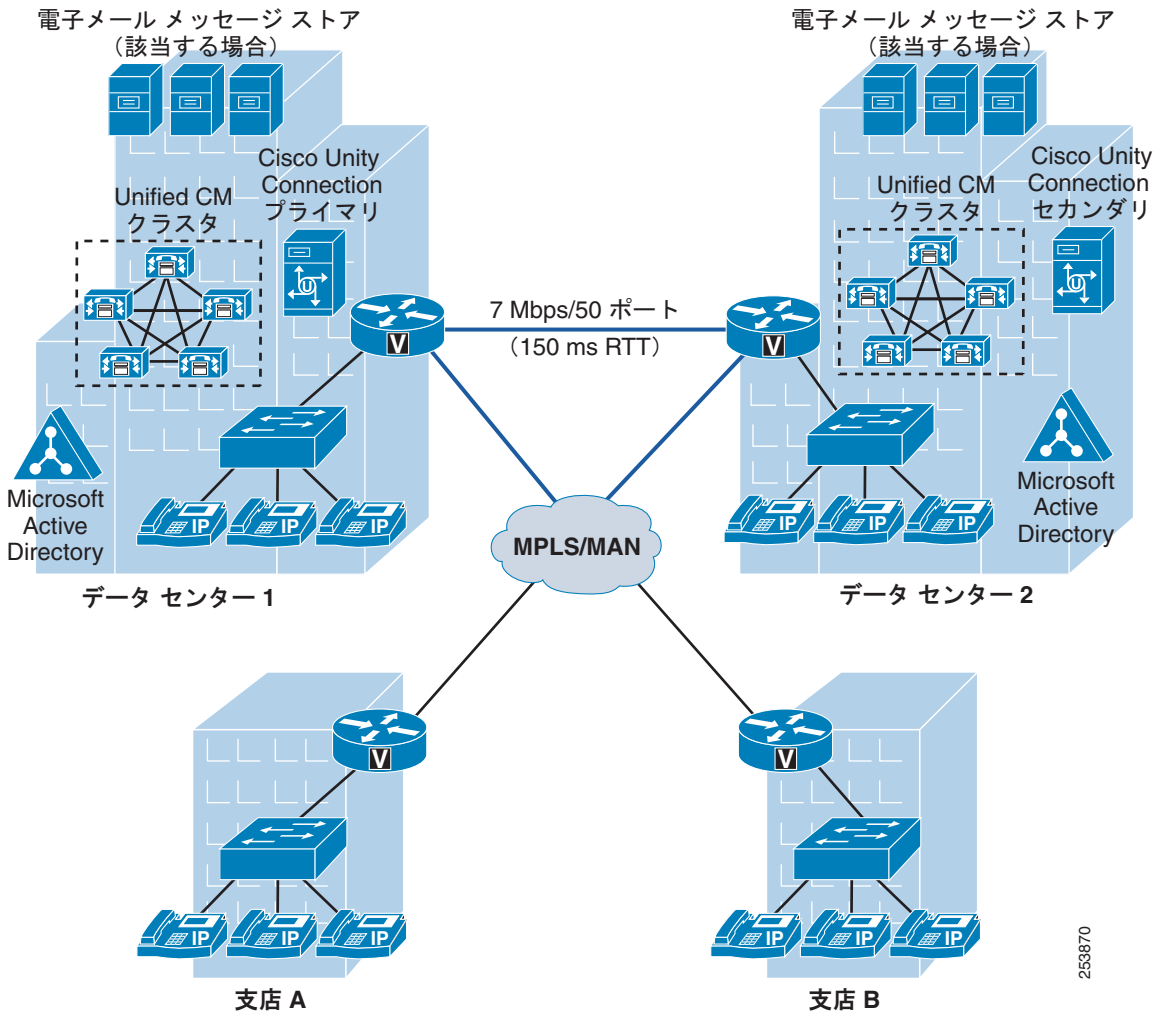
すべての要件の詳細については、次の Web サイトで入手可能な『*System Requirements for Cisco Unity*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_installation_guides_list.html

WAN 経由での Cisco Unity Connection の冗長性とクラスタリング

Cisco Unity Connection では、アクティブ/アクティブ型のクラスタリングを使用した冗長性がサポートされており、WAN 経由で配置できます。アクティブ/アクティブ設定、つまり「ハイ アベイラビリティ」設定では、ハイ アベイラビリティと冗長性の両方が提供されます。アクティブ/アクティブ ペアの両方のサーバでは Cisco Unity Connection アプリケーションが実行され、コールおよびクライアントからの HTTP 要求や IMAP 要求を受け付けます。クラスタの各サーバは、WAN 経由で異なるサイトに配置できます。その場合、以降に示す設計上の考慮事項に従う必要があります。図 21-11 に、地理的に離れたデータセンターにおける Cisco Unity Connection のアクティブ/アクティブ配置を示します。

図 21-11　　2 つのサイト間でハイ アベイラビリティが確保された Cisco Unity Connection



異なるサイトに Cisco Unity Connection サーバを配置した場合には、次の要件が適用されます。

- 異なるサイトにあるアクティブ/アクティブ ペア間の最大 RTT は 150 ms
- 50 ポートごとに最低 7 Mbps の帯域幅が必要（たとえば、250 ポートでは 35 Mbps が必要）

（注）　帯域幅および遅延の要件は、Cisco Unity Connection のバージョンによって異なることがあります。

すべての要件の詳細については、次の Web サイトで入手可能な『*System Requirements for Cisco Unity Connection*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps6509/prod_installation_guides_list.html

（注）　Cisco Unity Connection クラスタ機能は、Cisco Unified Communications Manager Business Edition 3000 および 5000 とともに使用することはできません。

集中型メッセージングと分散型 Unified CM クラスタ

Cisco Unity および Unity Connection は、複数の Unified CM クラスタによる集中型メッセージング設定に配置することもできます（図 21-12 を参照）。複数統合および 複数の Unified CM クラスタに伴う MWI の考慮事項の詳細については、「テレフォニー統合」（P.21-39）の項を参照してください。

図 21-12　Cisco Unity または Unity Connection と複数の Unified CM クラスタの統合

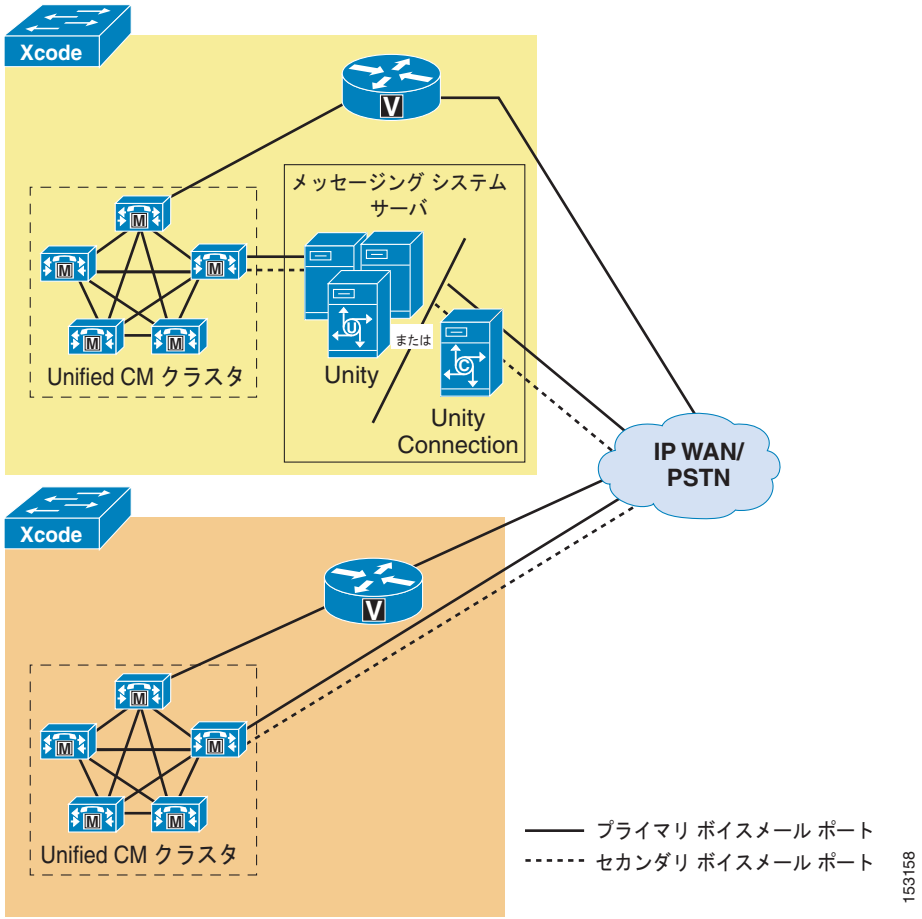


図 21-12 の設定では、クラスタ 1 とクラスタ 2 の両方のサイトのメッセージング クライアントが、物理的にクラスタ 1 に置かれている Cisco Unity または Unity Connection メッセージング インフラストラクチャを使用します。

Cisco Unity Express の配置モデル

ここではまず、Cisco Unity Express を概観し、製品に関する情報を提供します。次に、配置モデルについての項では、集中型と分散型の両方のコール処理における分散型音声メッセージングを中心に、Cisco Unity Express に関してサポートされている 3 つの配置モデルを紹介し、次いで配置の特徴と設計ガイドラインを示します。最後に、Cisco Unity Express と Unified CM、さらには Cisco Unity Express と Unified SRST または SRST モードの Unified CME の間で使用されるシグナリング コール フローとさまざまなプロトコルについて説明します。

Cisco Unity Express の概要

Cisco Unity Express は、Cisco Integrated Services Router（ISR; サービス統合型ルータ）の Cisco ネットワーク モジュール上で実行される Linux ベースのソフトウェアです。Cisco Unity Express は、Cisco Unified Communications Manager（Unified CM）、Cisco Unified SRST、または Cisco Unified Communications Manager Express（Unified CME）とともに配置できる、エントリレベルの Auto-Attendant（AA; 自動応答）およびボイスメール ソリューションです。以前のリリースでは、Cisco Unity Express は Unified CME または Survivable Remote Site Telephony（SRST）ルータとの共存配置に限定されていました。ただし、Cisco IOS Release 12.3(11)T で H.323-to-SIP コール ルーティング機能が導入されたため、Unified CM または Unified CME とともに配置する場合に、Cisco Unity Express と SRST または Unified CME を 2 つの異なるルータに配置できるようになりました。Cisco Unity Express は、SIP を使用して Cisco Unified Communications Manager Express（Unified CME）と通信し、JTAPI を使用して Cisco Unified Communications Manager（Unified CM）に接続します。

Cisco Unity Express のサポートされているハードウェア プラットフォームおよび容量の詳細については、http://www.cisco.com/en/US/products/sw/voicesw/ps5520/prod_release_notes_list.html で入手可能な製品リリース ノートを参照してください。

Unified CM と Unified CME の相互運用性の詳細については、「Unified CM と Unified CM Express の相互運用性」（P.8-54）を参照してください。

Unified CME でサポートされている配置モデルの詳細については、http://www.cisco.com で入手可能な Cisco Unified Communications Manager Express の設計に関する資料を参照してください。

配置モデル

Cisco Unity Express は、単一のサイトとして配置することも、Cisco Unified Communications Manager（Unified CM）または Unified Communications Manager Express（Unified CME）の分散型ボイスメールおよび自動応答（AA）ソリューションとして配置することもできます。ただし、Cisco Unity Express は、次のようなすべての Cisco Unified CM 配置モデルでサポートされます。

- 単一サイト配置
- 集中型コール処理を使用するマルチサイト配置
- 分散型コール処理を使用するマルチサイト配置

図 21-13 は、Cisco Unity Express を統合した集中型コール処理配置を、図 21-14 は、分散型コール処理配置を示しています。

Unified CME によって制御される Cisco Unity Express サイト、および Unified CM によって制御されるその他のサイトは、H.323 または SIP トランキング プロトコルを使用して相互接続できます。Cisco Unity Express は Unified CM または Unified CME のいずれかと統合できますが、両方と同時に統合はできません。

（注）　Cisco Unity Express は、最大 10 の Unified CME を持つ集中型配置モデルをサポートします。

図 21-13　集中型コール処理配置における Cisco Unity Express

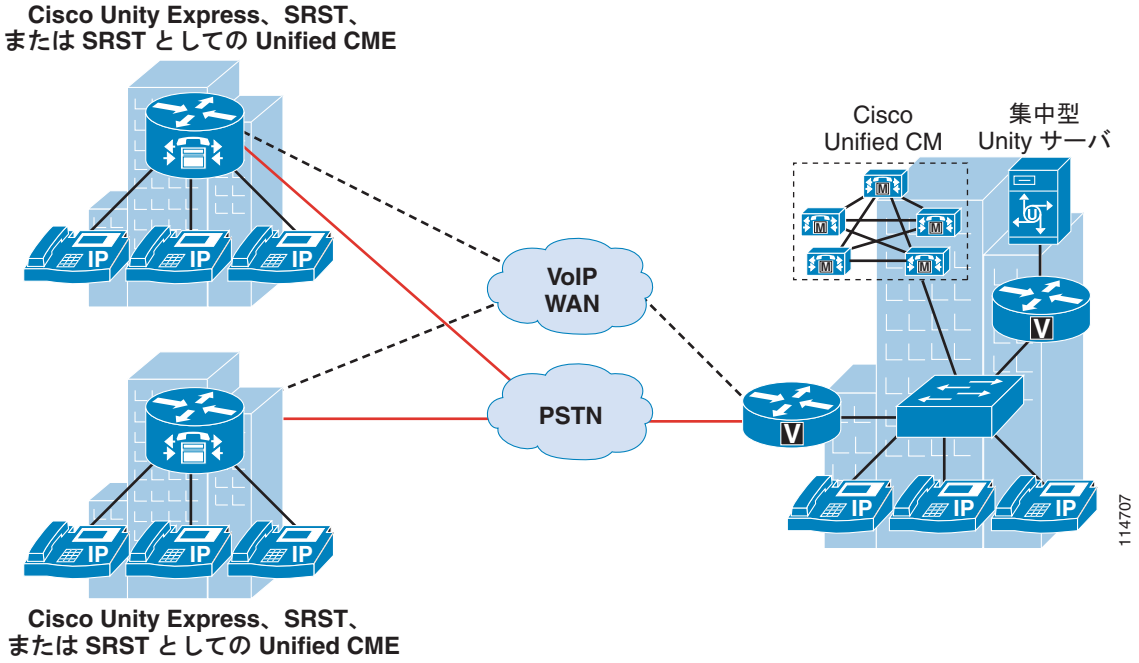
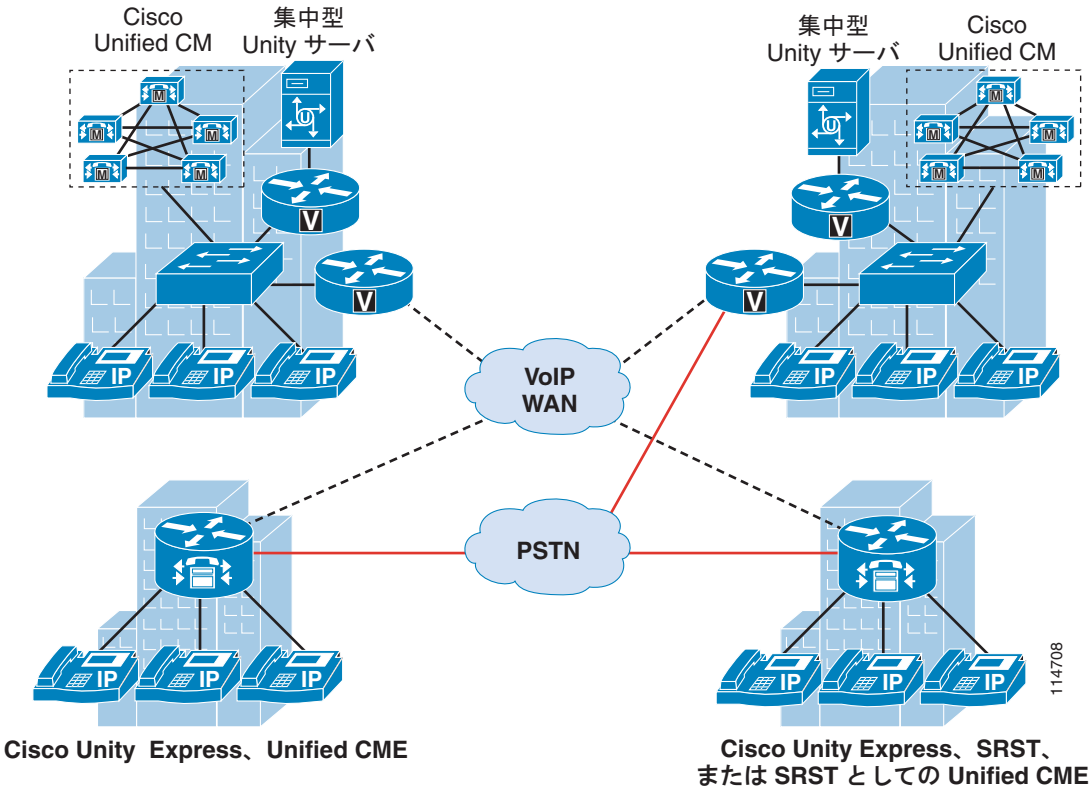


図 21-14　分散型コール処理配置における Cisco Unity Express



Cisco Unity Express を使用した最も一般的な配置モデルは、集中型コール処理を使用したマルチサイト WAN モデルです。このモデルでは、Cisco Unity Express が、小規模なリモート オフィスでボイスメール機能を提供し、中央の Cisco Unity システムが本社および大規模なリモート サイトにボイスメール機能を提供します。

Unified CM ネットワーク配置に次の条件のいずれかが該当する場合は、分散型ボイスメール ソリューションとして Cisco Unity Express を使用してください。

- WAN の可用性にかかわらず、ボイスメールと AA アクセスのサバイバビリティを確保する必要がある。
- 利用可能な WAN の帯域幅が不十分なために、WAN を介して中央のボイスメール サーバにアクセスするボイスメール コールがサポートできない。
- ローカル コミュニティに対して割り当てられている AA または 支店サイトの公衆網の電話番号のカバレッジが地域的に制限されているため、市外通話料金を支払わずにこれらの番号をダイヤルして中央の AA サーバに接続できない。
- 公衆網を使用して支店にかけた場合、コールが支店の AA から同じ支店内の内線番号に転送される可能性が高い。
- 経営理念上、リモート オフィスが、独自のボイスメールや AA テクノロジーを選択することを許可されている。

集中型または分散型の Unified CM 配置では、Cisco Unity Express に対して次の特徴とガイドラインが適用されます。

- 単一の Cisco Unity Express は、単一の Unified CM クラスタに統合できます。

- Cisco Unity Express は、JTAPI アプリケーションと Computer Telephony Integration（CTI; コンピュータ テレフォニー インテグレーション）Quick Buffer Encoding（QBE）プロトコルを使用して、Unified CM に統合できます。CTI ポートと CTI ルート ポイントは、Cisco Unity Express ボイスメールと自動応答（AA）アプリケーションを制御します。
- Cisco Unity Express は、Skinny Client Control Protocol（SCCP）を実行する Cisco Unified IP Phone に、ボイスメール機能を提供します。Cisco Unity Express 2.3 以降のリリースは、Unified CM を使用した Session Initiation Protocol（SIP; セッション開始プロトコル）の IP 電話もサポートします。
- Cisco Unity Express 対応の Unified CM には、次の CTI ポートが定義されています。
  - 自動応答機能エントリ ポイント（Cisco Unity Express は、最大 5 つの異なる AA を設定できるので、ルート ポイントも最大 5 つまで必要になることがあります）
  - ボイスメールのパイロット番号
  - グリーティング管理システム（GMS）パイロット番号（オプション。GMS を使用しない場合は、このルート ポイントを定義する必要はありません）
- Unified CM 上で Cisco Unity Express にサポートされる CTI ポートとメールボックスの数は、ハードウェア プラットフォームによって異なります。詳細については、次の URL から入手できる Cisco Unity Express のデータ シートを参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps5520/products_data_sheets_list.html
- サポートされている最大数より多くのメールボックスが必要な Cisco Unity Express 配置では、Cisco Unity またはその他のボイスメール ソリューションを使用することを検討してください。
- 各 Cisco Unity Express メールボックスは、必要に応じて最大 2 つの異なる内線に関連付けることができます。
- Cisco Unity Express と共に配置されたオフィスでは、自動応答機能をそのオフィスに置くことも（Cisco Unity Express の AA アプリケーションを使用）、中央サイトに置くことも（ボイスメールのみに Cisco Unity Express を使用）できます。
- Cisco Unity Express は、Voice Profile for Internet Mail (VPIM) version 2 経由で、他の Cisco Unity Expresses または Cisco Unity とネットワーク接続できます。これにより、Cisco Unity Express サブスクライバは、別のリモート Cisco Unity Express または Cisco Unity サブスクライバとの間で、メッセージの送受信や転送を行うことができます。
- Cisco Unity Express では、フェールオーバー用の Unified CM を最大 3 つまで指定できます。3 つの Unified CM のいずれにも IP 接続できなくなった場合、Cisco Unity Express は、Survivable Remote Site Telephony（SRST）コール シグナリングに切り替えて、AA 応答サービス、IP 電話へのメールボックス アクセス、および支店に着信する公衆網コールを提供します。
- Cisco Unity Express の自動応答機能は、内線によるダイヤルと名前によるダイヤルの機能をサポートしています。内線によるダイヤルの操作では、発信側が、ネットワーク内の任意のユーザ エンドポイントにコールを転送できます。名前によるダイヤル操作では、Cisco Unity Express 内部のディレクトリ データベースを使用し、外部の LDAP や Active Directory データベースとのインタラクションを行いません。
- Unified CM を使用した集中型 Cisco Unity Express はサポートされていません。
- Cisco Unity Express は、SIP 電話を制御する Cisco Unified CM や Unified CME がない純粋な SIP ネットワークではサポートされません。
- Cisco Unity Express は、Unified CME または SRST ルータ、あるいは公衆網ゲートウェイと別のルータ上に配置できます。
- Unified CME または SRST 以外のルータ上に Cisco Unity Express を配置する場合、コマンド、**allow-connections h323 to sip** を使用して H.323 から SIP へのルーティングを行います。

図 21-15 は、Unified CM と Cisco Unity Express の間のコール フローに関係するプロトコルを示します。

図 21-15　Cisco Unity Express と Unified CM の間で使用されるプロトコル

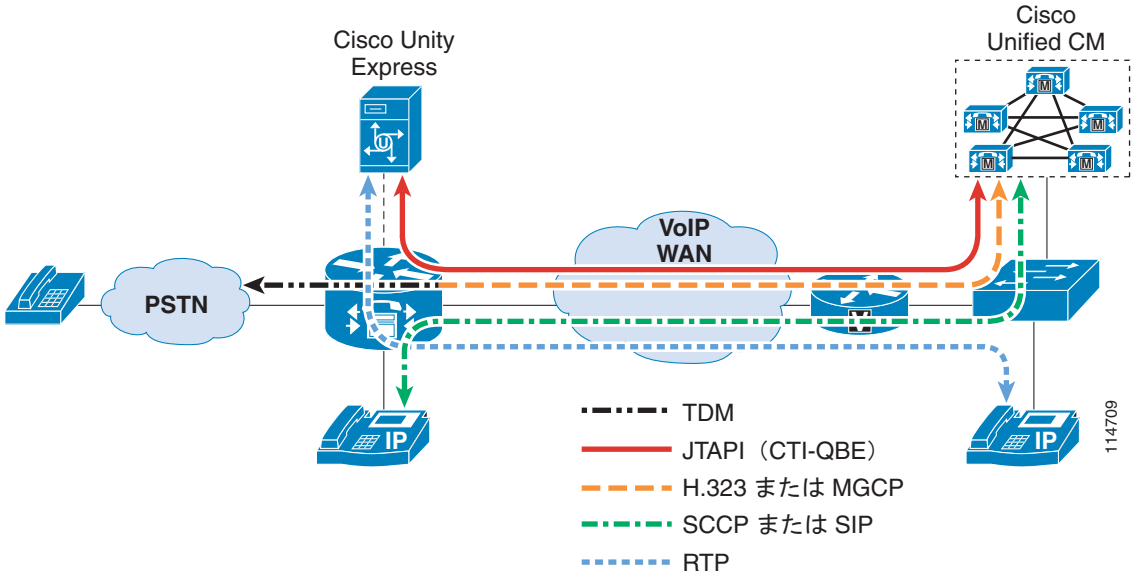


図 21-15 は、次のシグナリングとメディア フローを示しています。

- 電話機は、Unified CM から SCCP または SIP を介して制御されます。
- Cisco Unity Express は、Unified CM から JTAPI（CTI-QBE）を介して制御されます。
- 電話機の Message Waiting indicator（MWI; メッセージ待機インジケータ）は、メールボックスの内容の変化を CTI-QBE 経由で Unified CM に伝達する Cisco Unity Express と、それに対してランプの状態変更の MWI メッセージを電話機に送信する Unified CM によって制御されます。
- 音声ゲートウェイは、H.323、SIP、または MGCP 経由で Unified CM と通信します。
- Real-Time Transport Protocol（RTP）ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。

図 21-16 は、WAN リンクがダウンした場合に、SRST または SRST モードの Unified CME のルータと Cisco Unity Express の間のコール フローに関係するプロトコルを示しています。

図 21-16　Cisco Unity Express と SRST または SRST モードの Unified CME のルータの間で使用されるプロトコル

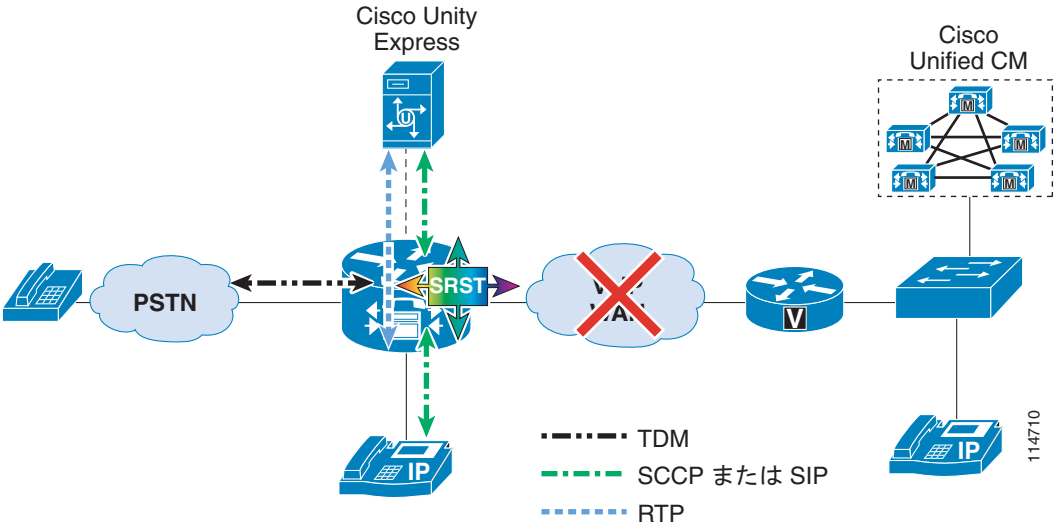


図 21-16 は、次のシグナリングとメディア フローを示しています。

- 電話機は、SRST または SRST モードの Unified CME のルータから SCCP または SIP 経由で制御されます。
- Cisco Unity Express は、内部 SIP インターフェイス経由で SRST ルータと通信します。
- 以前のリリースの Cisco Unity Express では、SRST モードでの MWI の変更はサポートされていませんが、通常動作で音声メッセージを送信および検索できます。しかし、Unified CM に電話機を再登録するまで、電話機の MWI ランプはそのままです。その時点で、すべての MWI ランプの状態が、ユーザの Cisco Unity Express ボイスメール ボックスの現在の状態に自動的に再同期されます。Cisco Unity Express 3.0 以降のリリースでは、SRST モードで MWI がサポートされています。
- Cisco Unity Express では、SIP Subscriber/Notify および Unsolicited Notify がサポートされており、MWI 通知を Unified CME モードと SRST モードの両方で生成できます。
- RTP ストリーム フローは、エンドポイント間の音声トラフィックを搬送します。
- SRST は、MWI 通知を受信するように登録された 各 ephone-dns の MWI について、Cisco Unity Express にサブスクライブします。

（注）　Unified CM MWI（JTAPI）は、SIP MWI 方式に依存しません。

ボイスメール ネットワーキング

この項では、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express を含むボイスメール ネットワーキングに関する留意点について説明します。また、Cisco Unified Messaging Gateway を使用したボイスメール ネットワーキングの概要についても説明します。Cisco Unity または Cisco Unity

Connection のボイスメール ネットワーキングに固有の情報については、http://www.cisco.com で入手可能な『*Design Guide for Cisco Unity*』または『*Design Guide for Cisco Unity Connection*』をそれぞれ参照してください。

ボイスメール ネットワーキングでは、Cisco Unity、Cisco Unity Connection、Cisco Unity Express などのシステム間で、組み込みの Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）サーバおよび Voice Profile for Internet Mail（VPIM）バージョン 2 プロトコルのサブセットを使用して、ボイスメール メッセージの送受信、返信、転送を行えます。3 つのボイスメール メッセージング製品はすべて、VPIM メッセージングにより、製品間の相互運用性をサポートしています。

Cisco Unity Express のボイスメール ネットワーキング

Cisco Unity Express は、メッセージのルーティングでは VPIM を、メッセージ配信では SMTP を使用して、Cisco Unity および Cisco Unity Connection と通信します。Cisco Unity Express ボイスメール ネットワーキングは、次の機能を提供します。

- サブスクライバは、発信側のシステム上でロケーション設定されたリモート Cisco Unity Express または Cisco Unity サブスクライバとの間で、メッセージの送受信や転送を行うことができます。
- サブスクライバはまた、リモート システムから受信したメッセージに対して返信できます。
- サブスクライバは、配布リストの受信者にも、Cisco Unity から発信される個別のメッセージの受信者にもなることができます。

特定の製品におけるボイスメール ネットワーキングの詳細については、http://www.cisco.com で入手可能な該当するボイスメール製品のマニュアルを参照してください。

Cisco Unified Messaging Gateway によるボイスメール ネットワーキング

Cisco Unified Messaging Gateway は、Cisco Integrated Services Router（ISR; サービス統合型ルータ）の Cisco ネットワーク モジュール上で実行される Linux ベースのソフトウェアです。Unified Messaging Gateway は、Cisco Unity、Cisco Unity Connection、Cisco Unity Express のハブとして動作して、VPIM v2 ボイスメール システムをハブアンドスポーク構造または階層構造でネットワーク化できます。このアプローチにより、ボイスメール システム間の VPIM 接続を劇的に削減し、各システムでの設定作業を簡素化できます。各ボイスメール システム（Cisco Unity、Cisco Unity Connection、Cisco Unity Express、または Avaya Interchange と Message Networking サーバ）は、それ自体と Cisco Unified Messaging Gateway との接続を設定するだけで十分です。これにより、Unified Messaging Gateway がシステム間のメッセージのルーティングと配信を処理します。中規模から大規模の分散した拠点を持つ企業が、Cisco Unified Communications ソリューションに移行するためには、このエンドツーエンドのメッセージ ネットワーキング機能が必要です。

Cisco Unified Messaging Gateway には、次の利点があります。

- VPIM を使用した複数の自律的ボイスメール ネットワークで、インテリジェント ルーティングを可能にします。
- スケーラブルなボイスメール ネットワークを提供し、VPIM ネットワークを介してサードパーティ製のボイスメール システム（Avaya Interchange など）との相互運用性を確保します。
- ボイスメール VPIM ネットワークの追加や拡張が容易になります。

Cisco Unified Messaging は、最大で 1000 ノードと 50,000 サブスクライバをサポートできます。サブスクライバの数は、Unified Messaging Gateway に登録された 1 つの Cisco Unity Express が 50 人のサブスクライバをサポートすると想定して計算されています。Unified Messaging Gateway の容量は、サ

ポートする最大ノード数と最大サブスクライバ数の両方に関係しており、一方が増加するともう一方が減少します。たとえば、ネットワーク上に多数のサブスクライバを持つ Cisco Unity や Avaya のエンドポイントがある場合、Unified Messaging Gateway に登録できるノードの数は非常に少なくなります。

Cisco Unified Messaging Gateway を配置する場合は、次のガイドラインに従ってください。

- ネットワーク モジュールをより容量の大きいネットワーク モジュールにアップグレードすることはできないため、1 つのネットワーク モジュールの最大容量を超える可能性がある配置を行う場合には、ネットワークのアップグレードを事前に計画します。
- Cisco Unity Express 3.1 以降のリリースは、Cisco Unified Messaging Gateway に自動的に登録し、ディレクトリの情報を交換しますが、Cisco Unity、Cisco Unity Connection、Avaya Interchange または Message Networking サーバは、Unified Messaging Gateway 上で手動でプロビジョニングする必要があります。
- 冗長性のために 2 つの Unified Messaging Gateway（プライマリとバックアップ）を配置します。
- 最大 10,000 ノードの大規模な配置の場合、最大 20 の Messaging Gateway（10 のプライマリと 10 のバックアップ）を配置します。

（注） Cisco Unified Messaging Gateway を使用したボイスメール ネットワーキングは、小規模企業向け Cisco Unified Communications 500 シリーズには該当しません。これは、Cisco Unified Communications 500 シリーズが、分散型環境でわずか 5 つのサイトしかサポートしないからです。

小規模企業向け Cisco Unified Communications 500 シリーズの配置に関する詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

分散型メッセージング ソリューションとしての VPIM の詳細、および Cisco Unified Messaging Gateway の設計上のガイドラインについては、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

ボイスメールの相互運用性

Cisco Unity および Cisco Unity Connection の両方において、優れたスケーラビリティ オプションと相互運用性サポートが提供されます。Cisco Unity（スタンドアロンまたはクラスタ）を使用した配置の多くは、次の機能を備えるように拡張または移行できます。

- Cisco Unity と Cisco Unity Connection との相互運用性
- Cisco Unity Connection と Cisco Unity Connection との相互運用性

これらの相互運用性オプションの詳細については、次の Web サイトで入手可能な『*Networking Guide for Cisco Unity Connection*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

上記の両方のタイプの相互運用性において、次のガイドラインが適用されます。

- Cisco Unity Connection スタンドアロン サーバ、クラスタ、またはデジタル ネットワークは、Cisco Unity サーバまたはデジタル ネットワークと相互運用できます。
- 1 つの Cisco Unity Connection デジタル ネットワークは、1 つの Cisco Unity または Unity Connection デジタル ネットワークとだけ結合できます。
- いずれの相互運用システムにおいても、最大ユーザ数または連絡先数は 100,000 です。この数に達した後は、削除および変更だけが可能です。
- Cisco Unified Communications Manager Business Edition 3000 および 5000 はサポートされていません。

- 2 つの Cisco Unity Connection および Cisco Unity デジタル ネットワークからそれぞれ 1 台のサーバをブリッジヘッドまたはサイト ゲートウェイとして指定します。
- サイト ゲートウェイとして指定された Cisco Unity Connection サーバのバージョンは 8.0 以上である必要があります。
- Cisco Unity にデジタル的にネットワーク接続されるすべての Cisco Unity Connection サーバのバージョンは 8.0 以上である必要があります。
- サイト ゲートウェイとして指定された Cisco Unity サーバのバージョンは 8.0 以上である必要があります。

Cisco Unity と Cisco Unity Connection の相互運用性

Cisco Unity と Cisco Unity Connection（デジタル ネットワーク）をデジタル的に結合して相互運用すると、ユーザはディレクトリを共有したり、簡単に管理を行ったり、その他の機能を使用したりできます。Cisco Unity と Cisco Unity Connection のネットワークを設計する場合には、次の考慮事項が適用されます。

- Cisco Unity Connection ネットワークのすべてのノードのバージョンは 8.0 以上である必要があります。
- バージョン 5.0 以上では、Cisco Unity デジタル ネットワークにサイト ゲートウェイ以外のサーバを配置できます。
- Microsoft Exchange Server には、Interoperability Gateway for Microsoft Exchange をインストールする必要があります。
- Microsoft Exchange Server は 2010、2007、2003、または Microsoft Business Productivity Online Services（BPOS）専用クラウド ソリューション（Cisco Unity Connection 8.6 以降のリリースのバックエンドの場合のみ Exchange 2010）にできます。Microsoft Exchange のバージョンの詳細については、次の URL で入手可能な Cisco Unity Connection に関する設計ガイドを参照してください。

  http://www.cisco.com/en/US/products/ps6509/tsd_products_support_design.html
- IBM Domino はサポートされていません。
- Cisco Unity Connection ネットワークには、最大で 10 のノードを配置できます。Cisco Unity Connection クラスタでは、パブリッシャ サーバだけがネットワークに参加するため、各サイトにおける 10 ノードの制限をカウントする場合、クラスタは 1 ノードとしてカウントされます。

Cisco Unity Connection と Cisco Unity Connection の相互運用性

Cisco Unity Connection（デジタル ネットワーク、スタンドアロン サーバ、またはクラスタ）は、他の Cisco Unity Connection（デジタル ネットワーク）と相互運用できます。これにより、ユーザは、ディレクトリを共有したり、簡単に管理を行ったり、その他の機能を使用したりできます。また、ノード（クラスタまたはスタンドアロン サーバ）の合計数を最大 20 まで拡張できます。Cisco Unity Connection を他の Cisco Unity Connection ネットワークと相互運用するように配置する場合には、次の点を考慮します。

- デジタル ネットワーク システム内のいずれかの Cisco Unity Connection ノードで Cisco Unity Connection 7.0 が実行されている場合、サポートされる最大ユーザ数は 50,000 です。
- IBM Domino はサポートされていません。
- 各 Cisco Unity Connection デジタル ネットワークでは、最大で 10 のサーバをサポートできます。

Cisco Unity と Unity Connection の仮想化

Cisco Unified Computing System（UCS）は、Total Cost of Ownership（TCO; 総所有コスト）を削減してビジネスの機動性を向上させることを目的として設計された統合システムに、コンピューティング、ネットワーキング、ストレージ アクセス、および仮想化を一体化した、次世代のデータセンター プラットフォームです。Cisco Unity と Cisco Unity Connection の両方において、Cisco Unified Computing System で VMware を使用した仮想化がサポートされています。

Cisco Unity Connection の仮想化には、次の主な設計上の考慮事項が適用されます。

- 最大 20,000 人のユーザがサポートされます。
- Tested Reference Configuration には、選択された Cisco Unified Computing System（UCS）プラットフォームが含まれます。その他のプラットフォームは、仕様ベースのハードウェアのサポート ポリシーによりサポートされる場合があります。
- 仮想化には、VMware ESXi が必要です。
- アクティブ/アクティブ クラスタのサーバは異なるブレードに配置する必要があります。可能であれば異なるシャーシに配置します。

（注） 物理サーバごとに 1 つの CPU コアをアイドルにして、ESXi スケジューラ用に予約しておく必要があります。

仮想システムでの Cisco Unified Communications、Cisco Unity、および Cisco Unity Connection の配置の詳細については、次の Web サイトで入手可能な資料を参照してください。

http://www.cisco.com/go/uc-virtualized

仮想サーバ上での Unified Communications の配置の全般的な情報については、「仮想サーバでの Unified Communications の配置」（P.5-59）のセクションでも確認できます。

Cisco Unity Connection の仮想化については、次の Web サイトで入手可能な最新バージョンの『*Design Guide for Cisco Unity Connection*』も参照してください。

http://www.cisco.com/en/US/products/ps6509/products_implementation_design_guides_list.html

Cisco Unity の仮想化については、次の Web サイトで入手可能な最新バージョンの『*Design Guide for Cisco Unity Virtualization*』も参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_implementation_design_guides_list.html

ボイス メッセージングのベスト プラクティス

ここでは、これまでに言及されていないが、ソリューションの中で、製品の重要な側面として考慮すべき一般的なベスト プラクティスとガイドラインを説明します。これらのベスト プラクティスとガイドラインは、Cisco Unity および Cisco Unity Connection のグループと、Cisco Unity Express のグループに分けて説明します。

Unified CM を使用した Cisco Unity と Cisco Unity Connection のベストプラクティス

この項の説明は、Cisco Unity と Unity Connection に適用されます。Cisco Unity Express については、「Cisco Unity Express の配置に関するベスト プラクティス」（P.21-46）を参照してください。

帯域幅の管理

Unified CM は、帯域幅を管理するためのさまざまな機能を備えています。リージョン、ロケーション、およびゲートキーパーさえも使用して、Unified CM は、WAN リンクを介して伝送される音声コールの数によって既存の帯域幅がオーバーサブスクリプションの状態になることがなく、音声品質が低下しないことを保証できます。Cisco Unity および Unity Connection は、帯域幅の管理とコールのルーティングを Unified CM に依存しています。コール（音声ポート）が WAN リンクを通過することのある環境に Cisco Unity または Unity Connection を配置する場合、このようなコールはゲートキーパーベースのコール アドミッション制御にとって透過的になります。このような状況は、Cisco Unity または Unity Connection サーバが分散クライアントにサービスを提供している場合（分散型メッセージングまたは分散型コール処理）、または Unified CM がリモートに置かれている場合（分散型メッセージングまたは集中型コール処理）、いつでも発生します。Unified CM は、コール アドミッション制御用のリージョンとロケーションを提供します。

図 21-17 では、集中型メッセージングと集中型コール処理を使用する小規模なサイトで、リージョンとロケーションを連携させて使用可能な帯域幅を管理する方法を示しています。リージョンとロケーションの詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください。

図 21-17　ロケーションとリージョン

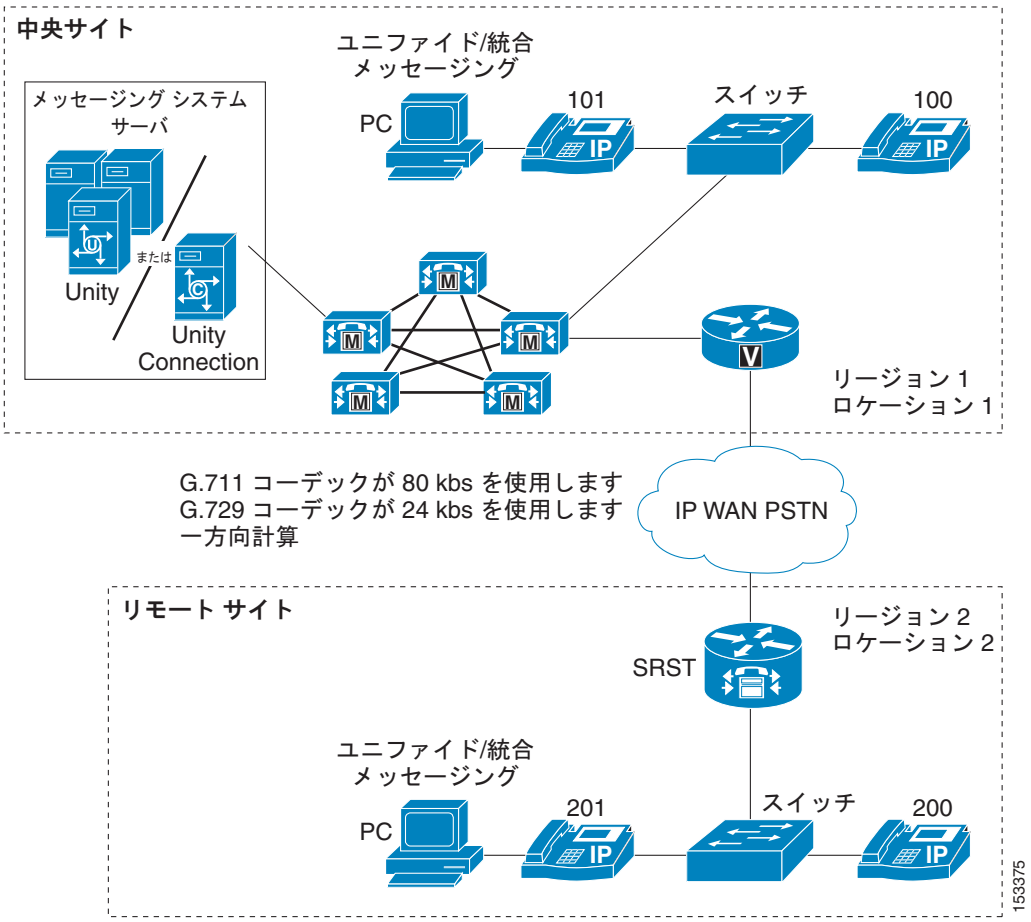


図 21-17 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。ロケーション 1 と 2 は、両方 24 kbps に設定されています。ロケーションの帯域幅は、ロケーション間コールの場合にだけ配分されます。

リージョン内（G.711）コールは、ロケーションの使用可能な帯域幅に対して配分されません。たとえば、内線番号 100 が内線番号 101 をコールする場合、このコールはロケーション 1 の使用可能帯域幅 24 kbps に対して配分されません。ただし、G.729 を使用するリージョン間コールは、ロケーション 1 とロケーション 2 の両方の帯域幅割り当て 24 kbps に対して配分されます。たとえば、内線番号 100 が内線番号 200 をコールすると、このコールは接続されますが、追加の（同時）リージョン間コールでは、リオーダー（ビジー）トーンが聞こえます。

ネイティブ トランスコーディング動作

Cisco Unity と Unity Connection では、IP エンドポイントと Cisco Unity または Unity Connection サーバとの間でコールがネゴシエートされたコーデックと、録音または再生のコーデック形式が異なる場合、ネイティブ トランスコーディングが行われます。コールが G.729 でネゴシエートされ、システム全体の録音形式が G.711 で行われる場合、サーバはそのコールをネイティブにトランスコードする必要があります。Cisco Unity と Unity Connection のネイティブ トランスコーディングは、外部ハードウェア トランスコーダを使用せず、サーバのメイン CPU を使用します。ネイティブ トランスコーディングという名称はここから来ています。

Cisco Unity の動作

デフォルトで、Cisco Unity サーバは、Skinny Client Control Protocol（SCCP）や SIP 経由のテレフォニー統合で、G.711 と G.729 をサポートします。Cisco Unity ではまた、デフォルトのシステム全体のメッセージング録音 形式が G.711 に設定されています。ネイティブ トランスコーディングを無効にするには、システムの録音形式と SCCP または SIP 統合コーデックのアドバタイズメントを同一に設定することを推奨します。たとえば、Unified CM の SCCP ポートまたは SIP トランクを使用して Cisco Unity を実装する場合、アドバタイズされるコーデックから G.729 を削除して、ポートまたはトランクが G.711 のみをアドバタイズするように設定できます。またデフォルトのシステム全体の録音形式を G.711 のままにすることにより、このシステムとネゴシエートされたすべてのコールが G.711 になり、録音もその形式で行われるため、メッセージング サーバ上でネイティブにトランスコードする必要がなくなります。

Cisco Unity でのネイティブ トランスコーディングの無効化

Cisco Unity での SCCP 統合の場合に限り、Unified CM がハードウェア トランスコーダを音声ポートコールに割り当てるようにするには、レジストリ設定によって、Cisco Unity サーバ上でネイティブ トランスコーディングを無効（オフ）にする必要があります。このレジストリ設定は **Audio - Enable G.729a codec support** と呼ばれます。これを設定するためのツールは、http://www.CiscoUnityTools.com で入手可能な Advanced Settings Tool です（SIP で統合するときに Cisco Unity のネイティブ トランスコーディングを無効にする方法の詳細については、http://www.cisco.com で入手可能な特定の Cisco Unity リリースの『*Cisco Unified Communications Manager SIP Trunk Integration Guide for Cisco Unity*』を参照してください。

デフォルトでは、コーデック レジストリ キーが存在しないため、ネイティブ トランスコーディングは有効（オン）です。Advanced Settings Tool により、使用可能な 2 つのコーデックのうちのどちらか 1 つを選択できる新しいレジストリ キーが追加されます。その後、Cisco Unity は、1 つのコーデックだけをサポートすることを Unified CM に「アドバタイズ」します。音声ポートを終端または起点とするコールが、Cisco Unity サーバに設定されているタイプと異なるコーデックを使用している場合、Unified CM はそのコールに外部トランスコーディング リソースを割り当てます。Unified CM 上でトランスコーディング リソースを設定する方法の詳細については、「メディア リソース」（P.17-1）の章を参照してください。

（注）　現在、Unified CM 対応の Cisco Unity TAPI Service Provider（TSP）は、Skinny Client Control Protocol（SCCP）音声ポートに対して G.729 と G.711 mu-law だけをサポートしています（a-law はサポートされていません）。mu-law から a-law への変換には、Unified CM 自体やサービス統合型ルータ（ISR）など、ソフトウェアの Media Termination Point（MTP; メディア ターミネーション ポイント）が必要です。

Advanced Settings Tool を使用して 1 つのコーデックだけをアドバタイズする場合は、Cisco Unity サーバのシステム プロンプトが、使用されるコーデックと同じである必要があります。デフォルトでは、システム プロンプトは G.711 です。コーデックが G.711 に設定されている場合、システム プロンプトは正常に機能します。ただし、G.729 が選択されている場合は、システム プロンプトを変更する必要があります。システム プロンプトを変更する方法の詳細については、http://www.cisco.com で入手可能な『*Cisco Unity System Administration Guide*』を参照してください。システム プロンプトが、レジストリで選択されているコーデックと同じでない場合は、エンド ユーザに、理解不能なシステム プロンプトが聞こえます。

Cisco Unity Connection の動作

Cisco Unity Connection は、Cisco Unity と異なる方法でトランスコーディング操作を処理します。Cisco Unity Connection では、Cisco Unity Connection SCCP または SIP シグナリングによってサポートされているすべてのコーデック形式（G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722）のコールは、常にリニア PCM にトランスコードされます。リニア PCM の録音は、General Configuration の設定でシステムワイドに指定されたシステムレベルの録音形式（リニア PCM、G.711 mu-law/a-law、G.729a、または G.726）にエンコードされます（G.711 mu-law がデフォルト）。したがって、Cisco Unity Connection では、トランスコーディングの全体的な影響が、Cisco Unity の場合と大きく異なります。この章ではこれ以降、発信側デバイスと Unity Connection の間でネゴシエートされるコーデックを「ライン コーデック」、システムレベルの録音形式として設定されたコーデックを「録音コーデック」と呼びます。

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。ただし、iLBC または G.722 を使用する場合は例外です。G.722 と iLBC は、トランスコードに要する処理能力が大きいので、システムに対する影響も大きくなります。G.722 と iLBC は、G.711 mu-law の約 2 倍のリソースを必要とします。そのため、G.722 または iLBC 接続の場合、システムは G.711 mu-law 接続の半分しかサポートできません。

原則として、デフォルトのコーデックは G.711 のままにしておくことを推奨します。設定がディスク容量に制約される場合は、G.729a や G.726 などの低ビット レート コーデックを録音形式として設定できますが、オーディオ品質は G.711 オーディオの忠実度とは異なることに留意してください。また、G.722 がライン上のデバイスで使用されている場合は、リニア Pulse Code Modulation（PCM; パルス符号変調）が、録音のオーディオ品質を高めるオプションです。ただし、この場合はディスク使用量が増加し、ディスク容量に影響を及ぼします。

また録音コーデックを変更したり、特定のライン コーデックのみをアドバタイズしたりする理由がいくつかあります。SCCP 統合または SIP 統合の際に、システムレベルの録音形式やアドバタイズされるコーデックについて決定する場合は、次の要因を検討してください。

- 大部分のエンドポイントと Cisco Unity Connection の間で、どのコーデックがネゴシエートされるか。これは、Cisco Unity Connection によるアドバタイズメントが必要なコーデックとそうでないコーデックの判断に役立ちます。次に、たとえば多くのクライアントを G.722 や iLBC によって Cisco Unity Connection に接続する必要がある場合など、大きな処理能力を必要とする Cisco Unity Connection のネイティブ トランスコーディングの代わりに、Unified CM が、ハードウェア トランスコーディング リソースを提供する必要がある場合を決定できます。
- どのタイプの GUI クライアント（Web ブラウザ、電子メール クライアント、メディア プレーヤーなど）で録音を取得するか、またその GUI クライアントはどのコーデックをサポートするか。
- 選択したコーデックは、どの程度の品質のサウンドを生成するか。コーデックの中には、他のコーデックより高品質なものがあります。たとえば、G.711 は G.729a より品質が高く、高い音質が求められる場合に適切です。
- 1 秒間の録音にどの程度のディスク容量が必要か。

表 21-5 では、Cisco Unity Connection がサポートするコーデック形式の特徴を概観します。

表 21-5　コーデックの特徴

録音形式（コーデック）	オーディオ品質	サポート状況	ディスク容量（帯域幅）
リニア PCM	高品質	広範なサポート	16 kbps
G.711 mu-law および a-law	中程度の品質	広範なサポート	8 kbps
G.729a	低品質	限定的なサポート	1 kbps

表 21-5　コーデックの特徴（続き）

録音形式（コーデック）	オーディオ品質	サポート状況	ディスク容量（帯域幅）
G.726	中程度の品質	中程度のサポート	3 kbps
GSM 6.10	中程度の品質	中程度のサポート	1.6 kbps

Cisco Unity Connection が SIP または SCCP ポートでサポートするコーデックをアドバタイズする方法を変更するには、Cisco Unity とは異なる設定を行います。Cisco Unity Connection がコーデックをアドバタイズする方法の変更の詳細については、『*System Administration Guide for Cisco Unity Connection*』を参照してください。アドバタイズするコーデックとして選択できるのは、G.711 mu-law、G.711 a-law、G.729、iLBC、および G.722 です。また優先順位の高い順にコーデックを記載したリストもあります。SCCP 統合では、コーデックがアドバタイズされ、ネゴシエートされるコールのポートとデバイスのロケーションに基づいて Unified CM がコーデックをネゴシエートするので、コーデックの順序は意味を持ちません。しかし SIP 統合では、順位のリストが意味を持ちます。コーデックに優先順位を設定すると、Cisco Unity Connection は両方のプロトコルをサポートするものの、指定された一方のみの使用が適していることをアドバタイズします。

Cisco Unity Connection Administration でシステムレベルの録音形式を変更する方法の詳細については、『*System Administration Guide for Cisco Unity Connection*』をそれぞれ参照してください。

Unified CM との統合

Cisco Unified CM は、Cisco Unity と Unity Connection のどちらにも SCCP または SIP で統合できます。ここでは、電話機、SIP トランク、および音声ポートに関して、その統合の詳細を説明します。

テレフォニー統合

Cisco Unity は、複数の異なるテレフォニー統合をサポートするので、ユーザを特定のテレフォニー統合に関連付けることができます。Message Waiting Indication（MWI; メッセージ待機インジケータ）ポートも特定の統合に関連付けられるので、その特定の統合に関連付けられたポートを通じて MWI 要求が行われます。

Cisco Unity Connection でも、この機能はほぼ同じです。ユーザは、1 つ以上のポート グループを含む電話機システムに関連付けられます。ポート グループは、MWI ポートに関連付けられているので、MWI 要求は、その特定のポート グループに関連付けられたポートを通じて行われます。

Cisco Unity テレフォニー統合は、Cisco Unity Telephony Integration Manager（UTIM）によって設定し、Cisco Unity Connection の電話システムとポート グループは、System Administrator によって設定します。

Cisco Unity と Unity Connection がサポートできるテレフォニー統合の数が無制限になり、システムあたりのポート数によってのみ制限されるようになりました。この機能は、SCCP 統合と SIP 統合のいずれでも同じ方法で動作します。詳細については、http://www.cisco.com で入手可能な該当する Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

複数クラスタを接続するオプションとして、クラスタごとに Cisco Unity に統合を追加するという方法と別に、Unified CM は Annex M.1（Message Tunneling for QSIG のメッセージ トンネリング）をサポートしています。これにより、管理者は、Unified CM クラスタの間にあるクラスタ間トランク（ICT）で QSIG を有効にできます。ICT で QSIG を有効にすると、複数のクラスタがサポートされている場合でも、Cisco Unity は 1 つの Unified CM クラスタのみに統合され、この 1 つのクラスタでのみ、MWI をオン / オフするポートを指定する必要があります。Unified CM の Annex M.1 機能によって、MWI 要求をそれらの ICT 経由で伝搬し、適切な Unified CM クラスタとそのクラスタ内の電話機

に伝達できます。他のクラスタから発信されたすべてのコールは、その 1 つのクラスタに統合された Cisco Unity サーバに転送できます。ICT で Annex M.1 が有効になっていれば、他のクラスタで MWI ポートを指定する必要はありません。

Annex M.1 の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager System Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Cisco Unity Connection による E.164 番号サポート

Cisco Unity Connection 8.6 以降のリリースでは、次のフィールドに対してのみ E.164 番号形式をサポートします。

- エンド ユーザに対する転送ルールの内線番号
- エンド ユーザに対する通知デバイスの電話番号
- エンド ユーザの個人的な連絡先電話番号
- Cisco Unity Connection System に関するシステムの連絡先電話番号
- Cisco Unity Connection System の Personal Call Transfer Rule（PCTR; パーソナル着信転送ルール）電話番号
- エンドユーザの代行内線番号
- Cisco Unity Connection System の規制パターン
- Cisco Unity Connection System の Message Waiting Indicator（MWI; メッセージ待機インジケータ）内線番号

E.164 形式の番号と連動する代行内線番号ラーニング機能に関しては、次の規制テーブルを更新する必要があります。

- User-Defined and Automatically-Added Alternate Extensions
- Default Outdial

E.164 電話番号を使用する場合は、次の点にも考慮します。

- エンド ユーザ アカウント（ボイスメール ボックスを使用するユーザ）の内線番号は、E.164 形式にできません。このフィールドで、「+」文字はサポートされません。
- E.164 形式のプライマリ電話番号とともに LDAP からユーザをインポートする場合、サポートされる正規表現を使用してトランスレーション パターンを設定します。

電話番号の内線番号への変換については（Cisco Unity Connection 8.5 以降のリリースのみ）、次の Web サイトで入手可能な『*System Administration Guide for Cisco Unity Connection*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

Cisco Unified Communications Manager（Unified CM）から、AXL 統合を経由して、E.164 形式の内線番号とともにユーザをインポートする場合、E.164 内線番号を Unified CM から、Comma-Separated Value（CSV; カンマ区切り値）ファイルにエクスポートする必要があり、Bulk Administration Tool（BAT）を使用して、それらの番号を Unity Connection にインポートする前に、代行内線番号で必要な変換（たとえば、Excel 形式）を実行しなければなりません。Cisco Unity Connection Bulk Administration Tool の使用の詳細については、次の Web サイトで入手可能な『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』を参照してください。

http://www.cisco.com/en/US/products/ps6509/prod_maintenance_guides_list.html

拡張メッセージ待機インジケータ（eMWI）

Enhanced Message Waiting Indicator（eMWI; 拡張メッセージ待機インジケータ）は、従来の MWI を拡張したものであり、音声メッセージの数が視覚的に表示されます。従来の MWI は、新しい音声メッセージが到着したときに電話機のメッセージ ランプをオンにし、ユーザのボイスメール ボックスから新しい音声メッセージが削除されたときにオフにするという 2 値形式の表示です。eMWI は、Cisco Unity と Cisco Unity Connection の両方で動作し、Cisco Unified IP Phone 8900 および 9900 シリーズ SIP 電話機でサポートされています。

eMWI では、ユーザのボイスメール ボックス内の未再生メッセージが視覚的に表示され、メッセージのステータスが色付きで表示されます。未再生のメッセージは、電話機の画面で赤く表示されます。eMWI は、Unified CM において、Cisco Unity と Cisco Unity Connection の両方の SIP および SCCP 統合でサポートされています。eMWI は、システムが SRST または SRSV モードで実行されている場合には機能しません。Cisco Unity Connection との統合においては、Cisco Unity Connection サーバ上に保管されているメッセージだけが eMWI で通知され、外部の IMAP サーバに保管されているメッセージについては通知されません。

eMWI は、Unified CM を使用した分散型コール処理環境で動作します。1 つのクラスタがクラスタ間トランク（H.323 または SIP）経由で音声メッセージング サーバへの接続を提供する、分散型コール処理と集中型音声メッセージング統合のシステムでは、クラスタ間トランク経由での eMWI 更新がサポートされており、エンド デバイスに表示されます（図 21-18 を参照）。

（注）　eMWI は、クラスタ間トランク（H.323 または SIP）経由の、集中型メッセージングと分散型コール処理の環境でも動作します。

図 21-18　Enhanced Message Waiting Indicator（eMWI; 拡張メッセージ待機インジケータ）

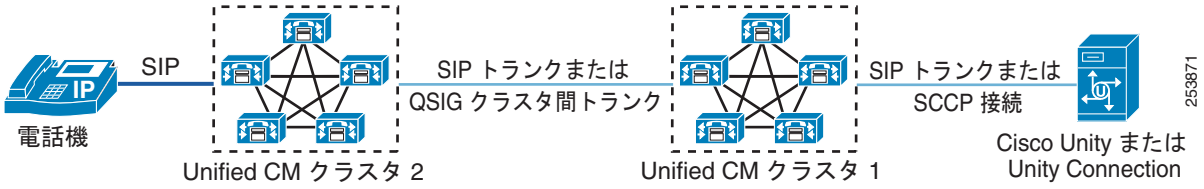


図 21-19 に、クラスタ間トランク（H.323 または SIP）経由の、分散型コール処理と集中型音声メッセージングの環境における eMWI を示します。

図 21-19　分散型コール処理と集中型音声メッセージングの eMWI

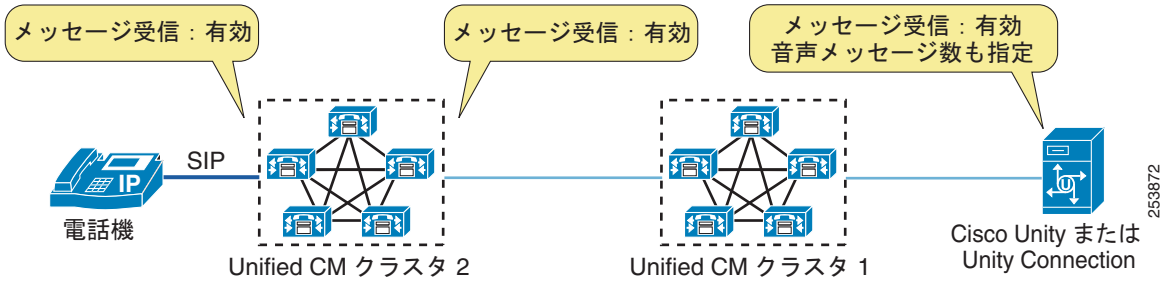


図 21-19 に示すように、クラスタ 2 およびその音声メッセージング ソリューションでは eMWI がサポートされますが、クラスタ 1 ではサポートされません。音声メッセージ数が含まれた eMWI 更新が音声メッセージ ソリューションからクラスタ 2 の電話機に送信された場合、クラスタ 1 では、音声メッセージ数なしの標準 MWI だけがクラスタ 2 に転送されます。

eMWI には、次のガイドラインが適用されます。

- すべてのクラスタで eMWI がサポートされている必要があります。中間クラスタで eMWI がサポートされていない場合、終端のクラスタでは、音声メッセージ数なしの標準 MWI だけが受信されます。
- 標準の MWI では、ランプ状態の変更（オンまたはオフ）だけが送信されるため、多くのトラフィックは生成されません。ただし、eMWI を有効にすると、メッセージング システムからメッセージ数も送信されるため、トラフィック量が増える可能性があります。トラフィック量は、メッセージ数と変更通知数に依存します。

Unified CM クラスタとの音声ポート統合

単一サイト メッセージング環境に Cisco Unity を配置する場合、Unified CM クラスタとの統合は SCCP 音声ポートまたは SIP トランクを介して行われます。Unified CM サブスクライバに障害が発生した場合でも（Unified CM フェールオーバー）、ユーザおよび外部コールが引き続き音声メッセージングにアクセスできるように、設計上の考慮事項には、Cisco Unified CM サブスクライバ間の音声ポートの適切な配置についても考慮する必要があります（図 21-20 を参照）。

図 21-20　Unified CM クラスタと統合された Cisco Unity サーバ（専用バックアップ サーバなし）

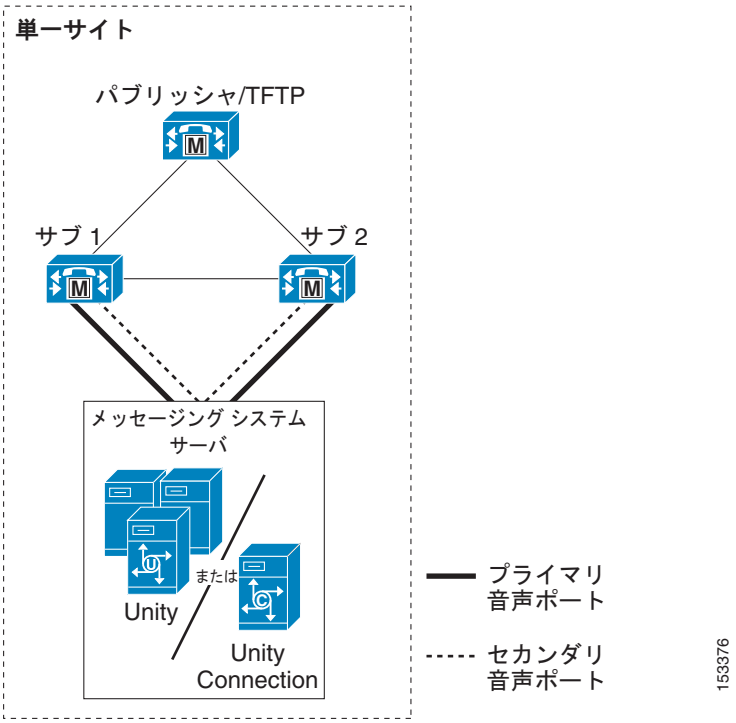


図 21-20 の Unified CM クラスタは、1 対 1 のサーバ冗長性および 50/50 のロード バランシングを採用しています。正常な動作時には、各サブスクライバ サーバがアクティブで、サーバの全コール処理負荷の最大 50% を処理します。1 台のサブスクライバ サーバに障害が発生すると、残りのサブスクライバ サーバが、障害の発生したサーバの負荷を担います。

この設定では、ボイスメール ポートのグループが 2 つ使用され、各グループに、ライセンスのある音声ポートの合計数の半分が含まれています。1 つのグループは、プライマリ サーバがサブ 1 で、セカンダリ（バックアップ）サーバがサブ 2 になるように設定されています。もう 1 つのグループは、サブ 2 がプライマリ サーバで、サブ 1 がバックアップになるように設定されています。

MWI 専用ポートや他の特殊なポートが、2 つのグループ間で等しく分散されていることを確認してください。音声ポートの設定中は、命名規則に特に注意してください。Cisco Unity Telephony Integration Manager（UTIM）ユーティリティでポートの 2 つのグループを設定する場合は、必ずデバイス名プレフィックスがグループごとに一意となるようにし、Unified CM Administration でボイスメール ポートを設定するときと同じデバイス名を使用します。この例では、デバイス名プレフィックスがポートのグループごとに一意になっています。グループ サブ 1 ではデバイス名プレフィックスとして CiscoUM1 が使用され、サブ 2 では CiscoUM2 が使用されています。

着信ボイスメール ポートと発信ボイスメール ポート（MWI、メッセージ通知、および TRaP 用）の比率に関する設計上の詳細情報については、http://www.cisco.com で入手可能な『*Cisco Unity System Administration Guide*』を参照してください。

（注） デバイス名プレフィックスは、ポートのグループごとに一意で、Unified CM Administration に設定されているボイスメール ポートの命名規則と一致する必要があります。

Unified CM Administration では、この例のポートの半分が一意なデバイス名プレフィックス CiscoUM1 を使用して登録されるように設定され、残りの半分が一意のデバイス プレフィックス（CiscoUM2）を使用して登録されるように設定されています（表 21-6 を参照）。表 21-6 に示すように、ポートが Unified CM に登録される場合、半分がサブスクライバ サブ 1 に登録され、残りの半分がサブ 2 に登録されます。

表 21-6　Unified CM Administration でのボイスメール ポート設定

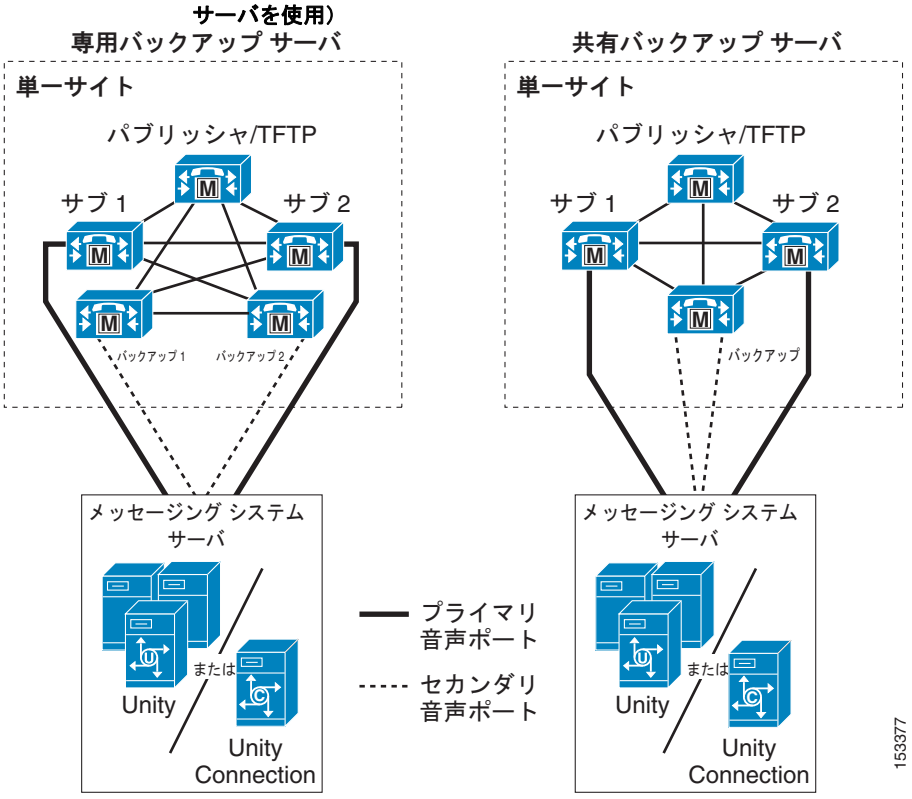
デバイス名	説明	デバイス プール	SCCP セキュリティ プロファイル	ステータス	IP アドレス
CiscoUM1-VI1	Unity1	Default	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI2	Unity1	Default	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI3	Unity1	Default	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM1-VI4	Unity1	Default	Standard Profile	サブ 1 に登録	1.1.2.9
CiscoUM2-VI1	Unity1	Default	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI2	Unity1	Default	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI3	Unity1	Default	Standard Profile	サブ 2 に登録	1.1.2.9
CiscoUM2-VI4	Unity1	Default	Standard Profile	サブ 2 に登録	1.1.2.9

（注） Unified CM Administration でボイスメール ポートに使用される命名規則は、Cisco UTIM で使用されるデバイス名プレフィックスと一致する必要があります。一致しないと、ポートの登録に失敗します。

専用 Unified CM バックアップ サーバを使用する音声ポート統合

この Unified CM クラスタ構成では、各サブスクライバ サーバが 50% を超えるコール処理負荷で動作できます。各プライマリ サブスクライバ サーバは、専用バックアップ サーバまたは共有バックアップ サーバを持ちます（図 21-21 を参照）。正常な動作時、バックアップ サーバはコールを処理しませんが、サブスクライバ サーバの障害時またはメンテナンス時に、バックアップ サーバはそのサブスクライバ サーバのすべての負荷を担います。

図 21-21　単一の Unified CM クラスタと統合された Cisco Unity サーバ（バックアップ サブスクライバ サーバを使用）



この場合のボイスメール ポートの設定は、50/50 のロード バランシング クラスタに似ています。ただし、もう 1 台のサブスクライバ サーバをセカンダリ サーバとして使用するように音声ポートを設定せず、個別の共有バックアップ サーバまたは専用バックアップ サーバを使用します。共有バックアップ サーバと共にクラスタリングされた Unified CM では、両方のサブスクライバ サーバのセカンダリ ポートが、単一のバックアップ サーバを使用するように設定されます。

音声ポート名（デバイス名プレフィックス）は、Cisco UTIM グループごとに一意で、Unified CM サーバ上で使用されるデバイス名と同じである必要があります。

Cisco Unity でボイスメール ポートを設定するには UTIM ツールを使用します。Cisco Unity Connection では、Unity Connection Administration コンソールの Telephony Integration セクションを使用します。詳細については、http://www.cisco.com で入手可能な Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

Cisco Unity Connection による IPv6 サポート

現行の IP アドレッシングに対する要件は、現行バージョンの IP アドレッシングである IPv4 で使用可能な IP アドレスのセットを上回っています。そのため、ほとんどの IP ベースのソリューションが、IPv4 より多くの IP アドレスが使用可能な IPv6 のサポートを取り込む方向に進んでいます。Cisco Unity Connection は、SCCP または SIP 経由の Cisco Unified Communications Manager システム統合を使用して IPv6 アドレッシングをサポートします。コンポーネント レベルでは、呼制御とメディア経由でのみ、デュアル スタック アドレッシング（IPv4 と IPv6 の両方）がサポートされます。

（注）　音声メッセージは .wav ファイルとして保存されるため、IPv6 や IPv4 とは無関係です。

IPv6 サポートはデフォルトで無効になっていますが、システム管理者は Cisco Unified Operating System Administration と Command Line Interface（CLI; コマンドライン インターフェイス）のどちらかで IPv6 を有効にして、IPv6 アドレス設定値を構成できます。Cisco Unity Connection は、ルータアドバタイズメントと DHCP のどちらかを経由して、または、Cisco Unified Operating System Administration と CLI のどちらかで手動で設定されたアドレスから、IPv6 アドレスを取得できます。

IPv4 と IPv6 の両方が実装されますが、同時に動作することはできません。Cisco Unity Connection は、「IPv6 のみ」のサーバ設定をサポートしていません。また、Cisco Unity Connection は、IPv6 専用のユニキャストをサポートしています。

（注）　Cisco Unity Connection は、Cisco Unified Communications Manager Business Edition 3000 および 5000 でのデュアル スタック アドレッシング モード（IPv4 と IPv6 の両方）をサポートしていません。

Cisco Unity Connection による単一受信トレイ

Cisco Unified Communications Manager 8.5 以降のリリースでは、Cisco Unity Connection および Microsoft Exchange 2003、2007、または 2010（クラスタ化または非クラスタ化）を使用した単一受信トレイ機能がサポートされているため、ボイスメールのユニファイド メッセージングが提供されます。Cisco Unity Connection は、この 3 つすべての Microsoft Exchange バージョンを同時にサポートすることも、いずれかを個別にサポートすることもできます。Cisco Unity Connection ViewMail for Microsoft Outlook から送られてくるものも含め、すべての音声メッセージが Cisco Unity Connection に保存されてから、すぐに受信者の Exchange メールボックスに複製されますが、複製はオプションです。また、この機能はユーザ単位で設定可能です。

Cisco Unity Connection でボイスメール用のユニファイド メッセージングをサポートするには、いくつかの設計上の留意点があります。ユーザの E メールは、E メールとボイスメールを含むすべてのメッセージに対する単一のコンテナになります。メッセージが受信トレイ下の別のフォルダに移動されても、Cisco Unity Connection から削除されることはありません。ただし、ユーザが音声メッセージを受信トレイ フォルダ下ではない Outlook フォルダに移動した場合は、Cisco Unity Connection からそのメッセージが削除されますが、コピーが Outlook 内に残っているため、ViewMail for Outlook で再生できます。ユーザがメッセージを受信トレイ フォルダまたは受信トレイ フォルダ下のフォルダに移動すると、そのメッセージがユーザの Cisco Unity Connection メールボックスに表示されます。また、ユーザが Cisco Unity Connection から音声メッセージを削除した場合、または、メッセージの有効期限が切れたために Cisco Unity Connection から自動的に削除された場合は、そのメッセージが Microsoft Exchange からも削除されます。同様に、Microsoft Exchange から音声メッセージが削除された場合は、Cisco Unity Connection からも削除されます。

メッセージが保護対象かつプライベートとしてマークされている場合は、実メッセージが Microsoft Exchange に複製されません。代わりに、そのメッセージに関する簡単な説明付きのプレースホルダーが作成されます。実メッセージの唯一のコピーが Cisco Unity Connection 上に保存され、ユーザがそのメッセージを取り出すと、通常のメッセージの場合と違って、ローカル ソースではなく、Cisco Unity

Connection から直接再生されます。これは、オーディオ ファイルが Outlook からボイルメール経由でアクセスされた場合は、ローカル アクセスできないことも意味します。保護対象でプライベートのメッセージを受信トレイおよび受信トレイ下のフォルダ以外のフォルダに移動した場合は、そのメッセージが完全に削除されるため、取り出せなくなります。

（注）　メッセージング展開の種類に関係なく、すべての音声メッセージが Cisco Unity Connection サーバ上に保存されます。Cisco Unity Connection は、音声メッセージング トラフィック、通知、および同期化の信頼できるソースです。

1 つのボイスメール メッセージに割り当て可能なスペース容量は、メッセージの有効期限と同様に、Cisco Unity Connection サーバ上で設定されます。ボイスメール メッセージの最大サイズは Microsoft Exchange サーバ上で設定されます。一般的に、Microsoft Exchange サーバには、メールボックスに同期される Cisco Unity Connection よりも大きなサイズが保存されます。そのため、Microsoft Exchange 上のメッセージの最大サイズは、Cisco Unity Connection 上の最大サイズよりも大きくする必要があります。

Cisco Unity Connection と Microsoft Exchange 間の通信のセキュリティ面から、デフォルト オプションとして HTTPS が選択されます。HTTP もサポートされていますが、セキュリティが低下するうえ、Microsoft Exchange 上で余分な設定が必要になる場合があるため、推奨できません。その一方で、証明書サーバへのアクセスが可能な場合に、Microsoft Exchange 証明書を確認するためのオプションが用意されています。

Cisco Unity Express の配置に関するベスト プラクティス

Cisco Unity Express を配置する場合は、次のガイドラインとベスト プラクティスを使用してください。

- ボイスメールの宛先として Cisco Unity Express を持つ IP 電話が、Cisco Unity Express をホストするルータと同じ LAN セグメントに置かれていることを確認します。
- Cisco Unity Express を使用して配置するサイトで無中断の自動応答機能（AA）と電子メール アクセスが必要な場合は、Cisco Unity Express、SRST、および公衆網の音声ゲートウェイがすべて同じ物理サイトに置かれていることを確認します。Hot Standby Router Protocol（HSRP; ホットスタンバイ ルータ プロトコル）やその他の冗長性ルータ設定は、現在、Cisco Unity Express ではサポートされていません。
- 各メールボックスは、プライマリ内線番号とプライマリ E.164 番号に関連付けることができます。通常、この番号は、公衆網の発信者が使用する Direct-Inward-Dial（DID）番号です。プライマリ E.164 番号が他の番号に設定されている場合、SRST モード時に正しいメールボックスに到達するように、Cisco IOS 変換パターンを使用して、プライマリ内線番号かプライマリ E.164 番号に一致させます。

Unified CM とのボイスメール統合

- 各 Cisco Unity Express サイトは、ボイスメール用と AA 用（ライセンスされ、購入している場合）に CTI ルート ポイントを 1 つずつ関連付ける必要があります。またライセンスされた Cisco Unity Express ポートと同じ数の CTI ポートを設定する必要があります。Cisco Unity Express の数が、「コール処理」（P.8-1）の章に示すスケーラビリティ ガイドラインを超えないことを確認します。
- Cisco Unity Express は、Unified CM 上の JTAPI ユーザに関連付けられます。単一の JTAPI ユーザをシステム内の Cisco Unity Express の複数のインスタンスに関連付けることは可能ですが、Unified CM 内の専用の JTAPI ユーザをそれぞれ単一の Cisco Unity Express に関連付けることを推奨します。

- Unified CM を以前のバージョンからアップグレードした場合、JTAPI ユーザのパスワードは、Unified CM で自動的にリセットされます。したがって、管理者は、アップグレードの後、JTAPI パスワードが Cisco Unity Express と Unified CM の間で同期化され、Cisco Unity Express を Unified CM に登録できることを確認する必要があります。
- CTI ポートと CTI ルート ポイントは、特定の場所で定義できます。Unified CM と Cisco Unity Express の間で、ロケーションベースのコール アドミッション制御を使用することを推奨します。RSVP を使用することもできます。
- Cisco Unity Express と Unified CM の間を通過する WAN のシグナリング トラフィックのための、適切な Quality of Service（QoS）と帯域幅を確保します。各 Cisco Unity Express サイトの CTI-QBE シグナリングのために、20kbps の帯域幅をプロビジョニングします。詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。
- Unified CM から Cisco Unity Express への CTI-QBE シグナリング パケットは、AF31（0x68）という DSCP 値でマーキングされています。Unified CM は、CTI-QBE シグナリングに TCP ポート 2748 を使用します。
- Unified CM JTAPI ライブラリは、すべての発信 QBE シグナリング パケットに、適正な IP Precedence ビットを設定します。その結果、Cisco Unity Express と Unified CM の間のすべてのシグナリングに、適正な QoS ビットが設定されます。

Cisco Unity Express コーデックと DTMF のサポート

Cisco Unity Express へのコールは、G.711 のみを使用します。ローカルのトランスコーダを使用して、WAN を通過する G.729 コールを G.711 コールに変換することを推奨します。Unified CM リージョンは、リージョン内コールに G.711 音声コーデックを、リージョン間コールに G.729 音声コーデックを使用するように設定できます。

Cisco Unity Express サイトにトランスコーディング機能がない場合、必要な数の G.711 ボイスメールに対応する十分な帯域幅を WAN 上にプロビジョニングします。IP 電話と Cisco Unity Express デバイス（CTI ポートと CTI ルート ポイント）の間のコールに G.711 音声コーデックを使用するように、Unified CM リージョンを設定します。

Cisco Unity Express は、DTMF リレーのみをサポートし、インバンド DTMF トーンはサポートしていません。Cisco Unity Express では、DTMF は、SIP または JTAPI のいずれかの呼制御チャネルを介してアウトオブバンドで搬送されます。Cisco Unity Express 2.3 は、RFC 2833 を使用した、Cisco Unity Express への G.711 SIP コールをサポートします。

JTAPI、SIP トランクおよび SIP 電話機のサポート

Cisco Unified CM は SIP トランク プロトコルをサポートしますが、Cisco Unity Express は Unified CM との通信に JTAPI を使用します。Cisco Unity Express は、SCCP 電話機と SIP 電話機の両方をサポートします。

- SRST を使用できるように SIP トランクを設定し、（JTAPI によって）SIP 電話機をサポートするように Unified CM を設定します。
- Cisco Unity Express は、トランスコーダ経由で G.729 SIP コールをサポートします。また Cisco IOS Release 12.3(11)XW で RFC 2833 がトランスコーダをパススルーする能力が追加されています。
- Cisco Unity Express は、Unified CM からのスロースタート コールの場合、コール設定のためのディレイド メディア（delayed media、INVITE メッセージ内に SDP なし）をサポートします。

- Cisco Unity Express は、ブラインド転送と打診転送の両方をサポートしますが、デフォルトの転送モードは、SIP コールで REFER を使用した打診転送（半自動）です。転送モードを、REFER を使用する打診転送または BYE/ALSO を使用するブラインド転送に明示的に変更するには、Cisco Unity Express コマンドライン インターフェイスを使用します。リモート エンドで REFER がサポートされていない場合は、BYE/ALSO が使用されます。
- Cisco Unity Express は、音声メッセージ通知のためのアウトコールをサポートしています。また、打診転送もサポートしています。これらのいずれのコール設定時でも、Cisco Unity Express は INVITE に対する 3*xx* 応答を受信できます。Cisco Unity Express は、INVITE に対する 301（Moved Permanently）と 302（Moved Temporarily）応答のみを処理します。これには、3*xx* 応答の Contact ヘッダーに含まれ、新しい INVITE の送信に使用する URL が必要です。305（Use Proxy）応答は、サポートされていません。

（注）　Cisco Unified CM と Cisco Unity Express との間の互換性については、http://www.cisco.com/en/US/docs/voice_ip_comm/unity_exp/compatibility/cuecomp.htm で入手可能な『*Cisco Unity Express Compatibility Matrix*』を参照してください。

Cisco Unity Express の詳細については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

サードパーティ製ボイスメールの設計

この項では、サードパーティ製ボイスメール システムを Cisco Unified Communications とともに配置する場合のさまざまなオプションについて説明します。統合とメッセージングの両方について説明します。

（注）　この項では、ポートやストレージに関するサードパーティ製ボイスメール システムのサイジング方法については説明しません。この情報については、ボイスメール ベンダーに連絡してください。ボイスメール ベンダーは、具体的なトラフィック パターンに基づいて、各ベンダーのシステムにおける個別の要件をより適切に判断できます。

統合

*統合*は、ボイスメール システムとその関連する PBX またはコール処理エージェントとの間の物理的な接続として定義されます。統合によって、これらの間に機能セットも提供されます。

ボイスメール ベンダーは数多くあり、Cisco Unified CM を配置する場合に既存のボイスメール システムを引き続き使用することも一般的です。この要件に留意し、シスコでは、Simplified Message Desk Interface（SMDI）という業界標準のボイスメール プロトコルをサポートしています。SMDI は、ボイスメール システムが適切にコールに応答するために必要なすべてのコール情報を提供するシリアル プロトコルであり、さまざまなベンダーの異なるシステム間でのボイスメール統合において配置される最も一般的な方式です。

（注）　シスコでは、サードパーティ製ボイスメール システムのテストや認証は行っていません。通常、この業界では、さまざまな PBX システムに対して自社の製品をテストまたは認証することはボイスメール ベンダーの責任であるとされています。シスコでは、そのような機器とのシスコのインターフェイスをテストし、どのようなサードパーティ製ボイスメール システムが接続されるかにかかわらずこれらのインターフェイスをサポートします。

ボイスメール統合における SMDI の代替選択肢として、QSIG があります。QSIG を使用しても、Primary Rate Interface（PRI; 一次群速度インターフェイス）T1/E1 トランク経由でサードパーティ製 PBX から Unified CM に接続できます。各方式にはそれぞれの利点と欠点があり、使用する方式はボイスメール システムと現在の PBX との統合方法に大きく依存します。

ボイスメール システムと Unified CM を接続する他の方式（PRI ISDN トランクと SMDI を組み合せる方式など）もありますが、それらは一般的ではありません。

現在、ボイスメール統合に使用できる他の方法には、H.323 や SIP があります。ただし、ベンダーにおけるさまざまな実装方式、サポートされる機能、およびその他の要因によって、これらのサードパーティ製ボイスメール統合は、お客様が評価する必要があります。これらのオプションの詳細については、シスコのアカウント チームまたはシスコ代理店に連絡してください。

メッセージング

*メッセージング*は、ボイスメール システム間でのメッセージの交換として定義されます。メッセージングの目的で使用できるいくつかのオープンな標準があります。

異なるシステム間でのメッセージングを可能にするために配置される最も一般的なプロトコルは、Voice Profile for Internet Mail（VPIM）です。VPIM の仕様は何度か更新されており、最新ではないバージョン 2 が現在でも最も広く採用されているようです。VPIM よりも前から存在するメッセージング プロトコルに Audio Messaging Interchange Specification - Analog（AMIS-A）がありますが、ユーザ インターフェイスが使いにくく、アナログ テクノロジーが使用されており、機能も少ないことから、ほとんど使用されていません。

CHAPTER 22

Cisco コラボレーティブ会議

シスコは、ユーザが仮想コラボレーティブ環境で作業できるようにすることを最終的な目標とする広範囲のコラボレーション テクノロジーを提供しています。そのような環境では、意思決定プロセスが迅速化および効率化され、生産性が向上します。コラボレーションという大きな領域には数多くのテクノロジーがありますが、この章では特に、音声、ビデオ、および豊富なコンテンツ共有機能による同時通信を可能にするシスコ製品に関する設計ガイドラインを示します。また、さまざまなソリューションの違いを調べ、どのような場合に、あるソリューションが別のソリューションよりも適しているかについて提案します。

いくつかの側面は、すべての Cisco コラボレーティブ会議ソリューションに共通します。たとえば、会議の作成がユーザにとって使い慣れた直感的なものになるように、スケジューリング システムやカレンダー システムと統合する機能などです。組織内の参加者を招待するための LDAP ディレクトリとの接続や、一貫性のある認証方式も重要です。ユーザは、オフィス内でも企業外でも仮想会議を主催および参加でき、外出先でも生産性を持続させることができます。

この章で説明する Cisco コラボレーティブ会議ソリューションは、オンプレミス、オフプレミス、または混合配置として利用できます。そのため、組織はすでに投資している Unified Communications ソリューションと統合でき、または、「クラウド内」でホストされるサービスを実装できます。このことは、さまざまなソリューションを区別する重要な点の 1 つであり、組織に最も適したソリューションを決定する際の最初の決定ポイントです。この章では、次のトピックについて説明します。

- Cisco WebEx Software as a Service（SaaS）
- Cisco Unified MeetingPlace
- Cisco Unified Videoconferencing

各項では、ソリューションのハイレベルなアーキテクチャを定義してから、ハイ アベイラビリティの設計ガイドライン、キャパシティ プランニング、およびソリューションに関係するその他の設計上の考慮事項について説明します。

シスコのさまざまなコラボレーティブ クライアント製品の詳細と、それらがコラボレーティブ会議ソリューションにどのように適しているかについては、「Cisco Collaboration クライアントおよびアプリケーション」（P.24-1）の章を参照してください。

この章の新規情報

この章は、このマニュアルの以前のバージョンの複数の章からの情報を組み合せており、シスコのコラボレーティブ会議に関する設計上の議論をまとめるために新しい資料を組み込んでいます。初めてこの章を読む場合は、章全体に目を通すことを推奨します。

表 22-1 に、この章に新しく追加されたトピック、または、このマニュアルの以前のリリースから大幅に変更されたトピックの一覧を示します。

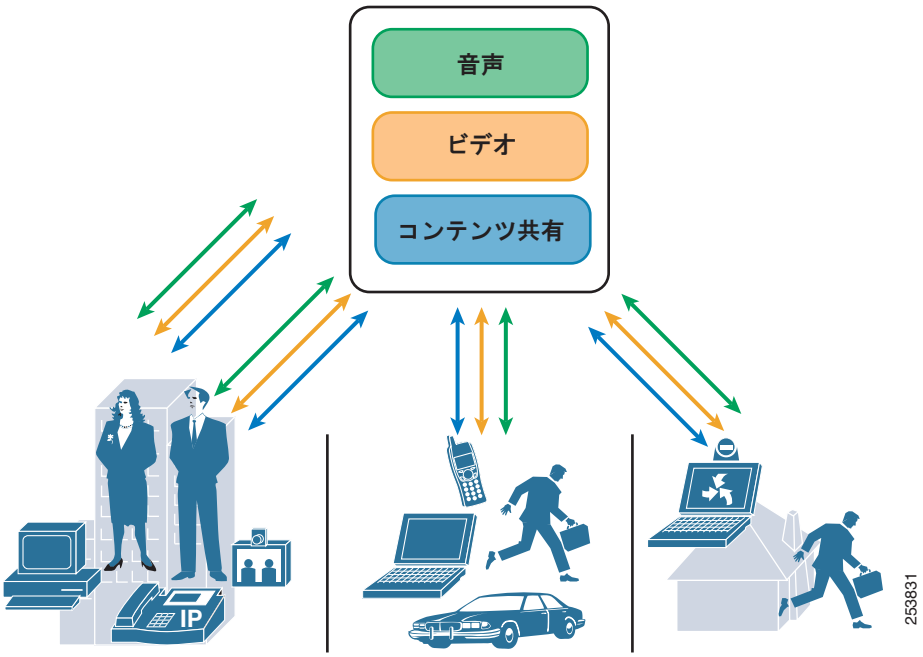
表 22-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Unified MeetingPlace 8.5	「Cisco Unified MeetingPlace」（P.22-13）	2011 年 6 月 2 日
その他の訂正および変更	この章の各項で説明	2011 年 6 月 2 日
Cisco Unified MeetingPlace のキャパシティ プランニング	「Unified MeetingPlace 音声会議のサイジングに関するガイドライン」（P.22-40）	2010 年 11 月 15 日
高画質ビデオ	「アーキテクチャ」（P.22-5） 表 22-4	2010 年 11 月 15 日

コラボレーティブ会議のアーキテクチャ

ハイレベルでは、コラボレーティブ会議には、会議の参加者の一部またはすべてからの音声、ビデオ、およびコンテンツの受信、それらのストリームのミキシング、およびミキシングされた音声、ビデオ、およびコンテンツの参加者への返信が含まれます。図 22-1 に、内部と外部両方の参加者、外勤職員と遠隔地の職員、または他の組織からの参加者も含む論理的な会議を示します。

図 22-1　コラボレーティブ会議の論理的な表示



音声、ビデオ、およびコンテンツ共有というコラボレーティブ会議の 3 つの側面は、排他的ではありません。Cisco コラボレーティブ会議ソリューションは、これら 3 つを統合して、ユーザ エクスペリエンスを拡張します。発言中の参加者を決定する機能、ユーザのコンテンツ共有インターフェイスからの消音、コンテンツ共有に表示されるビデオ レイアウトの選択などの機能はすべて、これら 3 つの要素がソリューションによって統合されていることを示します。この章で説明するすべてのコラボレーティブ会議ソリューションは、コンテンツ共有のために Cisco WebEx インターフェイスを使用します。これにより、すべてのソリューションにわたって一貫性のあるユーザ エクスペリエンスが提供されます。

特定の組織に最適なソリューションを検討するときは、多くの要素を評価する必要があります。組織のユーザの特性（遠隔地の職員の数、アクセス機能、ビデオの使用状況）や、使用できるエンドポイントの範囲と機能を考慮することが重要です。高品位などのビデオ要件または既存のビデオ インフラストラクチャとのインターワーキングも、ソリューションに影響する場合があります。会議自体の性質（トレーニング シナリオ、コラボレーティブ会議、組織の外部の会議参加者数など）は、識別する必要がある重要な特性です。初期コスト、メンテナンス コスト、Return On Investment（ROI; 投資収益率）もすべて関係します。

ソリューション間で最初に明らかにすることの 1 つは、各タイプの会議（つまりミキシング）を実行するリソースの場所がオンプレミスかオフプレミスかです。クラウド サービスへのアクセス、外勤職員の規模、およびサポート スタッフのレベルは、すべて考慮事項です。Cisco WebEx Software as a Service（SaaS）は、クラウドをオンプレミスで拡張するオプションを備えた完全にオフプレミスのソリューションを提供します。一方、Cisco Unified MeetingPlace および Cisco Unified Videoconferencing は、リソースの大部分をオンプレミスでプルするオプションを備えたハイブリッド（オンプレミスとオフプレミスの混合）です。Cisco Unified Communications を配置している組織は、オンプレミス ソリューションを利用することで最も利益を得ます。この章の以降の項では、各ソリューションの詳細な配置オプションについて説明します。

このマニュアルでは、高性能なコラボレーション ソリューションを提供するための 2 つのアプローチについて説明します。2 つのソリューションは、次のいずれかとして大きく分類できます。

- クラウドベース（SaaS）サービス（オンプレミスの促進を含む）
- オンプレミス ソリューション（クラウドベースの拡張を含む）

表 22-2 は、オンプレミス クラウドの観点から利用可能なソリューションを要約したものです。

表 22-2　Cisco コラボレーティブ ソリューションのオンプレミス、クラウド、およびハイブリッド機能

	音声		ビデオ		コンテンツ共有	
ソリューション	オンプレミス	クラウド	オンプレミス	クラウド	オンプレミス	クラウド
Cisco WebEx SaaS	なし	あり	なし	あり[1]	なし	あり
Cisco WebEx SaaS と アグリゲーション サービス ルータ（ASR）向け Cisco WebEx ノード	あり（VoIP）	あり	あり	あり[1]	あり[2]	あり
Cisco Unified MeetingPlace と WebEx SaaS[3]	あり	なし	あり	なし	なし	あり
Cisco Unified MeetingPlace と Cisco MCS 向け Cisco WebEx ノード[3]	あり	なし	あり	あり	あり[2]	あり
Cisco Unified MeetingPlace と Cisco ASR 向け Cisco WebEx ノード[3]	あり	あり	あり	あり[1]	あり[2]	あり
Cisco Unified MeetingPlace（音声 / ビデオだけの配置）	あり	なし	あり	なし	なし	なし
Cisco Unified Videoconferencing（音声 / ビデオだけの配置）	あり	なし	あり	なし	なし	なし

1. Cisco WebEx Web カメラ ビデオ。
2. ASR および MCS 向け Cisco WebEx ノードには、Cisco WebEx ネットワークへの接続が必要です。
3. Cisco Unified MeetingPlace および Unified Videoconferencing ソリューションは、代わりにクラウドの WebEx Web カメラ ビデオ ストリーミング機能を使用できます。ただし、相互運用性がないため、両方とも使用することは推奨しません。

Cisco WebEx Software as a Service

Cisco WebEx は、ハードウェアをオンサイトに配置する必要がないコラボレーション ソリューションです。すべてのサービス（音声、ビデオ、およびコンテンツ共有）は、インターネットまたはクラウドでホストされます。これは、多くの場合、Software-as-a-Service（SaaS）と呼ばれます。会議は、任意の場所からでもいつでも開始および参加でき、企業への接続は必要ありません。ここでは、ソリューションの特性について説明し、WebEx SaaS の配置の設計ガイドラインを示します。

会議のスケジューリングと開始に関して、WebEx にはクラウドベースの Web スケジューリング機能がありますが、ほとんどの組織は企業電子メール システム（Exchange、Lotus Notes など）またはその他の企業アプリケーションからスケジューリングします。WebEx Productivity Tools は、単一のアプリケーションに組み込まれた既知のデスクトップ ツールとの統合のバンドルです。WebEx 管理者は、組織のユーザにツールを介して提供される特定の統合を制御できます。WebEx サイト名にアクセスした

ときに自動的にインストールすることも、標準的なデスクトップ管理ツールを使用してローカルでプッシュすることもできます。WebEx Productivity Tool の詳細については、次の Web サイトで入手可能な WebEx の『*Productivity Tools FAQs*』を参照してください。

https://vnc.WebEx.com/docs/T26L/pt/mc0800l/en_US/support/productivitytools_faq.htm

クラウド内に組織の WebEx ユーザ プロファイルを作成する方法は 3 つあります。実際のユーザ名とパスワード、および大量のユーザ アカウントの処理について、セキュリティ上の考慮事項を検討する必要があります。WebEx 管理者は、CSV テンプレートのバルク インポートによって手動で、またはプログラムによるアプローチによって、ユーザ プロファイルを作成できます。プログラムによるアプローチでは、WebEx API、URL、および XML のいずれかまたは組み合せ、あるいはフェデレーション SSO ソリューションが使用されます。プログラムによるアプローチはカスタマー ポータルで使用できます。カスタマー ポータルは、WebEx に直接統合される CRM ツールや Learning Management System などのアプリケーションです。WebEx ディレクトリ統合および認証の詳細については、次の Web サイトで入手可能な WebEx の『*Approaches to Single Sign-On Developer Technical Note*』を参照してください。

http://developer.WebEx.com/c/document_library/get_file?folderId=11421&name=DLFE-213.pdf

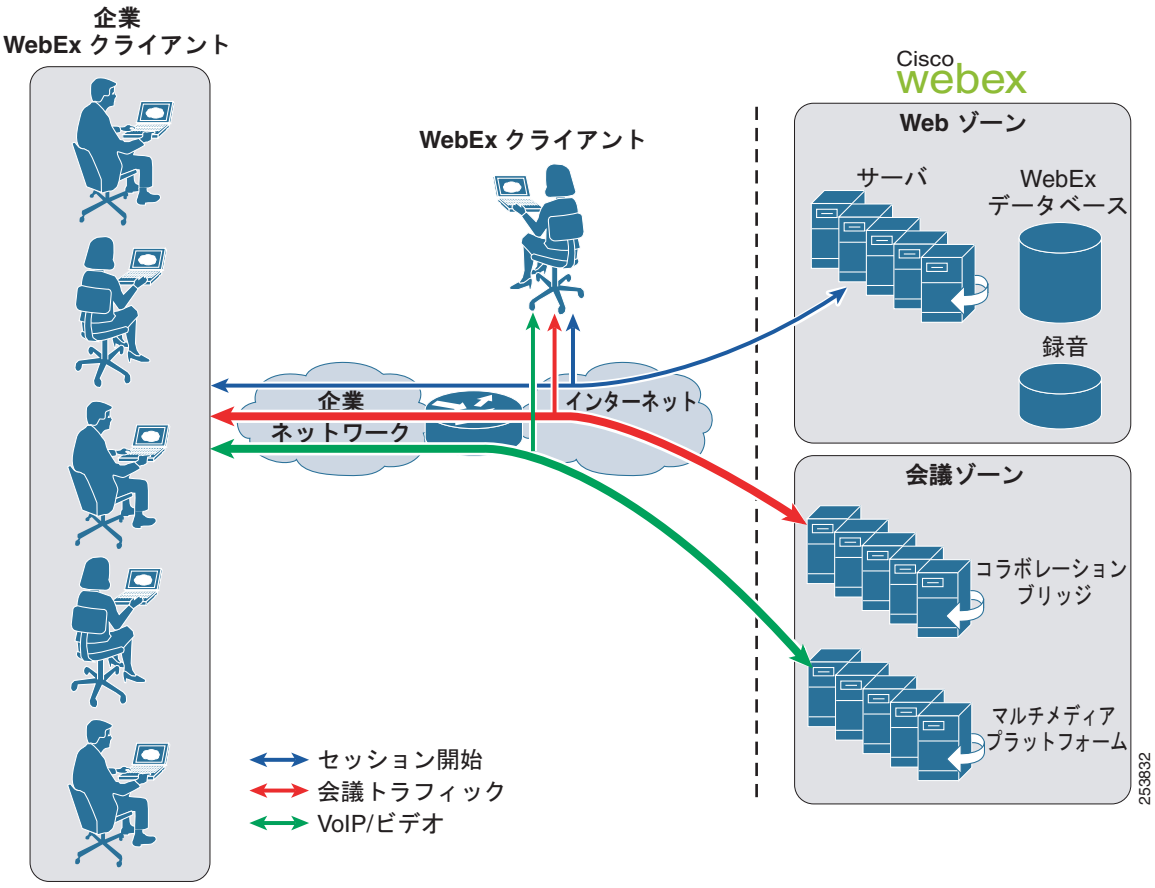
組織の LDAP ディレクトリとの直接統合の場合、Security Assertion Markup Language（SAML）を使用したフェデレーション SSO が望ましいアプローチです。フェデレーション SSO の詳細については、次の Web サイトで入手可能な WebEx の『*Federated SSO Authentication Service Technical Overview*』を参照してください。

http://developer.WebEx.com/c/document_library/get_file?folderId=11421&name=DLFE-201.pdf

アーキテクチャ

組織の IT 部門は、Cisco Collaboration Cloud ベース ソリューションのアーキテクチャを理解する必要があります。図 22-2 に示す従来の WebEx 配置モデルでは、すべてのクライアントからのすべてのコンテンツ、音声、およびビデオ トラフィックは、インターネットを通過し、クラウド内で WebEx データ センターでミキシングおよび管理されます。WebEx データ センターは、論理的には、会議ゾーンと Web ゾーンに分割されます。Web ゾーンは、Web 会議の前後に発生することを処理します。スケジューリング、ユーザ管理、課金、レポート、ストリーミング レコーディングなどのタスクが組み込まれています。会議ゾーンは、実際の会議がエンドポイント間で進行中になると、その切り替えを処理します。

図 22-2　　従来の WebEx 配置



会議ゾーンは 2 つのサブシステムで構成されます。会議ゾーンには、会議コンテンツを切り替えるコラボレーション ブリッジがあります。マルチメディア プラットフォームは、会議内の VoIP ストリームおよびビデオ ストリームすべてのミキシングを処理します。WebEx セッションに参加するには、参加者は最初に Web ゾーンに接続する必要があります。Web ゾーンのトラフィックは、会議の前後にだけ流れ、比較的低い帯域幅であり、主にリアルタイムではありません。リアルタイムの会議コンテンツ共有は、会議ゾーンへ、または会議ゾーンから流れ、帯域幅に大きな影響を与える可能性があります。そのリアルタイムという性質から、企業のアクセス インフラストラクチャに大きな負荷がかかる場合があります。ネットワーク トラフィック プランニングの詳細については、「キャパシティ プランニング」（P.22-9）を参照してください。

デフォルトでは、すべての WebEx 会議データは、128 ビット SSL 暗号化を使用してクライアントとシスコの Collaboration Cloud の間で暗号化されます。クラウド内の SSL アクセラレータによって、コンテンツ共有情報は復号化され、コンテンツを処理して SSL アクセラレータを介して返信する WebEx カンファレンス ブリッジに送信されます。情報は SSL アクセラレータで再度暗号化されてから、参加者に返信されます。Web ゾーンと会議ゾーンのトラフィックはすべて、128 ビット SSL を使用して暗号化されます。SSL 機能を Web ゾーンと会議ゾーンのサーバからオフロードするために、SSL アクセラレータが使用されます。

会議の終了後は、WebEx クラウドまたは参加者のコンピュータにセッション データは保持されません。2 種類のデータだけが長期的に保持されます。これらのデータは、課金とレポート情報、およびオプションのネットワーク ベースのレコーディングであり、どちらも許可された企業ユーザだけがアクセスできます。

会議データの一部の制限されたキャッシュが、会議ゾーンで実行されます。これは、接続に問題のあるユーザまたは開始されたあとで会議に参加するユーザが、最新の完全に同期がとれたバージョンの会議コンテンツを受信できるようにするために実行されます。

文書化されたセキュリティのベスト プラクティスに WebEx クラウドが準拠していることを保証するために、独立した第三者によって、商業的および政治的なセキュリティ要件を対象とした外部監査が実行されます。WebEx では、AICPA によって確立された標準に従って、SAS-70 Type II 監査を年次で Pricewaterhouse Cooper によって実行しています。WebEx に対して監査される制御は、ISO-17799 の標準に基づきます。この重視および認知されている監査によって、顧客データの処理に関して、WebEx サービスが制御の目的および制御のアクティビティ（情報技術およびセキュリティ関連プロセスの制御を含む場合もあります）に対して詳細に監査されていることが検証されます。

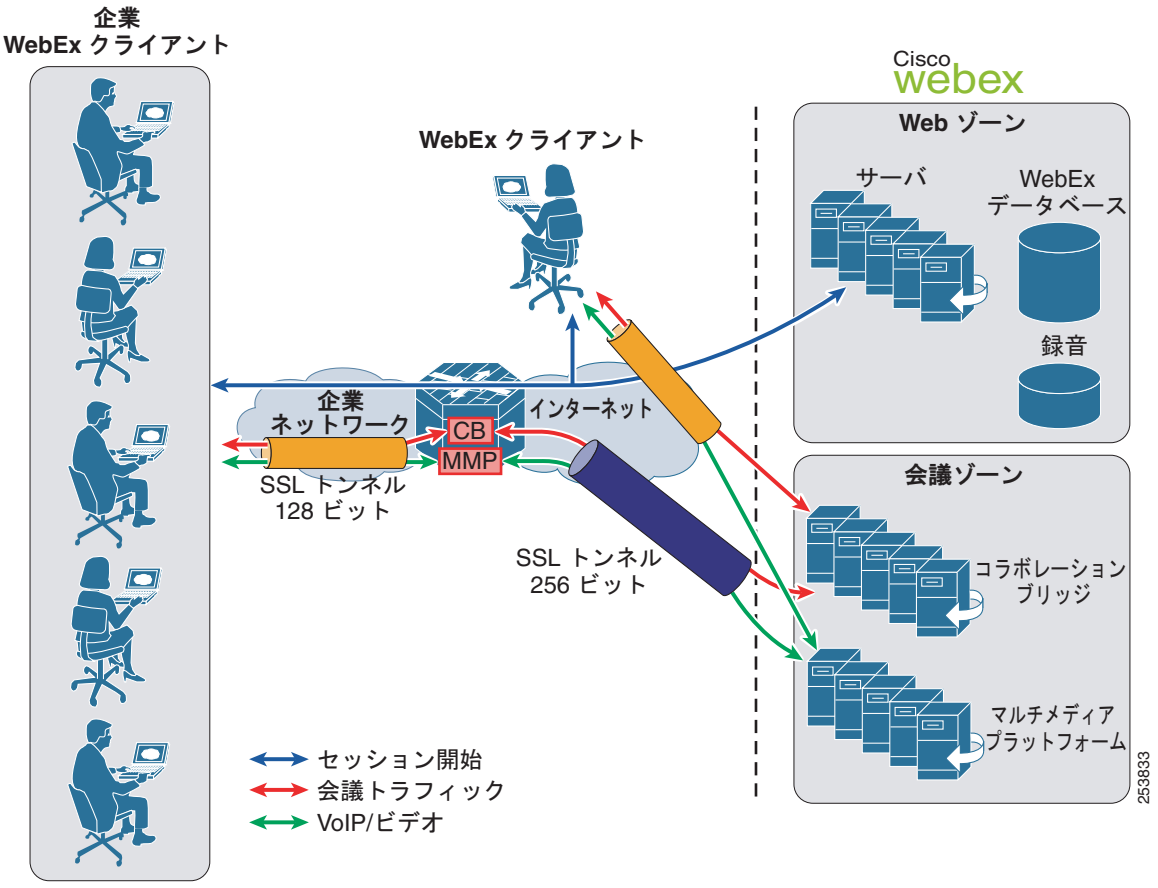
セキュリティの強化を必要とするお客様の場合、クラウド内でトラフィックが復号化されないように、コラボレーション ブリッジおよびマルチメディア コンテンツに対してエンドツーエンド 256 ビット AES 暗号化を実行するオプションもあります。また、エンドツーエンド AES 暗号化をさらに強化するために、PKI ID 検証サポートをオプションで使用できます。エンドツーエンド暗号化の結果、NBR などの一部の機能は失われます。拡張 WebEx セキュリティ オプションの詳細については、次の Web サイトで入手可能な『*Security Overview of Cisco WebEx Solutions*』を参照してください。

http://static.WebEx.com/fileadmin/WebEx09/files_en_us/pdf/whitepapers/cwe_securityoverview.pdf

（注） 拡張 WebEx セキュリティ オプションは、Meeting Center 会議に対してだけ使用できます。WebEx セキュリティ オプションに追加コストはかかりません。

Cisco WebEx リリース WBS27 以降、組織は Aggregation Services Router（ASR; アグリゲーション サービス ルータ）1000 シリーズ向け WebEx ノードを使用して、オプションで WebEx 会議トラフィックを加速できます。ASR 向け WebEx ノード（ルータ内に設置されたブレード）を使用すると、図 22-3 に示すように、クラウドの主要コンポーネントを企業内にオンプレミスで存在するプラットフォーム上に拡張できます。これにより、コラボレーション ブリッジおよびマルチメディア プラットフォームのインスタンスは ASR 上に移動され、パフォーマンスおよび帯域幅は純粋なクラウドベース ソリューションよりも向上します。これは、完全にカスケード化されたソリューションであり、企業内の参加者はノードに、外部参加者はクラウドに接続できます。ノードからクラウドへのフェールオーバーおよびオーバーフローが完全にサポートされ、処理上は透過的です。WebEx ノードの処理は、ユーザにも WebEx サイト管理者にも明らかにされません。ASR 向け WebEx ノードは、スタンドアロンの WebEx SaaS アカウント、およびオンプレミスの MeetingPlace 8.5 音声と連動します。

図 22-3　ASR 向け WebEx ノードを使用した WebEx 配置



参加者が WebEx 会議に参加すると、WebEx クラウドの Web ゾーンがクライアント エントリ ページにサービスを提供し、WebEx クライアントに接続場所を指示します。クライアントには常に、会議に使用できるクラウドベースの会議ゾーンのリストが URL で渡されます。ASR 向け WebEx ノードが組織の WebEx サイトについてプロビジョニングされている場合、ノードのホスト名も会議ゾーンのリストに含まれます。クライアントは、すべてのクラウドおよびオンプレミス リソースに ping し、遅延の観点から、最も近い会議ゾーン インスタンスを判別します。オンプレミス ノードは企業ネットワークを介して利用できるため、これらが最初に応答し、オンプレミス クライアントはこれらのリソースに接続します。また、クライアントは 128 ビット SSL 暗号化を使用してノードに接続します。ノードは、Meeting Center、Event Center、Training Center、および Support Center のサポートを提供します。

（注）　マルチメディア モードで配置された場合、ASR 向け WebEx ノードは VoIP（WebEx クライアント自体から）と Web カメラ ビデオのミキシングが可能です。混合モードの音声には公衆網発信者が含まれ、クラウド内で常に混合されます。

図 22-3 を図 22-2 に示した従来の WebEx 配置モデルと比較すると、セッション開始は引き続きクラウド内の Web ゾーンで行われますが、社内 WebEx クライアントは企業ネットワーク上の ASR 内の WebEx ノードのカンファレンス ブリッジまたはマルチメディア プラットフォームを使用していることがわかります。これはインターネットの帯域幅の節約になり、パフォーマンスが向上します。ASR 向け WebEx ノードは、制御トラフィックと会議コンテンツまたは VoIP とビデオ コンテンツをカスケー

ドし、SSL トンネルを通してクラウドに返します。これにより、外部参加者は会議にアクセスし、Network Based Recording（NBR）をサポートできます。SSL トンネルは WebEx ノードが起動されたときに作成され、企業から WebEx クラウドへのすべての発信接続が行われます。

（注）　ASR 向け WebEx ノードは、コンテンツ ブリッジまたはマルチメディア ノードとして機能するように設定できますが、両方の機能を同時にはサポートしません。データとマルチメディア両方の加速をサポートするには、最低 2 つの WebEx ノード ブレードが必要です。これらは同じ ASR シャーシまたは異なるシャーシに配置できます。企業ネットワーク内に配置できるノードの数に制限はありません。

ASR 向け WebEx ノードを使用したネットワーク トラフィックの最適化の詳細については、「キャパシティ プランニング」（P.22-9）を参照してください。

ASR 向け WebEx ノードをマルチテナント キャパシティで配置する可能性もあります。相互の社内で作業するスタッフと緊密に連携して作業する 2 つの企業が、他方の WebEx サイトを自社の ASR ノード上に定義できます。つまり、企業 B のスタッフが自社の WebEx サイトに企業 A を介してアクセスする場合、ローカル ASR ノードを使用して会議を加速しながら、企業 A の帯域幅を節約できます。この機能は、複数の WebEx サイトを持つ組織にも役立ちます。

Cisco WebEx リリース WBS27-FR20 から、Meeting Center で H.264 AVC/SVC コーデックを使用した高画質ビデオを会議で使用できるようになりました。このような環境を展開するには、より広いネットワーク帯域幅が必要です。高画質ビデオのネットワーク トラフィック最適化の詳細については、「キャパシティ プランニング」（P.22-9）を参照してください。

（注）　Cisco TelePresence は、OneTouch を使用して WebEx を統合します。Cisco TelePresence WebEx OneTouch の詳細については、http://www.cisco.com/en/US/solutions/ns669/webex_engage.html で入手可能なマニュアルを参照してください。

ハイ アベイラビリティ

WebEx クラウド自体は、高レベルの冗長性を持ち、シスコによって管理されます。ASR 向け WebEx ノードについては、ノードに障害が発生するか輻輳した場合、ユーザ会議はクラウドに再接続します。クライアントが会議ゾーンの URL に ping すると、ASR ノードから応答がないため、クライアントは別の会議ゾーンに接続します。ノード上にアクティブな会議があり、ノードがオフラインになった場合、参加者がすべて内部であっても、クラウド内にコンテンツのコピーがキャッシュされています。WebEx クライアントは別の会議ゾーンに再接続し、ユーザの介入なしに会議は続行されます。

キャパシティ プランニング

特定のお客様について、同時会議の実際の数は本質的には無制限です。WebEx 会議のタイプが異なると、参加者数に関するキャパシティも異なります。詳細な製品比較表については、次の Web サイトで入手可能な『*Cisco WebEx Web Conferencing Product Comparison*』を参照してください。

http://www.cisco.com/en/US/prod/ps10352/product_comparison.html

ASR 向け WebEx ノードのキャパシティは、どのような機能のために実装されるかによって異なります。コラボレーション ブリッジ（Web 会議）として配置される場合、ノードは最大 500 人の参加者をサポートします。ノードが最大参加者の制限に達すると、WebEx クライアントは代替オンプレミス ノードを使用するか、クラウドに直接オーバーフローします。配置する ASR ノード数に制限はなく、冗長性およびキャパシティのために複数のノードにわたって Web 会議をカスケードできます。

VoIP とビデオのローカルでの切り替えのために使用する場合、ASR 向け WebEx ノードのサイジングは、大なり小なりノードのパフォーマンスに影響するさまざまなビデオおよび VoIP トラフィック タイプがあるため、少し複雑です。マルチメディア会議のノードのサイジングに役立つように、11,600 ポイントから始まるポイント システムがあり、ノードを通過するストリームのタイプと数に従って、ポイントはこの合計から減少します。表 22-3 に、VoIP およびビデオのさまざまなタイプと、消費するポイントを示します。Web 会議バージョンのノードの場合と同様に、マルチメディア ノードによってキャパシティが使い果たされると、WebEx クライアントは単純に使用可能な別の ASR ノードまたはクラウドに接続します。これにより、特定のノードのキャパシティが過剰に利用される、予期しない偶発的なビジー期間のキャパシティの問題が緩和されます。

表 22-3　ビデオまたは VoIP のタイプによって消費される ASR 向け WebEx ノードのポイント

統合 VoIP またはビデオのタイプ	使用ごとのポイント	1 つのサービスを使用する場合の最大キャパシティ
アクティブ ビデオ 360p + 5x90p	97	120
アクティブ ビデオ 180p	18	640
アクティブ ビデオ 180p + 6x90p	60	192
シングル ポイント ビデオ	8	1,450
VoIP	19	600
音声ブロードキャスト	6	1,933

アクティブ ビデオは、次の解像度で発言中の参加者がメインのビデオ ウィンドウに表示され、他の参加者がサムネール イメージとして表示されることを意味します。

- 360p：640x360 の解像度
- 180p：320x180 の解像度
- 90p：160x90 の解像度

（注）　マルチポイント ビデオのポイントは、会議中にビデオ パネルを見る参加者ごとに差し引かれます。WebEx クライアントごとに最大 6 つの Web カメラ ビデオ セッションを表示できますが、どれを表示するかは各参加者が制御できます。

表 22-3 には、控えめな見積もりを示しています。ただし、使用状況を正確に予測してユーザの動作を制御することは困難です。システムの平均的な負荷を処理するのに十分なリソースをプロビジョニングし、ピーク時使用時間にはクラウドにオーバーフローすることを推奨します。

ネットワーク トラフィック プランニング

インターネットへのトラフィックが増加するにつれて、ネットワーク トラフィック プランニングを考慮することが重要になります。WebEx アーキテクチャを発展させてオンプレミス ASR ノードを含めることにより、パフォーマンスを最適化でき、インターネット アクセスの帯域幅を大幅に節約できます。表 22-4 に、WebEx 会議中に企業ネットワークに負荷をかける可能性があるさまざまなトラフィック タイプを示します。WebEx にとってネイティブではない唯一のトラフィック タイプは、IP テレフォニーです。IP テレフォニーは、WebEx と統合されたオンプレミスまたはオフプレミスの会議サービスで使用される場合があります。

表 22-4　WebEx 会議トラフィックの帯域幅見積もり

トラフィック（テスト シナリオ）	平均（kbps）	最大（kbps）
アイドル会議： iPad（16G）、iPhone（3G）、および Blackberry Bold9700 は、データ接続に WiFi ネットワークを使用します。	0.8（PC 用） 8.9（iPad 用） 0.17（iPhone 用） 0.42（Blackberry デバイス用）	3.7（PC 用） 9（iPad 用） 0.4（iPhone 用） 0.45（Blackberry デバイス用）
デスクトップ共有（30 秒の遷移のスライド表示）	43（PC 用） 95（iPad 用） 67（iPhone 用） 24.8（Blackberry デバイス用）	598（PC 用） 241（iPad 用） 232（iPhone 用） 29.9（Blackberry デバイス用）
プレゼンテーション共有（5 秒の遷移のスライド表示）	6.5（PC 用） 30（iPad 用） 23（iPhone 用） 54.56（Blackberry デバイス用）	7.5（PC 用） 62（iPad 用） 41（iPhone 用） 55.28（Blackberry デバイス用）
ビデオ（15 fps で 352 x 288 の解像度の Web カメラ）	172	298
ビデオ標準画質（160x90 の解像度で最大 10 fps の 6 サムネール ビデオ）	350	500
ビデオ高画質中画面（320x180 の解像度で最大 12 fps の Webcam）	300	500
ビデオ高画質大画面（640x360 の解像度で最大 30 fps の Webcam）	900	1,500

ユーザによる WebEx の実際の使用方法によって、会議で生成されるトラフィック量は大きく異なります。たとえば、参加者がネイティブ プレゼンテーション共有（ドキュメントは共有の前に WebEx サイトにロードされます）を使用する場合、生成されるデータはデスクトップを共有する場合よりも大幅に少なくなります。大企業の場合、特にインターネット アクセス ポイントなどのネットワーク内の混雑するポイントで、このことを理解して正しいトラフィック エンジニアリングを確保することが重要です。煩雑時にホストされる平均会議数と平均参加者数を事前に見積もる必要があります。そのあとで、これらの会議のタイプと特性に応じて、帯域幅の要件を見積もることができます。ネットワーク トラフィック プランニングの詳細については、次の Web サイトで入手可能な『*WebEx Network Bandwidth White Paper*』を参照してください。

http://www.WebEx.com/pdf/wp_bandwidth.pdf

説明したように、ASR 向け WebEx ノードは、コラボレーション ブリッジおよびマルチメディア プラットフォーム エンジンをオンプレミスでプルするために実装できます。ASR ノードの影響を定量化するために、表 22-5 および表 22-6 に理論的な帯域幅の節約の例を示します。これらの例では、かなり大規模なお客様の配置が前提となっています。それぞれピーク時には同時に 1,000 人の会議参加者があり、例ごとに 2 つの異なる平均参加者数が数多くの別々の会議に分散しています。例 1 ではデスクトップ共有が使用され、例 2 ではプレゼンテーション共有が使用されます。どちらの例でも、組織のインターネット アクセス パイプ全体で WebEx トラフィック帯域幅は大きく削減されます。

表 22-5　帯域幅計算例のパラメータ

パラメータ	例 1	例 2
ピーク時の参加者数	1,000	1,000
会議あたりの平均参加者数	6	10
内部参加者の比率	80%	50%
内部プレゼンターの比率	90%	90%
VoIP を受信する平均参加者数	10%	30%
ビデオを受信する平均参加者数	30%	40%
平均会議トラフィック帯域幅	43 kbps	6.5 kbps
320x180 の解像度の高画質ビデオを使用した平均ビデオ トラフィック帯域幅	300 kbps	300 kbps
平均 VoIP 帯域幅	35 kbps	35 kbps

表 22-6　帯域幅見積もり計算の例

	例 1		例 2	
トラフィック タイプ	ノードを使用しない場合の帯域幅	ノードを使用する場合の帯域幅	ノードを使用しない場合の帯域幅	ノードを使用する場合の帯域幅
平均会議トラフィック帯域幅	34 Mbps	1 Mbps	22 Mbps	1 Mbps
平均シングルポイント ビデオ トラフィック帯域幅	72 Mbps	15 Mbps	60 Mbps	12 Mbps
平均 VoIP 帯域幅	3 Mbps	1 Mbps	5 Mbps	1 Mbps

（注）　表 22-5 および表 22-6 の例は、2 つの ASR 向け WebEx ノードが配置されることを前提としています。1 つはコラボレーション ブリッジ モード、もう 1 つはマルチメディア モードです。

設計上の考慮事項

Cisco WebEx SaaS ソリューションを実装する場合は、次の設計上の考慮事項に従ってください。

- 通常、コラボレーティブ会議システムによって、正時のコール処理の負荷が大きくなります。シスコ代理店と従業員は、コラボレーティブ会議固有のパラメータが設定されたキャパシティ プランニング ツールにアクセスして、大規模構成の Cisco Unified Communications システムのキャパシティを計算できます。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を http://tools.cisco.com/cucst で入手できます。
- ASR 向け WebEx ノードは、通常は DMZ 内にあります。これは、WebEx クラウドの拡張として機能し、したがってクラウドから管理されるためです。ただし、DMZ の要件はなく、ノードはネットワーク内の任意の場所に配置できます。WebEx クラウドは、ノードへの着信接続を行いません。セキュアな接続は常にノードからクラウドへポート 443 で開始されます。

- WebEx クライアントおよび WebEx ノードからのすべての接続は、クラウドに対して開始されます。通常、イントラネット デバイスがインターネットへの TCP 接続を開始することをファイアウォールが許可するかぎり、ネットワーク ファイアウォール内の開いているピンホールは必要ありません。
- WebEx 高画質ビデオがサードパーティのオーディオ ブリッジに組み込まれている場合は、発言中の参加者のビデオではなく、プレゼンタのビデオが発言中の参加者のウィンドウに表示されます。
- シスコのさまざまなコラボレーティブ クライアント製品の詳細と、それらがコラボレーティブ会議ソリューションにどのように適しているかについては、「Cisco Collaboration クライアントおよびアプリケーション」（P.24-1）を参照してください。

Cisco Unified MeetingPlace

Cisco Unified MeetingPlace では、Cisco WebEx コンテンツ共有の利点と機能を、コラボレーション会議の音声部分と標準ベースのビデオ部分をオンプレミスでホストする機能と結合できます。Unified Communications ソリューションを購入されたお客様は、既存の導入環境を活用し拡張して、完全な SIP アーキテクチャを使用した音声およびビデオ会議を取り入れることができます。Unified MeetingPlace の導入環境は、スケーラビリティ、スケジューリング インターフェイス オプション、メディア リソース オプション、必要となるハイ アベイラビリティの程度など、いくつかのオプションによって異なります。これらのオプションについては、この項で詳しく説明します。

Unified MeetingPlace アーキテクチャでは、2 つの異なる展開モデルが使用できます。

- マルチノードの Unified MeetingPlace 音声と WebEx サイト（大規模なグローバル企業向け）
  - 複数の会議ノードを使用して G.711 音声ポートを 14,400 まで拡張できるスケーラビリティを提供します。
  - 音声会議にアクティブ/アクティブの復元性を提供します。
  - Cisco UCS プラットフォームで仮想化のサポートを提供します。
  - 強化された WebEx 統合機能を提供します。
  - 内部ネットワーク ユーザ向けの Web 会議をオンプレミスでミキシングするために、MCS または ASR 1000 向け WebEx ノードのオプション サポートを提供します。
  - アクティブ ユーザ用にユーザベースのライセンスを提供し、ポートにはハードウェアベースのサーバ キャパシティを提供します。

（注）　マルチノード展開のサポートは、Cisco Unified MeetingPlace 8.5 以降のリリースで提供されます。

- Unified MeetingPlace Scheduling モデル
  - Unified MeetingPlace 設置ベースのお客様のみ使用可能です。
  - 新規のお客様または設置ベースのお客様が Web 会議を使用しない音声 / ビデオ専用（WebEx なし）として使用できます。
  - ブラスト発信ダイヤルによる継続会議を提供します。
  - Cisco Unified Communications Manager ビデオ テレフォニーのアドホック サポートを提供します。
  - Cisco Unified MeetingPlace Express Media Server（EMS）を使用して最大 1,200 音声ポート、または G.711 で 2,000 音声ポートまで拡張できるスケーラビリティを提供します。
  - 手動フェールオーバーによるアクティブ / ウォーム スタンバイの復元性を提供します。

（注）　この章では、特に音声、ビデオ、および Web 共有ソリューションについて説明します。ただし、Unified MeetingPlace では、音声だけ、音声とビデオだけ、または音声と Web 共有だけを利用する展開もサポートされます。

ここでは、Cisco Unified Communications 環境における Cisco Unified MeetingPlace のシステム レベルの設計ガイドラインを示します。この章では、Unified MeetingPlace のシステム設計に関係のないハードウェア要件やソフトウェア コンポーネント設定については説明しません。このようなトピックについては、次の Web サイトで入手可能な Unified MeetingPlace の製品マニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html

（注）　Cisco Unified MeetingPlace 8.*x* Web 会議ソリューションの実装には、WebEx サイトの購入が必要です。WebEx サービスは、Cisco Unified MeetingPlace のライセンスとは別です。

Unified MeetingPlace アーキテクチャ

ここでは、各 Unified MeetingPlace コンポーネント、およびソリューションにおける各コンポーネントの機能の概要について説明します。

Unified MeetingPlace Meeting Director Server

Meeting Director ノードは、WebEx Scheduling フロント エンドを使用したマルチノード展開用に、いくつかの機能をサポートします。これはマルチノード構成をサポートするために使用される必須コンポーネントです。Meeting Director モジュールには、音声コマンド用の双方向通信パス専用に発信 TCP 443 を使用して統合を行うために、WebEx Collaboration Cloud への WebEx Telephony Service Provider（TSP; テレフォニー サービス プロバイダー）接続が含まれています。Meeting Broker Director は、均等なロード シェアリングで、異なる会議ノード間の音声会議を分散させる処理を行います。Events Aggregator は、会議ノードのキャパシティとリアルタイムに発生するイベントをモニタします。UserSync は、WebEx サイトからすべてのプロファイルを同期させるのに使用されます（有効にした場合）。

マルチノード システムには、冗長性のために 1 つのプライマリ Meeting Director ノードと 1 つのセカンダリ Meeting Director ノードがあります。これらは社内ファイアウォールの背後にあるお客様の任意のデータ センターに配置できます。プライマリ Meeting Director に障害が発生した場合、セカンダリ Meeting Director がアクティブになります。Meeting Director は両方ともリージョン内のマスターとして設定し、システムの復元性をより高めるために別のデータ センターに配置することを推奨します。

「複合ノード」により、Meeting Director と会議機能の両方が提供されます。このノードは、1 つのシステム内の会議ノードが 4 つ未満である場合にサポートされます。会議ノードが 4 つを超える場合は、両方の Meeting Director が 1 台の専用ハードウェア サーバ（Cisco MCS または UCS）に存在する必要があります。

Unified MeetingPlace アプリケーション サーバ（会議ノード）

Unified MeetingPlace ソリューションでは、Unified MeetingPlace アプリケーション サーバ（マルチノード構成では会議ノードとも呼ばれる）が中心になります。これは Unified CM または Session Management Edition 呼制御システムから SIP トランキングによって音声およびビデオ ミキシング機能を提供します。会議をホストするためには、少なくとも 1 つの会議ノードが必要です。会議ノードの追加により、キャパシティと復元性が向上します。

Unified MeetingPlace アプリケーション サーバは、Linux オペレーティング システムと IBM Informix Dynamic Server（IDS）データベースを実行している Cisco Media Convergence Server（MCS）または Unified Computing System（UCS）プラットフォーム上にインストールされ、企業ネットワーク内の音声と標準ベースのビデオ会議をミキシングする音声 / ビデオ会議ノード コンポーネントとして機能します。Unified MeetingPlace アプリケーション サーバは、ソリューションのメディア サーバを制御し、マルチノード構成の Unified MeetingPlace Meeting Director コンポーネントと通信します。Unified MeetingPlace アプリケーション サーバは、SIP Back-To-Back User Agent（B2BUA; バックツーバック ユーザ エージェント）をサポートします。また、着信および発信コールバックのコール送信用の Cisco Unified CM または Session Management Edition（SME）との SIP トランク接続経由でコールを送信 / 受信します。Cisco Unified MeetingPlace Express Media Server も、Unified MeetingPlace アプリケーション サーバ上に共存インストールできるオプションのソフトウェア コンポーネントで、ほとんどのお客様に適したメディア ミキサーです。オプションの Hardware Media Server を使用することにより、ノードごとのスケーラビリティが高まります（音声ノードごとに最大 2,000 の G.711 音声ポート）。

メディア サーバ

Cisco Unified MeetingPlace メディア サーバは、音声およびビデオ会議機能をソリューションに提供します。これには次の 2 つのオプションがあります。

- Unified MeetingPlace Express Media Server（EMS）
- Hardware Media Server（HMS）

Express Media Server は Cisco Unified MeetingPlace のオプションで、コスト効率が高く、推奨されるオプションです。Unified MeetingPlace アプリケーション サーバ上に共存するソフトウェアで音声ミキシングと標準ベースのビデオ スイッチングを実行します。EMS では、Cisco Unified MeetingPlace の音声 / ビデオだけの展開用に、単一ボックス ソフトウェアだけのソリューションが可能です。または、マルチノード構成で展開することもできます。EMS インスタンス間でメディアをカスケードすることはできません。そのため、Unified MeetingPlace EMS ソリューションのキャパシティは、インストール先の MCS または UCS プラットフォームに依存します。または、マルチノード展開でのスケーラビリティを確保するために複数の Unified MeetingPlace アプリケーション サーバおよび Express Media Server をインストールしているかどうかに依存します。マルチノード配置でのスケーラビリティにより、G.711 ポートを最大 14,400 まで拡張できます。これには WebEx Scheduling モデルを使用する必要があります。EMS 間のカスケーディング機能はありません。HMS オプションおよび EMS マルチノード展開オプションにより、ノードごとのキャパシティがさらに向上します。

Express Media Server での最終的なキャパシティでは、G.711 音声だけの場合に、音声会議用として最大数の同時ポートが提供されます。G.729 または G.722 音声コーデックが必要な場合、キャパシティは大幅に小さくなります。また、標準ベースのビデオ ミキシングを使用する場合、ミキシングのタイプと最大帯域幅の設定によってキャパシティはさらに小さくなります。たとえば、G.711 音声だけを使用する Cisco UCS B シリーズ ブレード サーバでは、最大 1,200 ポートをサポートできます。最大のキャパシティを実現するために、コールが G.729 または G.722 で WAN を通過し、Unified MeetingPlace 会議ノードまたは単一システムで終了するように、Cisco Integrated Services Router（ISR; サービス統合型ルータ）でネットワーク層の音声コーデックを G.711 にトランスコーディングすることを強く推奨します。詳細については、「キャパシティ プランニング」（P.22-37）を参照してください。

Hardware Media Server は、Unified MeetingPlace ソリューション固有のブレードが装備された Cisco Unified MeetingPlace 3515 または 3545 です。音声ブレードとオプションの標準ベースのビデオ ブレードがあり、どちらにもそれぞれ音声会議とビデオ会議を提供するためのオンボード DSP リソースがあります。HMS は、Unified MeetingPlace アプリケーション サーバによって SIP API および Unified MeetingPlace Media Control プロトコルを介して制御されます。HMS はオーディオ ストリームとビデオ ストリームのカスケードをサポートしているため、複数の HMS 3545 シャーシを 1 つのロケーションに展開して、必要なキャパシティとハイ アベイラビリティを実現できます。HMS をネットワーク全体に分散させることはできません。Unified MeetingPlace アプリケーション サーバと同じ

データ センターに設置する必要があります。HMS 標準ベースのビデオは、「Continuous-Presence（連続表示）」を提供します。これは標準形式でビデオ ストリームあたり最大 2 MB をサポートする合成ビデオです。また、HMS ビデオはトランスコーディングとレート変換も完全にサポートします。これは、標準ベースのビデオで高度なビデオ MCU 機能を提供するために重要な機能です。高品位形式は現在サポートされていませんが、HD ビデオ デバイスは標準形式の会議に参加できます。

EMS または HMS を使用するように Unified MeetingPlace アプリケーション サーバを設定できますが、2 つを同じ会議ノードで一緒に使用することはできません。ただし、一方から他方へ切り替えるのは比較的簡単です。どちらを使用しているかはユーザには見えませんが、サポートされるビデオ形式と、発言中の参加者または Continuous-Presence（連続表示）、レート変換、トランスコーディング、ビデオ レコーディング、ビデオ ミュート、HD ビデオ機能などの機能に違いがあります。EMS と HMS では、機能に大きな違いがいくつかあります。したがって、選択する前にこれらの違いを確認することが重要です。詳細については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

MCS または ASR 向け WebEx ノード（オプション コンポーネント）

Unified MeetingPlace ソリューションの設計は、システムでホストされる会議の性質に影響を受けます。たとえば、会議に内部参加者だけが含まれるか、外部参加者も許可されるかなどです。Unified MeetingPlace ソリューションのすべての Web 会議は WebEx によって提供されます。ただし、MCS 向け WebEx ノードまたは ASR 1000 向け WebEx ノードを使用することにより、オプションで、必要に応じてコンテンツ共有リソースをオンプレミスでプルできます。すべての会議に外部参加者が含まれる場合、またはお客様が WebEx Collaboration Cloud だけを使用する場合は、MCS または ASR 1000 向け WebEx ノードは必要ありません。ただし、すべての音声、ビデオ、およびコンテンツ共有をオンプレミスのままで内部会議を行う要件がある場合は、MCS 向け WebEx ノードを配置する必要があります。ASR 向け WebEx ノードでは、内部 Web 会議の参加者と WebEx Web カメラ高画質ビデオ（HQ ビデオ）の両方またはいずれかがオンプレミスでミキシングされます。このノードは、本質的に、専用の MCS または ASR 1000 ハードウェアと WebEx ソフトウェアを使用して、WebEx クラウドのコラボレーション ブリッジ テクノロジーをお客様の組織に拡張します。Unified MeetingPlace アプリケーション サーバとは直接通信します。ただし、WebEx サイト管理を介して操作および管理されるため、ノードが組織の WebEx サイトへの発信 TCP ポート 443 SSL 接続を開始できるように、インターネットへの接続が必要です。

WebEx クライアントは、ASR 向け WebEx ノードの場合と同じ方法で MCS 向け WebEx ノードを見つけます。WebEx ノード名がクラウド内でプロビジョニングされ、WebEx サイトへの初期接続後に、会議ゾーンの URL のリストが会議エントリ ページからクライアントに渡されます。内部だけの会議の場合は、MCS 向け WebEx ノードのホスト名だけがクライアントに渡されます。これにより、すべてのユーザは MCS 向け WebEx ノードに内部的に接続され、会議情報はその会議の Collaboration Cloud にカスケードされません。ASR または MCS 向け WebEx ノードでの外部会議の場合は、登録ユーザにはクラウドベースの URL と MCS 向け WebEx ノードのホスト名があり、外部ユーザ（ゲスト）にはクラウドベースの URL だけがあります。次に、クライアントはすべての会議ゾーンに ping し、遅延が最小の URL に接続します。つまり、すべての MCS 向け WebEx ノードは負荷を共有し、特定のユーザが特定のサーバを使用するように指定できません。一般的には、ユーザは最も近いノードに接続されますが、ネットワークの状況や輻輳によってはそうならない場合もあります。外部会議のゲスト ユーザは常に Collaboration Cloud に接続され、内部ユーザは最も近い MCS または ASR 1000 向け WebEx ノード上にいます。MCS または ASR 1000 向け WebEx ノードとクラウドのユーザは、会議中、共有割り当てを持つ任意のユーザによって共有されるコンテンツを表示できます。

（注）　MCS 向け WebEx ノードと ASR 向け WebEx ノードは異なる製品です。MCS 向け WebEx ノードはコラボレーション ブリッジ機能（マルチメディアではない）だけを提供し、Unified MeetingPlace 8.*x* ソリューションに固有です。WebEx SaaS 実装には使用できません。Web 会議と HQ ビデオをオンプレミスでミキシングする ASR 向け WebEx ノードの詳細については、「Cisco WebEx Software as a Service」（P.22-4）を参照してください。

（注）　MCS 向け WebEx ノードでホストされる内部会議は、Meeting Center 会議だけをサポートします。Event Center および Training Center 会議トラフィックを MCS 向け WebEx ノード上で集約できますが、外部会議としてしか指定できません。WebEx HQ ビデオと Network Based Recording（NBR）サービスはクラウドで提供されるため、内部会議ではどちらもサポートされません。WebEx HQ ビデオと NBR レコーディングの両方を提供するのは、「外部」としてスケジュールされる会議だけです。

また、MCS 向け WebEx ノードは HQ ビデオ（Web カメラのみ）と WebEx VoIP スイッチングをサポートしないことに留意してください。そのため、WebEx Web カメラ ビデオがサイトに対して無効ではない場合は、クラウドに伝播され、そこで切り替えられます。「内部」としてスケジュールされる会議では、Web カメラ ビデオを取得するための WebEx Collaboration Cloud へのデータ接続が備わっていないので、ユーザが Web 会議の帯域幅集約とクラウド内で混合される Web カメラ ビデオの両方を使用するためには、会議を「外部」としてスケジュールする必要があります。お客様は Unified MeetingPlace の標準ベースのビデオを使用するか、クラウド内の WebEx HQ ビデオを使用するかを選択する必要があります。さらに、ASR 向け WebEx ノードを配置することにより、ASR での Web カメラ ミキシングを使用して WebEx Web 会議と WebEx HQ ビデオの両方の帯域幅集約を実現できます。

また、お客様は WebEx サイトの HQ ビデオを無効にし、ビデオを使用しない、またはネイティブの Web カメラで Unified MeetingPlace 標準ベースのビデオ（H.323、SIP、および SCCP デバイスのみ）を使用するという選択をすることも可能です。

WebEx サイト

すべての Unified MeetingPlace 8.*x* Web 会議ソリューションには WebEx サイトが必要です。特定の組織の WebEx サイトの形式は、*companyXYZ*.**WebEx.com** です。大企業では、Meeting Center だけを使用することも、WebEx の全センターの組み合わせを使用することもできます。これは Enterprise Edition と呼ばれ、Meeting Center（MC）、Event Center（EC）、Training Center（TC）、および Support Center（SC）をサポートします。Cisco Unified MeetingPlace 8.5 以降のリリースでは、WebEx ノードがある場合もない場合も、アクティブ ホスト、指定ホスト、ポート、または分単位用の WebEx パッケージがすべてサポートされます。

Event Center と Training Center は、追加の統合機能を提供します。Event Center 音声ブロードキャストにより、Unified MeetingPlace 音声の効率的な使用が可能になります。イベント会議のプレゼンタだけが Unified MeetingPlace 音声システムに接続され、すべての参加者（最大 3,000）はブラウザの URL によって参加し、（マルチキャストではなく）ストリーミング モードで音声ブロードキャストを聞くことができます。Unified MeetingPlace の音声では、必要に応じて自動ミュートを使用することに

より、1 つの大規模な会議で最大 500 の音声ポートをサポートできますが、大規模な会議では、1 対多の役割を果たすために Event Center の音声ブロードキャスト機能を使用することを強く推奨します。Training Center では、音声 /Web サブ会議室を使用し、参加者を入席時にミュートします。

1 つの WebEx サイトは 1 つの Unified MeetingPlace システムだけに結合されます。マルチノード展開モデルの Unified MeetingPlace システムでは、WebEx Scheduling モデルだけを使用する必要があります。1 つの Unified MeetingPlace システムで複数の WebEx サイトをサポートすることはできません。また 1 つの WebEx サイトで複数の Unified MeetingPlace システムをサポートすることはできません。

Cisco Unified MeetingPlace 8.5 以降のリリースと WebEx WBS27 FR 26 以降を使用することで、Unified MeetingPlace をプロビジョニングの必要なしに統合することができます。このリリースを所有する既存の WebEx のお客様は、プロビジョニング要求や変更を行うことなく、Unified MeetingPlace 音声を既存のサイトに容易に追加できます。また、このリリースの WebEx ではデュアル音声ベンダーもサポートされています。そのため、同一サイトでの WebEx 音声と Unified MeetingPlace 音声、または同一サイトでの Unified MeetingPlace 音声と TSP 音声の使用が可能になります。WebEx サイトには、Unified MeetingPlace 展開環境にサイトを結合する主要なパラメータの設定に使用する管理ポータルがあります。WebEx サイトの設定の詳細については、次の Web サイトで入手可能な『*Administration Documentation for Cisco Unified MeetingPlace*』を参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html

（注）　Unified MeetingPlace の音声 / ビデオだけの配置には、WebEx サイトは必要ありません。

WebEx サイトのデュアル音声サポート

リリース 27 FR23 以降を使用する WebEx サイトは、デュアル音声ベンダー サポートという新機能をサポートします。この機能により、次の構成および統合が可能になります。

- WebEx 音声 /VoIP + Unified MeetingPlace 音声
- TSP 音声 + Unified MeetingPlace 音声

デュアル音声ベンダー機能を使用すると、TSP 音声または WebEx 音声を使用する既存の WebEx サイトで、Unified MeetingPlace 音声も設定できます。また、1 つのタイプから別のタイプへ段階的な移行ができるので、新しい将来の会議がすべて Unified MeetingPlace 音声を使用し始めても、最初の音声プロバイダーですでにスケジュールされている将来の会議を引き続き使用することができます。また、この機能により、プロファイルのデフォルト設定に基づいて、世界の異なる地域で異なる音声システムを使用することが可能になります。たとえば、北米の全ユーザが Unified MeetingPlace 音声だけを使用するように設定されていても、シンガポールでは WebEx 音声を使用できます。

また、プロファイルでは両方の音声プロバイダーを提供するように設定できるので、ユーザは会議ごとに各プロバイダーを使用してスケジュールする方法を知っている必要があります。さらに、特定の WebEx セッション タイプについて、スケジュールされた会議タイプに基づいて 1 つのタイプの音声プロバイダーを使用するように設定することも可能です。

デュアル音声ベンダー サポートでは、一方から他方への自動オーバーフローや、両方の音声システムを結合する機能は提供されません。

Unified MeetingPlace 音声では現在、WebEx VoIP 機能との「混合」音声会議はサポートされません。そのため、お客様が VoIP で WebEx 音声を使用する場合は、このデュアル音声ベンダー サポートが設定されている必要があり、ユーザは、この機能を使用するために WebEx 音声 /VoIP オプションを選択することを知っている必要があります。

Cisco TelePresence WebEx One Touch では、この統合のために 1 つのサイト上で WebEx 音声とコールバック機能が必要になります。このデュアル音声ベンダー サポート機能により、TelePresence One Touch 統合セッション タイプだけに WebEx 音声を配置し、他のすべての会議には Unified MeetingPlace 音声を使用することができます。合計 WebEx 音声ポート数のサイジングは、ピーク時にスケジュールされた各 TelePresence 会議に参加する必要のあるピーク音声ユーザの要件によって決定

されます。たとえば、さまざまな TelePresence デバイスが Cisco TelePresence Manager（CTS-Manager）を使用して参加する TelePresence One Touch 会議が 3 つあり、さらに 10 の WebEx 音声ユーザが会議ごとに存在する場合、必要なポート数は、使用中の 3 + (3 * 10) = 33 音声ポートです。それぞれの TelePresence One Touch 会議は、接続される TelePresence デバイスの数に関係なく、各会議用に 1 つのビデオ ストリームを送信し、1 つのオーディオ ストリームを使用します。

ユーザベース ライセンス

Cisco Unified MeetingPlace 8.5 から、ユーザベース ライセンス モデルが使用されます。Unified MeetingPlace の以前のバージョンでは、ポートベース ライセンスが使用されていました。ユーザベース ライセンス モデルでは、お客様は Unified MeetingPlace システム上の「アクティブ」ユーザに基づいてシステムを購入できます。アクティブ ユーザは、Unified MeetingPlace で会議をスケジュールしたり会議をホストしたりする登録アカウントとして定義されます。システムが購入されたユーザ数を超えていないかどうか確認するために、アクティブな使用状況をモニタできるシステム レポートが提供されます。また、アクティブ ユーザ数がライセンスされたユーザ数を超えると、マイナー SNMP アラームが送信されます。Unified MeetingPlace が電話会議をブロックしたり、登録ホストが会議を開くのを妨げたりすることは決してありません。お客様は必要な数のユーザをプロビジョニングすることができ、WebEx で使用できるさまざまなプロビジョニング オプションや Unified MeetingPlace 固有のオプションを使用することによる問題はありません。Unified MeetingPlace データベースは、最大 400,000 のプロファイルをサポートします。

同時に接続する音声発信者の総数に対するシステム キャパシティは、配置されているハードウェア サーバのモデルと数によってまったく異なります。Unified MeetingPlace のオンプレミス ソリューションを設計する際には、ピーク時の使用時間と将来の拡張の両方を考慮する必要があります。2 台の Cisco UCS B シリーズ ブレード サーバまたは C210 シリーズ ラックマウント サーバと Unified MeetingPlace アプリケーションおよび EMS ソフトウェアを配置する場合は、サーバあたり 1,200 の G.711 ポート（合計 2,400 ポート）またはすべての登録ユーザとゲストが使用できる 1,200 の冗長ポートを持つことになります。会議ノードでは、すべての会議でアクティブ/アクティブのロード シェアリングが行われます。一方のサーバがダウンした場合、そのサーバのコールはドロップされ、ユーザはすぐにダイヤルインして戻るか、WebEx 会議室ユーザ インターフェイスからコールバック機能を使用できます。その会議は他方のサーバ（またはリージョン内で最も使用率の低いサーバ）で自動的に再確立されます。Unified MeetingPlace は最大 14 の会議ノードと合計 14,400 の G.711 ポートをサポートします。G.729、G.722、標準ベースのビデオのすべて、またはいずれかが使用される場合、これらのキャパシティの上限は低下します。

Unified MeetingPlace はスケジュールされた会議と予約なし会議の両方をサポートします。予約なし会議は、音声だけ（ビデオが有効になっている場合は音声/ビデオだけ）を使用します。

スケジューリング インターフェイス

Cisco Unified MeetingPlace ソリューションには、次の 2 つのスケジューリング インターフェイス オプションがあります。

- Productivity Tool、One Click、および WebEx スケジューリング インターフェイスを使用する WebEx Scheduling モデル
- Outlook、Lotus Notes、または Web スケジューリング インターフェイスを使用する Unified MeetingPlace Scheduling モデル

多くの場合、ユーザが特定のインターフェイスを使い慣れていることが、どのオプションを選択するかの決定に影響します。ユーザが現在 WebEx SaaS 配置を使用しており、音声/ビデオ リソースをオンプレミスでプルする場合、またはこれが新しい Unified MeetingPlace インストールである場合は、WebEx Scheduling 展開モデルを推奨します。Unified MeetingPlace 8.5 以降のリリースのマルチノード展開には、WebEx Scheduling モデルが必要です。ただし、現在 Unified MeetingPlace が配置されている場合は、同じスケジューリング インターフェイスを維持するのが有益な場合があります。確かに

違いはありますが、どちらにも Web ベースのユーザ スケジューリング ポータルがあり、一般的なカレンダー システム（Outlook または Lotus Notes）と独自に統合されます。また、WebEx Scheduling は Enterprise Edition 会議（Meeting Center、Event Center、および Training Center セッション）をサポートしますが、Unified MeetingPlace Scheduling は Meeting Center セッションだけをサポートします。Unified MeetingPlace 8.5 を展開する新規のお客様は、Unified MeetingPlace Scheduling モデルを使用できません。

WebEx Scheduling の展開

WebEx は、次の 2 つの展開モデルをサポートします。

- 「単一サイト WebEx Scheduling の展開」（P.22-20）
- 「マルチサイト WebEx Scheduling の展開」（P.22-22）

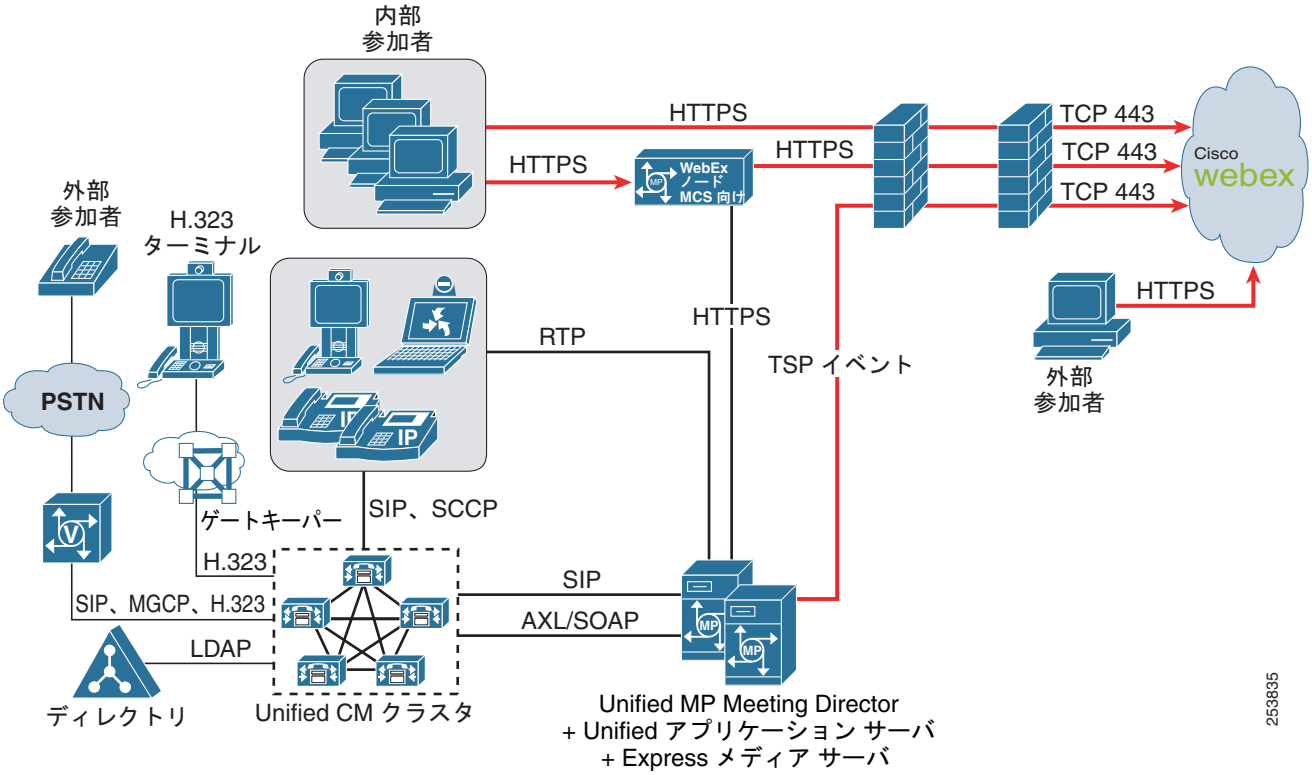
WebEx Scheduling 展開モデルは、Meeting Center だけ、または WebEx Enterprise Edition（EE）をサポートします。WebEx Enterprise Edition は Meeting Center、Event Center、および Training Center セッション タイプを含み、これらはすべて Unified MeetingPlace 音声に統合できます。Meeting Center 会議だけが、MCS 向け WebEx ノードとクラウド（ゲスト ユーザ用）の両方に混在します。Event Center および Training Center は常に外部会議タイプと見なされ、内部ユーザはそれらのセッション タイプについては MCS または ASR 向け WebEx ノードまたはクラウドに参加します。

WebEx Scheduling は最新の WebEx Productivity Tools（「Cisco WebEx Software as a Service」（P.22-4）を参照）をすべて利用し、外部会議のすべての音声および WebEx レコーディングは、Network Based Recording サイトの下の WebEx Collaboration Cloud にホスト アカウントごとに保存されます。

単一サイト WebEx Scheduling の展開

WebEx Scheduling には Unified MeetingPlace Web サーバは必要ありません。会議の招待にあるクリック参加 URL で、ユーザは直接 WebEx サイトにアクセスします。図 22-4 に、WebEx Scheduling、アクティブ/アクティブの冗長性を持つ 2 台の Express Media Server、および MCS 向け WebEx ノードを使用した Unified MeetingPlace ソリューションの例の概要を示します。MCS 向け WebEx ノードはオプションであり（内部だけの会議に必要、また、ASR は Web および HQ ビデオの帯域幅集約も可能）、EMS の代わりに HMS を使用することもできます。

図 22-4　WebEx Scheduling、EMS、および MCS 向け WebEx ノードを使用した Unified MeetingPlace 単一サイト ソリューション



（注）　MCS 向け WebEx ノードが展開されている場合、WebEx Scheduling で Network Based Recording と HQ ビデオ Web カメラをサポートできるのは外部会議だけです。

MCS 向け WebEx ノードまたは ASR 1000 向け WebEx ノードは、お客様の詳細な帯域幅集約の要件や「内部」会議だけの使用が提供されるかどうかに基づいて、オプションで利用できます。音声会議がオンプレミスで発生する一方で、Web 会議はクラウドと WebEx ノードの両方で発生するため、会議に関するすべてのサービス要求は、クラウドに対する Unified MeetingPlace または WebEx ノード Application Programming Interface（API; アプリケーション プログラミング インターフェイス）との Telephony Service Provider（TSP; テレフォニー サービス プロバイダー）API 通信経由で交換および処理されます。システムは効果的に結合され、参加者の消音または発言中の参加者の表示機能などの会議内制御が可能になります。この TSP リンクは、Meeting Director によってクラウドへ向けて確立されます。お客様の WebEx サイトへの接続は、TCP ポート 443 の TLS 暗号化専用ソケット経由で行われます。

ネットワーク要件

このハイブリッド アーキテクチャでは、ファイアウォールを通過して開かれる「着信」ポートは必要ありません。Meeting Director TSP は、（HTTP または HTTPS プロキシではなく）SOCKS プロキシ サーバだけをサポートします。MCS または ASR 向け WebEx ノードは、どのタイプの Web プロキシ システムもサポートしないため、クラウドへの TCP 443 発信が許可される必要があります（配置されている場合）。WebEx 会議に参加するユーザも、ファイアウォールを通過して WebEx Collaboration Cloud に向かう TCP 443 発信だけを使用します。インターネット アクセスを制限するファイアウォール設定が不可欠な場合、WebEx は必要な IP の範囲を公開します。

コンポーネントが企業ネットワーク内のどの場所に展開されている場合でも、すべてのコンポーネント間の最大遅延を 300 ms Round Trip Time（RTT; ラウンドトリップ時間）にすることを推奨します。標準的な VoIP ネットワークのベスト プラクティスは、Unified MeetingPlace のオンプレミス会議リソースを展開する場合にも適用されます。最適な会議パフォーマンスを得るために、Unified MeetingPlace 会議ノードと Unified CM 間の SIP トランキング遅延は、この同じ標準に従う必要があります。

すべてのネットワーク要件については、次の Web サイトで入手可能な『*System Requirements for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html

マルチサイト WebEx Scheduling の展開

マルチサイト展開は、サイトとリージョンから構成されます。キャパシティと復元性に対するお客様の要件に応じて、会議ノード、Meeting Director ノード、そしてオプションで WebEx ノードがデータ センターにインストールされます。

*サイト*は、同様の機能と能力を持つノードの論理グループです。たとえば、サイトには高品位ビデオ機能を備えたノードが含まれる場合があります。サイトはシステム内で固有の名前によって識別され、1 つのリージョンだけに所属できます。1 つのサイトには、リージョン内の任意のノードが含まれます。希望のサイトを、特定ユーザ プロファイルのすべての会議をホストするように設定できます。

*リージョン*は、1 つ以上のサイトのグループです。リージョンはシステム内で固有の名前によって識別されます。システム内に最大 4 つのリージョンを設定でき、リージョンは時間帯の割り当てにも使用されます。

マルチノード Unified MeetingPlace 音声システムのキャパシティは、次のとおりです。

- 14,400 の G.711 音声ポート
- 2 つの Meeting Director ノードと 14 の会議ノード（12 ノード X 1,200 の G.711 ポート = 14,400 ポート、および復元性のために 2 つの追加の会議ノードをサポート）で構成される 16 の Cisco Unified MeetingPlace アプリケーション サーバ ノード
- 上限の 14,400 に達するまで、会議ノードごとに 1,200 ポート（G.711）
- サイトごとに最大 4 ノード
- リージョンごとに最大 2 サイト（2 つの各サイトに最大 2 ノード、または 1 つのサイトに最大 4 ノード）
- 最大 4 つのリージョン

（注） キャパシティは、G.729 または G.722 コーデックの使用、ビデオ使用タイプ、および許可される帯域幅によって、さらに小さくなります。

WebEx Web Conferencing（スケジューリングおよび Web 会議に必要）のキャパシティは、次のとおりです。

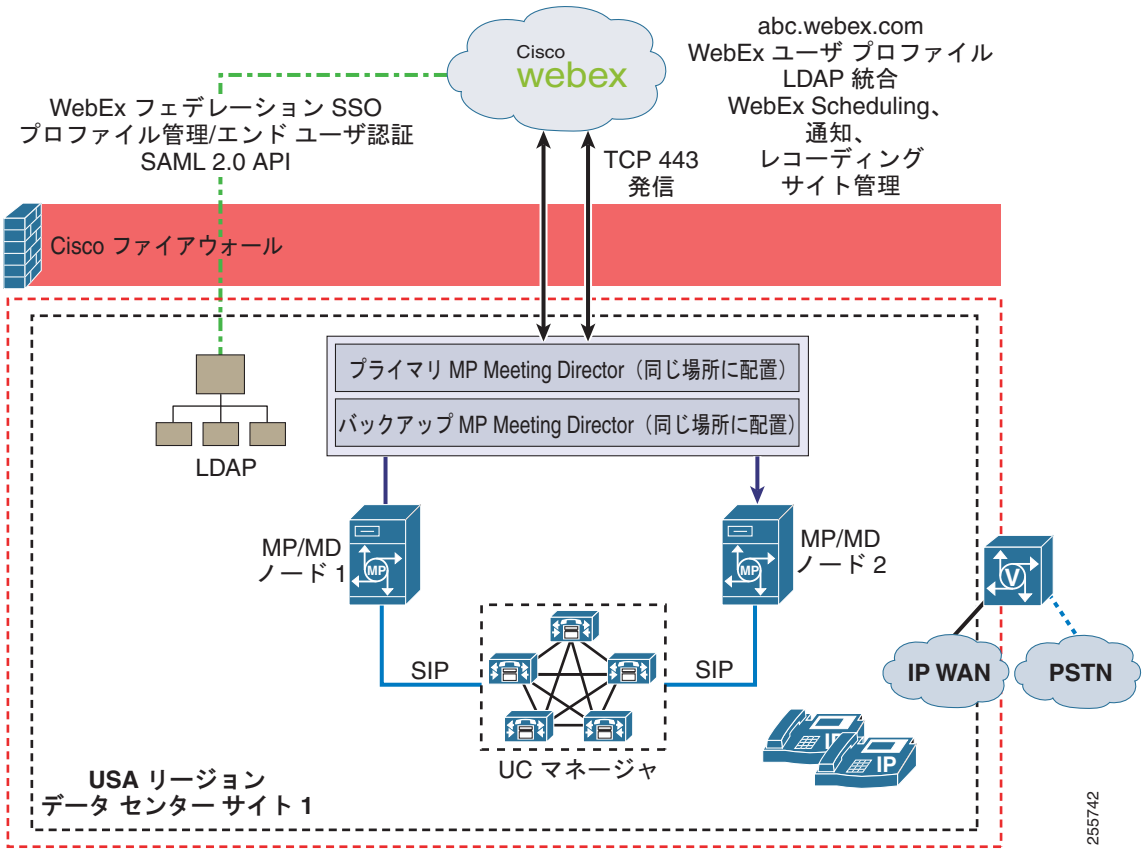
- 14,400 の Web セッション（クラウドとノードの両方またはいずれか）
- 2,000 の内部 Web セッション（MCS 向け Cisco WebEx ノードを使用）、最大 4 つの Cisco WebEx ノード（それぞれ最大 500 セッション）で構成
- ASR 向け Cisco WebEx ノードは、次のものをサポートします。
  - Shared Port Adapter（SPA; 共有ポート アダプタ）ごとの Web 会議（それぞれ最大 500 セッション）
  - SPA ごとの HQ ビデオおよび VoIP（使用状況に基づくキャパシティ）

Unified CM または Session Management Edition ですべての会議ノードへの着信 SIP トランクを順繰りに設定することにより、会議は均等に分散されます。WebEx 会議室内から発信されるコールバックは、すべての会議ノードのトラフィックをモニタする Meeting Director によって分散されます。Meeting Director が新しい会議を開始する際には、その会議をスケジュールしたホストの時間帯に基づいて、リージョン内で最も使用率の低いノードで開始します。着信コールについては、会議に最初に参加する人が、SIP 循環ハント モードに基づいてどの会議ノードに着信するかを決定します。その会議 ID が同じリージョン内または異なるリージョンの異なるノードで開始された場合、ホストが割り当てられている会議ノードにその発信者を自動的にリダイレクトするために、SIP Refer コマンドが自動的に発行されます。同じ会議 ID への発信者はすべて、時間帯、または最初の参加者によって会議が開始されたノードのいずれかに基づいて、システム内の 1 つのノードにルーティングされます。このように、システム内のすべてのユーザは、常にローカルの Unified MeetingPlace ダイヤルイン番号をダイヤルして（またはコールバックを使用して）、世界中の任意の場所の任意の会議に参加します。SIP Refer は、会議をスケジュールしたホストの時間帯に基づいて、その特定の会議に適したノードにユーザを自動的にリダイレクトします。予約なし会議 ID が使用された場合も、そのホストが存在する時間帯に基づいてコールバックが分散されますが、最大限のキャパシティと復元性を確保するために、複数ノード間でのロード シェアリングが使用されます。

マルチノード WebEx Scheduling を使用した集中型展開モデル

図 22-5 の例は、単一サイトでアクティブ/アクティブの復元性を持つ 1 つのリージョンで構成されています。このシステムでは、1 つのサイトおよび 1 つのリージョンに 2 つの Meeting Director または EMS サーバ（あるいはその両方）を展開するために、2 つの Cisco MCS または UCS サーバが必要です。これが集中型展開モデルです。スケーラビリティは 1,200 の G.711 ポートで、アクティブ/アクティブの冗長性があり、両方のサーバにはすべての時間帯からの会議負荷が均等に振り分けられます。Unified CM SIP トランクのサイジングでは、2,400 ポートの SIP トラフィックではなく、ピーク時の同時 SIP トラフィックだけを考慮に入れる必要があります。Meeting Director は、2 つの異なる会議ノードと同じ場所に設置されます。1,200 ポートは一般に、標準的な会議の使用パターンで 20 ユーザ対 1 ポートの比率をサポートできます。したがって、この構成では合計で 24,000 ユーザをサポートできる必要があります。

図 22-5　WebEx Scheduling を使用した Unified MeetingPlace マルチノード展開（1 リージョンの場合）

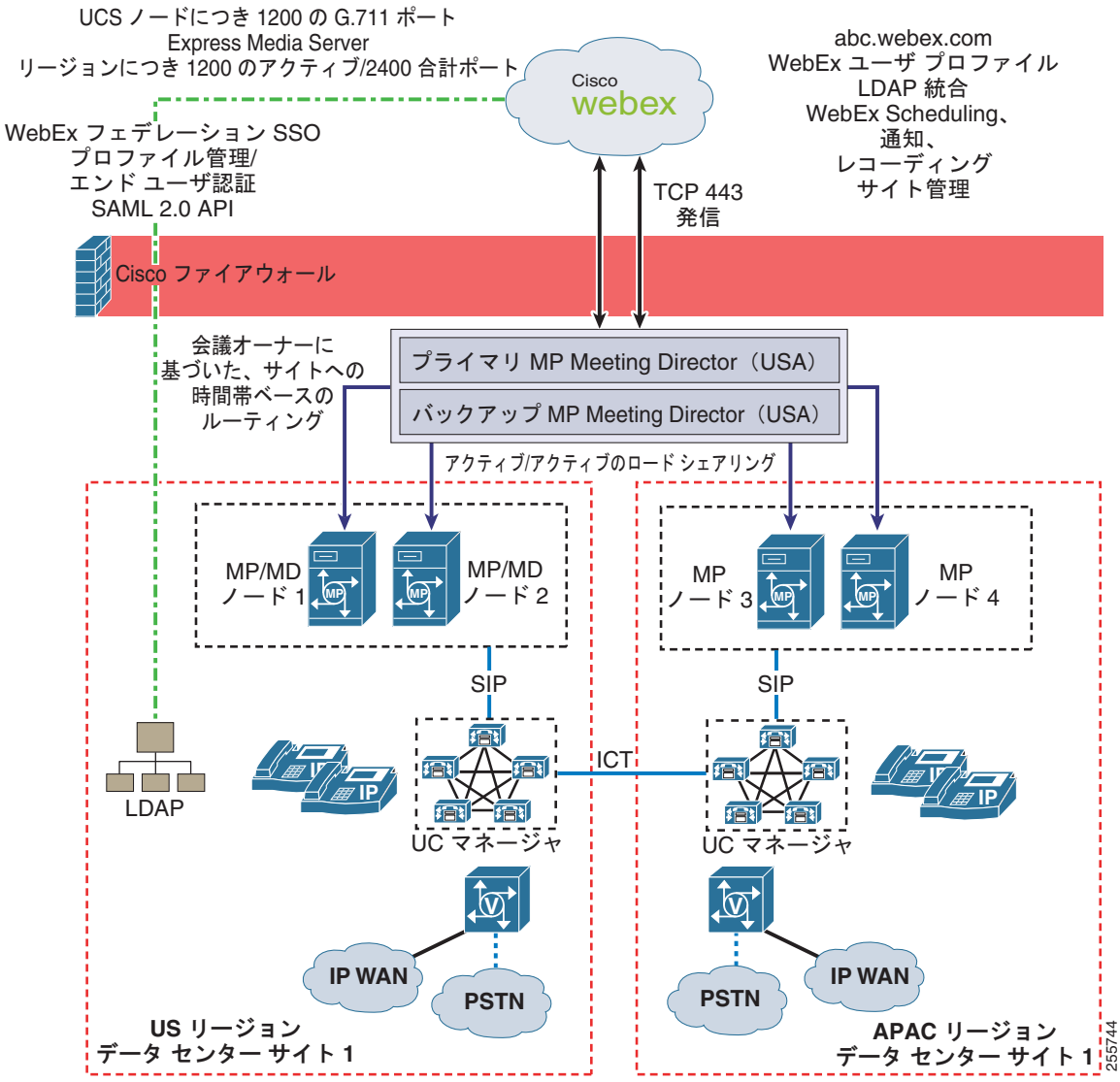


Webex Scheduling を使用した 2 リージョンのマルチノード Unified MeetingPlace 展開モデル

図 22-6 の例は、2 つのリージョンで構成されており、各リージョンにアクティブ/アクティブの復元性を持つグローバルな分散型設計です。また、データ センター サイトはお客様のデータ センター設計に基づいて構成されています。1 つのリージョン内のすべての会議ノードはロードバランスされ、別個のサイトまたはリージョンのノードは、管理設定により、他のリージョンにフェールオーバーすることができます。

このシステムでは、2 つのサイトおよび 2 つのリージョンに 2 つの Meeting Director または EMS サーバ（あるいはその両方）、および 2 つの会議ノードを提供するために、4 つの Cisco MCS または UCS サーバが必要です。スケーラビリティはリージョンごとに 1,200 の G.711 ポートで、アクティブ/アクティブの冗長性があります。Unified CM SIP トランクのサイジングでは、2,400 ポートの SIP トラフィックではなく、ピーク時の同時 SIP トラフィックだけを考慮に入れる必要があります。Meeting Director は、2 つの異なる会議ノードと同じ場所に設置され、お客様の要件に応じてどちらのデータ センターにも配置できます。

図 22-6　WebEx Scheduling を使用した Unified MeetingPlace マルチノード展開（2 リージョンの場合）

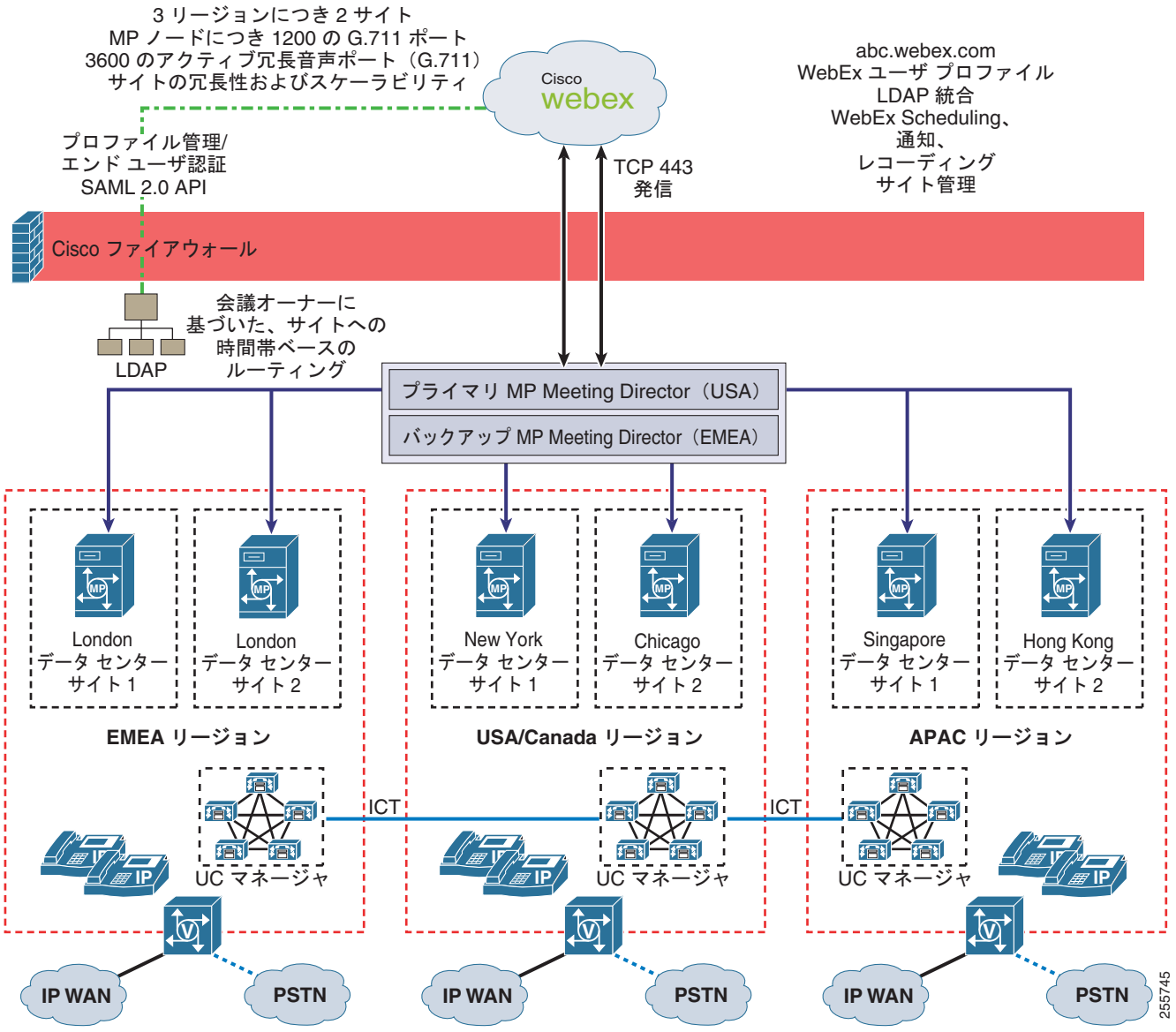


WebEx Scheduling および 3 リージョンを使用した Unified MeetingPlace マルチサイト ソリューション

図 22-7 の例は、3 つのリージョンで構成されており、各リージョンにアクティブ/アクティブの復元性を持つグローバルな分散型設計です。また、サイトの冗長性を確保するために、別個のデータ センター サイトが設定されています。1 つのリージョン内のすべての会議ノードはロードバランスされ、別個のサイトまたはリージョンのノードは、管理設定により、他のリージョンにフェールオーバーすることができます。

このシステムでは、2 つの Meeting Director と 6 つの会議ノードを提供するために、8 台のサーバが必要です。スケーラビリティはリージョンごとに 1,200 の G.711 ポートで、リージョンごとにアクティブ/アクティブの冗長性があります。

図 22-7　WebEx Scheduling を使用した Unified MeetingPlace マルチサイト ソリューション（3 リージョンの場合）



ビデオ

お客様が使用できるビデオには、次の 2 つのタイプがあります。

- Unified MeetingPlace 標準ベースのサードパーティ製の会議室/デスクトップまたは Unified Communications ビデオ（H.323、SIP、または SCCP）
- Web カメラだけを使用した Meeting Center および Training Center 用 WebEx HQ ビデオ

現在はこれらの間に相互運用性がないため、お客様は 2 つのオプションから選択する必要があります。両方を有効にするとエンド ユーザの混乱を招くため、両方を有効にしないでください。

標準ベースの Unified MeetingPlace ビデオに関して、ビデオが Unified MeetingPlace コンポーネントによってオンプレミスでミキシングされる場合、ビデオは標準会議室およびデスクトップ エンドポイント自体に表示されます。Web 会議内の WebEx ビデオ ポッドには表示されないため、WebEx サイトの Web カメラ HQ ビデオ機能は無効にすることを推奨します。そうしないと、ビデオ会議とエンドポイントおよび Web カメラ ビデオが何の結び付きもなく混在して、WebEx アプリケーションに表示される場合があります。ユーザベース ライセンスでは、任意の Unified MeetingPlace システムで、音声とビデオ両方の使用がサポートされます。会議ノードでビデオを有効にすると、使用されるビデオのタイプと帯域幅に基づいて、キャパシティに影響が及びます。

Unified MeetingPlace でサポートされる標準ベースのビデオ デバイスの詳細については、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html

一方、Unified MeetingPlace ビデオ会議が展開されていない場合、ユーザはクラウド内で混合される純粋な Web カメラだけを使用して WebEx HQ ビデオ機能を利用できます。また、ビデオ Shared Port Adapter（SPA; 共有ポート アダプタ）を備えた ASR 向け WebEx ノードが展開されている場合は、オンプレミスで帯域幅集約が発生します。MCS 向け WebEx ノードが展開され、ユーザが会議を「内部」としてスケジュールしている場合は、WebEx HQ ビデオは使用できず、クラウドへのデータ共有接続は行われません。会議が「外部」としてスケジュールされている場合、ユーザは Web カメラ ビデオを見ることができ、Web 会議の帯域幅集約のために MCS 向け WebEx ノードに引き続き接続されます。

Unified Communications Client Services Framework（CSF）デバイスおよび Cisco Unified Video Advantage はいずれも、Web カメラのみ、または SCCP/SIP ビデオ標準ベースのデバイスです。クライアントの会議への参加方法、および有効になっているビデオ オプションによって、エンド ユーザのビデオ エクスペリエンスが決定されます（表 22-7 を参照）。

表 22-7　サポートされるビデオ オプション

ビデオのタイプ	WebEx HQ ビデオ	MeetingPlace ビデオ
H.323、SIP、および SCCP の標準ベースのサポート	なし	あり
Web カメラのサポート	あり	なし
ASR 向け WebEx ノード	あり	なし
内部施設ベース	なし	あり
グローバル アクセス ゲスト/ユーザ	あり	なし

WebEx 所有プロファイルの管理

プロファイル管理を設定する方法は 2 つあります。つまり、WebEx 所有プロファイルまたは Unified MeetingPlace 所有プロファイルです。

WebEx 所有プロファイルの管理では、プロファイルを次の方法でプロビジョニングできます。

- アカウントのサインアップ（自動承認、またはシステム管理者の承認が必要）
- 手動のアカウント作成
- Excel スプレッドシート ファイルから定期的にインポート
- フェデレーション Single Sign-On（SSO; シングル サインオン）オプション（ログイン時にアカウントを自動作成）
- WebEx XML API（カスタムのアカウント管理）

WebEx 所有プロファイルを有効にすると、Unified MeetingPlace は X.509 暗号化リンク経由でクラウドからすべてのユーザ プロファイルを自動的に同期し、Unified MeetingPlace 会議ノードにユーザを作成します。これにより、ユーザはプロファイル番号と PIN コードを使用して、予約なしの音声だけの会議にアクセスできます。

（注）　プロファイル番号は 8 桁の長さで、ユーザ プロファイルの作成時にランダムに割り当てられます。PIN コードは、ユーザが WebEx サイトに最初にログインした際に作成できます。オプションとして、プロファイル番号をカスタマイズすることもできます。その場合は、LDAP のフィールドを WebEx プロファイルのフィールドにマッピングするカスタム コードを使用して、WebEx XML API 経由で LDAP ディレクトリからプロファイル番号を取得します。

Unified MeetingPlace は XML API User Synch モジュール経由で登録ユーザの情報にアクセスし、Unified MeetingPlace 会議ノードのすべてのユーザを自動的に設定します。Meeting Director プライマリ サーバ（インストール サイクルの最初のもの）をインストールする際に、[WebEx Owned Profile] 設定を選択すると、システムは X.509 暗号化リンク経由でクラウドからユーザ プロファイルを自動的に同期するように動作します。

WebEx 所有プロファイルが有効になると、Unified MeetingPlace システムはプロファイル番号と PIN コードを使用します。これは、ユーザが予約なしの音声だけの会議に対してのみ入力するものです。ユーザ プロファイルが新規に作成されると、WebEx サイトと Unified MeetingPlace は、そのユーザにランダムなプロファイル番号を自動的に割り当てます。WebEx サイトへの最初のログイン時に、そのユーザは PIN コードを設定するように要求されます。お客様が LDAP フィールドに基づいて特定の番号をユーザに割り当てる場合は、LDAP フィールドを使用するカスタム コードをプロビジョニングして WebEx プロファイルのフィールドにマッピングするために、WebEx XML API を使用する必要があります。プロファイル番号と PIN の長さの要件は、Unified MeetingPlace のシステム管理パラメータで設定します。プロファイル番号は 4 ～ 8 桁の長さ、PIN コードは 6 ～ 32 桁の長さにすることができます。

（注）　オプションの WebEx Federated Authentication Service（FAS）LDAP 機能を有効にするためには、WebEx 所有プロファイルが必須です。FAS の詳細については、http://developer.webex.com/c/document_library/get_file?groupId=10465&folderId=11421&name=DLFE-201.pdf で入手可能な『WebEx *Federated SSO Authentication Service Technical Overview*』を参照してください。

WebEx XML API

LDAP プロファイルに存在するフィールドを使用して MeetingPlace のプロファイル ID の作成を制御する場合は、WebEx XML API を呼び出して User Service および Create Users 関数を使用するスクリプトを記述する必要があります。この XML API のパラメータの 1 つに、Unified MeetingPlace のプロファイル番号（mpProfileNumber）の割り当てがあります。Unified MeetingPlace のプロファイル番号は、4 ～ 8 桁の長さにする必要があります。Unified MeetingPlace のプロファイル番号は、音声だけの会議または音声だけの予約なし会議にのみ使用されます。この場合ホストは、会議 ID と PIN コードであるこのプロファイル番号で会議にログインして、会議を開始する必要があります。他のすべての発信者は、ホストがログインして会議を開始するまで、Unified MeetingPlace の待合室に入ります。通常のスケジュールされた WebEx と Unified MeetingPlace の複合会議では、このプロファイル番号と PIN コードを使用して会議を開始する必要はありません。

XML API の詳細については、次の Web サイトで入手可能な Cisco WebEx Collaboration Cloud のマニュアルを参照してください。

http://developer.webex.com/web/meetingservices/xmlapi

Unified MeetingPlace 所有プロファイルの管理

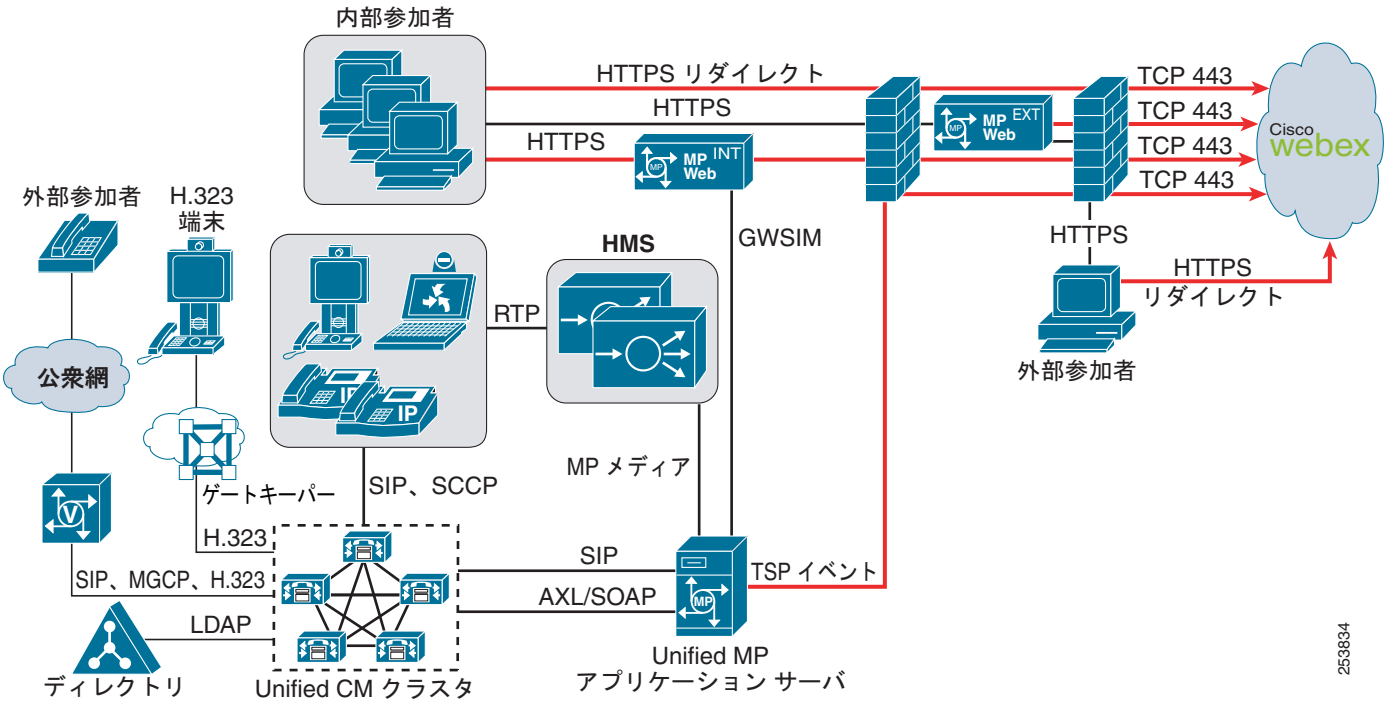
Unified MeetingPlace 所有プロファイルの管理は、既存のお客様が現在のプロファイルの使用を維持し、WebEx で使用したい場合にのみ使用できます。新規のお客様は、Unified MeetingPlace から WebEx への SSO 統合を使用して WebEx サイトをプロビジョニングすることはできません。これは、この方法でプロビジョニングされたインストール済みシステムでのみサポートされます。

Unified MeetingPlace と WebEx の間で SSO が有効ではない場合、すべての WebEx ホスト アカウントは（定期的に更新されるように）管理者によって Unified MeetingPlace から WebEx サイトへの手動エクスポートでプロビジョニングされる必要があり、すべてのエンド ユーザ認証はローカル WebEx ホスト アカウント パスワードによって提供される必要があります。WebEx ホスト アカウントは、プロファイル管理のために WebEx サイト経由で要求されて Unified MeetingPlace システムにエクスポートされる場合もあります。SSO オプションは、オンプレミスでの Unified MeetingPlace との統合のために WebEx サイトを注文する場合に選択する必要があります。これは Unified MeetingPlace と WebEx をすでにインストールしている既存のお客様だけに提供されます。

Unified MeetingPlace Scheduling の展開

Unified MeetingPlace Scheduling の展開オプションには、会議のスケジューリング専用と参加専用の 2 つの Unified MeetingPlace Web サーバを使用する必要があります。これらは Web 会議機能は提供しません。図 22-8 に、Unified MeetingPlace Scheduling および HMS を使用した Unified MeetingPlace ソリューションの例の概要を表示します。HMS の代わりに EMS を使用でき、MCS 向け WebEx ノードは示されていませんがオプションで追加することもできます。

図 22-8　Unified MeetingPlace Scheduling および HMS を使用した Unified MeetingPlace ソリューション



Unified MeetingPlace Scheduling では、招待にあるクリック参加 URL をユーザが選択すると、最初に Unified MeetingPlace Web サーバのカスタマー設定 URL（HTTPS オプションを推奨）に接続します。Unified MeetingPlace Web サーバはすぐに組織の WebEx サイトへの接続を開始し、会議を作成しま

す。WebEx サイトは参加 URL を返し、MeetingPlace Web サーバはそれをセキュア HTTPS による WebEx Media Tone Network へのリダイレクトという形式でクライアントに渡します。このリダイレクト動作はユーザにはまったく認識されません。また、ユーザ認証はオンプレミス Unified MeetingPlace システムでだけ実行されます。これは、SSO 機能を有効にするために必要です。スケジュールされた会議の音声およびビデオ オンプレミス リソースは予約されますが、Web リソースは会議が WebEx でオンデマンドで開始されたときに作成されます。内部ユーザは、オンプレミスの MCS 向け WebEx ノードを使用することもできます。

Unified MeetingPlace 登録ユーザが WebEx 会議をスケジュールする、または、Unified MeetingPlace Web ユーザ インターフェイスから My WebEx リンクにアクセスしようとすると、WebEx によって自動的に Unified MeetingPlace ユーザ プロファイルに基づくユーザ アカウントが SSO オプションを有効にして作成されます。Unified MeetingPlace プロファイルは、ローカル Unified MeetingPlace ユーザ ID とパスワードから、または Unified CM との LDAP 統合から（最も一般的に使用されます）作成されます。ユーザ名、パスワード、ファースト ネーム、ラスト ネーム、電話番号、電子メール アドレスなどの一部の Unified MeetingPlace ユーザ プロファイルが WebEx に継承されます。WebEx サイトは特定のお客様専用であり、WebEx ユーザ プロファイルは Unified MeetingPlace ユーザ プロファイルをベースにしていることから、ユーザ プロファイルが矛盾しないようにする必要があります。WebEx ホスト アカウントは手動では作成されません。この機能は、Unified MeetingPlace SSO 統合によって WebEx TSP リンク経由で提供されるためです。パスワードは TSP リンクで WebEx に送信されません。WebEx は、Unified MeetingPlace Web サーバによってリダイレクトされたすべての内部ユーザ トラフィックを信頼します。ゲスト ユーザは、WebEx 会議に参加するためにパスワードまたは認証を使用しません（WebEx 会議パスワードが設定されている場合を除きます）。

（注）　Unified MeetingPlace Scheduling を使用して内部会議をレコーディングできますが、そのためには MCS 向け WebEx ノードがオンプレミスで展開されている必要があります。

Cisco Unified Communications Manager

Cisco Unified Communications Manager（Unified CM）も、アーキテクチャの中心部分であり、SIP トランクによる着信およびコールバックを提供します。Unified CM で Unified MeetingPlace アプリケーション サーバの宛先アドレスを使用して SIP トランクを設定してから、ルート パターンを使用して SIP トランク経由のコールを Unified MeetingPlace にルーティングする必要があります。通常、ダイヤルイン機能を使用するために電子メール通知で送信される電話番号には、フリーダイヤル（オプション）、有料ダイヤル、および Unified CM 内部 DN（内部発信者向けの短縮ダイヤル用）の 3 つがあります。Unified MeetingPlace では、SIP トランクによるプライマリ Unified CM サブスクライバへのコールバックまたは発信ダイヤル機能をサポートするために、個別の設定があります。さまざまな条件により、プライマリがコールを受け付けない場合は、以降のサブスクライバが使用されます。複数の Unified CM コール処理サブスクライバの IP アドレスまたはホスト名が、ハント モードでの発信コール送信用にリストされています。

Unified CM サーバは、参加後の WebEx 会議室内のコールバック要求から受け取るすべてのダイヤル ストリングを解決できることが不可欠となります。サイト管理設定により、コールバックを WebEx サイトのシステム全体で無効にすることもできます。Unified CM は、さまざまな国に対するすべての料金制限や、ほとんどの企業がブロックするその他の番号も制御します。Unified MeetingPlace には、それ自体をブロックする料金制限がないためです。

マルチノード展開では、Unified CM または Session Management Edition システムが、地理的に分散した企業で Unified MeetingPlace をサポートする重要なコンポーネントです。固有の割り当て済みダイヤルイン番号を持つ Unified MeetingPlace 会議サーバに対応し、サイト間のコールと、ゲストまたは外部モバイル ユーザの公衆網へのコールすべてをダイヤル プランに基づいて解決するためには、Intercluster Trunk（ICT; クラスタ間トランク）を使用する Unified CM クラスタが必要となります。ゲスト ユーザは、参加後の会議室内でダイヤルインすることも、WebEx コールバック機能を使用することもできます。リージョン内のマルチノード Unified MeetingPlace 会議ノードは、ルート グループ内

で順繰りに設定されるので、すべての着信コールがすべてのノード間で均等に分散されます。コールバックは Meeting Director によって開始されます。Meeting Director は、その会議のホストの時間帯に基づいて、リージョンごとに最も使用率の低い会議ノードを選択します。その会議 ID をホストするために選択された会議ノードにダイヤルイン発信者を送信するために、SIP Refer コマンドが使用されます。

「ハイ アベイラビリティ」（P.22-9）の項に、冗長性に関する追加のガイドラインがあります。サードパーティ製の PBX を Unified MeetingPlace と統合できるのは、Unified CM を使用する場合だけです。PBX と Unified CM との相互運用性の詳細については、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns728/networking_solutions_products_genericcontent0900aecd805b561d.html

Unified MeetingPlace は、Early Offer（EO; アーリー オファー）と Delayed Offer（DO; ディレイド オファー）の両方の SIP Invite メッセージの受信をサポートします。Unified MeetingPlace は発信コールについて EO SIP Invite を開始し、Unified CM は DO SIP Invite を使用してコールを Unified MeetingPlace に送信します。Unified CM は EO を使用するように設定できますが、そのためには Media Termination Point（MTP; メディア ターミネーション ポイント）リソースを使用する必要がある場合があります。詳細については、「SIP ディレイド オファーおよびアーリー オファー」（P.14-20）を参照してください。

（注）　Express Media Server（EMS）を含む Unified MeetingPlace の音声 / ビデオ配置では、Unified MeetingPlace は Cisco IOS SIP ゲートウェイまたは Cisco Unified Border Element によるコール送信もサポートします。この配置では、LDAP 同期機能は失われます。詳細については、http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html で入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

録音

展開モデルを選択するもう 1 つの基準は、お客様が会議レコーディングを保存およびアクセスする場所です。会議参加者は、電話などの音声ユーザ インターフェイスを介して音声だけのレコーディングを開始することも、WebEx 会議室から音声と Web のレコーディングを開始することもできます。音声レコーディングは、WebEx Collaboration Cloud から Unified MeetingPlace メディア サーバへのコール イベントを、公衆網の音声ゲートウェイを介して呼び出します。Unified MeetingPlace Scheduling 展開モデルの場合、レコーディングされた会議は Unified MeetingPlace Web ユーザ インターフェイスからダウンロードし、WebEx レコーディング再生プログラムを使用して再生できます。内部 Unified MeetingPlace Web サーバ（およびオプションの SAN/NAS）には、内部会議としてスケジュールされたレコーディングが保存されます。すべての内部会議レコーディング（WebEx 音声レコーディング、音声だけ、または音声 / ビデオ レコーディング）は、オンプレミスで保存されます。ビデオ レコーディングは、Hardware Media Server オプションおよび Unified MeetingPlace Scheduling オプションの場合にだけ使用できます。

Unified MeetingPlace Scheduling は、外部会議としてスケジュールされるすべての会議に対して、WebEx Network Based Recording（NBR）ストレージを使用します。ただし、ユーザはこれらの外部レコーディングに内部レコーディングと同じ方法でアクセスします。ファイルが単に別のロケーションに保存されるだけです。

すべての Unified MeetingPlace および WebEx レコーディングは、ローカル ユーザの PC へのダウンロードによって提供される標準の NBR レコーディング再生プログラムで再生されます。すべてのファイルは、NBR レコーディング用の WebEx 編集ツールによって編集することもできます。

アーキテクチャのその他の考慮事項

Unified MeetingPlace Scheduling 展開モデルで使用できる一部の統合オプションでは、追加の統合サーバが必要な場合があります。Outlook および Exchange カレンダー統合は、本質的に Unified MeetingPlace アプリケーション サーバに組み込まれています。ただし、Lotus Notes 統合には、内部 Unified MeetingPlace Web サーバ上に共存する追加ソフトウェアが必要ですが、他の統合では内部 Unified Meeting Web サーバを展開する必要がありません。

Unified MeetingPlace は、IBM Sametime Web と統合して Web 会議機能をソリューションに提供することもできます。使用可能な Unified MeetingPlace 統合の詳細については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

展開オプション

大多数の Unified MeetingPlace 展開は、単一サイト モデルに従っています。ここでは、それぞれの展開オプションのハイレベルな詳細について説明します。

単一サイト Unified MeetingPlace Scheduling の展開

この展開モデルは、すでに Unified MeetingPlace Web コンポーネントを展開している現行のお客様のためのモデルです。このモデルを展開するその他の要件として、次の機能の使用が挙げられます。

- 音声だけ、または音声 / ビデオだけの展開（WebEx 統合を含まない）
  - この展開では、プライマリ / ウォーム スタンバイ冗長性が提供されます。
- ブラスト発信ダイヤルによる継続会議（音声だけの会議の場合）
  - この展開では、プライマリ / ウォーム スタンバイ冗長性が提供されます。
- Unified CM ビデオ テレフォニーのアドホック音声 / ビデオ ミキシング（カンファレンス ブリッジ リソース用）
  - Unified CM クラスタごとに、アドホック モードの Unified MeetingPlace の複数インスタンスを使用できます。各 Unified CM クラスタに、固有の Unified MeetingPlace 音声専用サーバが必要です。
  - クラスタごとのカンファレンス ブリッジ リソース グループ設定のハント方式で、複数の Unified MeetingPlace サーバを設定できます。
  - 標準ベースのビデオは、Unified MeetingPlace のビデオ設定のタイプと帯域幅によって、全体的なキャパシティに影響を及ぼします。

ほとんどの展開では単一サイト展開モデルが使用され、すべてのサーバ コンポーネントとユーザが単一のサイトに設置され、単一の LAN で相互接続されます。ソリューションのコンポーネントは、「アーキテクチャ」（P.22-5）の項で説明するようにさまざまです。単一サイト展開モデルには、次のような共通の特徴があります。

- Express Media Server は、自動的にアプリケーション サーバと同じ場所に設置されます。Unified MeetingPlace Hardware Media Server は、アクティブな Unified MeetingPlace アプリケーション サーバと同じデータ センターに設置する必要があります。
- Network Time Protocol（NTP; ネットワーク タイム プロトコル）を実装して、Unified MeetingPlace コンポーネントのクロックをネットワーク タイム サーバまたはネットワーク対応クロックに同期できるようにする必要があります。NTP によって会議の正確なスケジューリングが保証されることから、NTP は Unified MeetingPlace にとって重要なネットワーク サービスと言え

ます。Unified MeetingPlace アプリケーション サーバのインストール中に外部の NTP ソースを指定できます。他の Unified MeetingPlace コンポーネントは自動的にこのアプリケーション サーバに同期されます。

- 既存のお客様のインストール環境の場合のみ、オプションで、Unified MeetingPlace Scheduling の音声、ビデオ、および Web レコーディングと会議添付ファイルを、お客様が用意した外部の SAN/NAS ストレージ サーバ上に保存できます。
- Unified MeetingPlace Scheduling による展開の場合、内部ユーザ用の単一の Unified MeetingPlace Web サーバと、外部参加者用に DMZ 内に設置された単一の Unified MeetingPlace Web サーバを展開する必要があります。
- Unified MeetingPlace Scheduling による展開の場合、ソリューションでのアクティブな Unified MeetingPlace アプリケーション サーバと Unified MeetingPlace Web サーバ間の往復遅延は、150 ms 以下にする必要があります。
- MCS 向け WebEx ノードの展開については、会議の参加者に最も近い内部ネットワーク上に設置することを推奨します。MCS 向け WebEx ノードは HTTPS プロキシ サーバをサポートしないため、WebEx サイトにアクセスするには TCP ポート 443 を使用して直接外部へルーティングする必要があります。

コンポーネント別の着信および発信ポートの詳細リストについては、次の Web サイトで入手可能な『*System Requirements for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html

ハイ アベイラビリティ

この項では、次の Unified MeetingPlace コンポーネントの冗長性に関する考慮事項について説明します。

- Unified MeetingPlace アプリケーション サーバ
- Unified MeetingPlace メディア サーバ
- Unified MeetingPlace Web サーバ
- MCS 向け WebEx ノード
- 呼制御

Unified MeetingPlace アプリケーション サーバ

WebEx Scheduling によるマルチノード展開の Unified MeetingPlace では、アクティブ/アクティブの復元性が自動的に提供され、お客様はリージョンおよびサイトごとに冗長性のレベルを選択できます。リージョンは、必要に応じて別のリージョンにオーバーフローするように設定できます。

MeetingPlace Scheduling モデルを使用する Unified MeetingPlace では、フェールオーバー用に 1 つのアクティブ（プライマリ）Unified MeetingPlace アプリケーション サーバと 1 つのウォーム スタンバイ Unified MeetingPlace アプリケーション サーバを使用できます。フェールオーバー配置内の各 Unified MeetingPlace アプリケーション サーバには、その物理 Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）に関連付けられた共通の IP アドレスと仮想ネットワーク インターフェイスに関連付けられた一意の IP アドレスが設定されます。両方の Unified MeetingPlace アプリケーション サーバで同じ IP アドレスを共有するための要件は、両方のアプリケーション サーバを同じ Virtual LAN（VLAN; 仮想 LAN）または IP サブネットに接続することです。このことは、両方のサーバが単一のデータ センター内に存在する場合は問題になりません。ただし、デュアル データ センター設計は、両方のデータ センターが同じ VLAN（IP サブネット）上に存在する場合にのみサポートされます。すべての Unified MeetingPlace コンポーネントと同様に Unified CM

もこの共有 IP アドレスを使用してデータをやり取りします。スタンバイ サーバの物理 NIC（共有 IP アドレスを含む）は、プライマリ サーバに障害が発生して手動フェールオーバー プロセスが IT 担当者によって開始されるまで、無効にされます。

マルチノードまたはスタンバイ サーバを配置する場合のネットワーク要件については、次の Web サイトで入手可能な最新バージョンの『*Planning Guide for Cisco Unified MeetingPlace*』で、フェールオーバーの情報を参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

プライマリ サーバとスタンバイ サーバ間の Informix データベース レプリケーションに仮想ネットワーク インターフェイスが使用されます。データベース レプリケーションでは、ユーザ、グループ、および会議に関係するデータベース テーブルがプライマリ サーバとスタンバイ サーバ間で同期されることが保証されます。アクティブ サーバとスタンバイ サーバの仮想ネットワーク インターフェイスを同じ VLAN に配置することを推奨します。Unified MeetingPlace アプリケーション サーバの冗長性の詳細については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

Unified MeetingPlace ソリューションに関するその他の重要な要件は、アクティブな Unified MeetingPlace アプリケーション サーバとアクティブな Unified MeetingPlace メディア サーバを同じ場所に設置する必要があることです。Express Media Server は Unified MeetingPlace アプリケーション サーバ自体にあるソフトウェア内で実行されるため、スタンバイの Unified MeetingPlace アプリケーション サーバへのフェールオーバーによって、スタンバイ サーバの EMS 機能が使用されます。Hardware Media Server の場合は、デュアル データ センター設計と比較して、シングル データ センター設計を検討するときはいくつかの考慮事項があります。

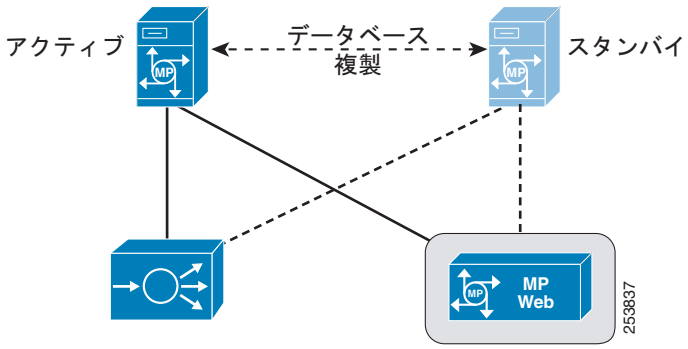
シングル データ センター設計

シングル データ センター設計では、アクティブ/アクティブ モードでマルチノードの復元性が自動的に使用可能になり、Meeting Director コンポーネントにより両方のノード間で会議が均等に分散されます。1 つの会議ノードで障害が発生した場合、コールはドロップされ、ユーザが同じ会議 ID にダイヤルインして戻ったとき、または会議室 GUI の WebEx コールバック機能を使用したときに、それらの会議はリージョン内の別のノードで自動的に確立されるか、設定されている場合は別のリージョンにオーバーフローします。サイトごとに最大 4 つの会議ノードを配置できます。

Unified MeetingPlace Scheduling モデルでは、地理的に同じ場所で Unified MeetingPlace アプリケーション サーバのフェールオーバーが発生します。この種の展開では、一般に、一連の Unified MeetingPlace Hardware Media Server がプライマリとスタンバイの Unified MeetingPlace アプリケーション サーバで共有されます。プライマリ Unified MeetingPlace アプリケーション サーバに障害が発生した場合は、Unified MeetingPlace メディア サーバをスタンバイ（現在のプライマリ）サーバに同期させる必要があります。Unified MeetingPlace Web サーバも Unified MeetingPlace Scheduling 展開に対して共有されます。図 22-9 に、シングル データ センター展開における Unified MP アプリケーション サーバのフェールオーバー プロセスを示します。

（注）　高度に冗長なソリューションでは、シングル データ センター内にスタンバイの Unified MeetingPlace メディア サーバと Web コラボレーション サーバのセットを配置することもできます。Unified MeetingPlace 8.*x* システムで Unified MeetingPlace Web サーバを冗長にすることはできません。WebEx Scheduling 展開モデルは、より信頼性の高い冗長展開モデルです。

図 22-9　シングル データ センター展開における Unified MeetingPlace アプリケーション サーバのフェールオーバー



デュアル データ センター設計

デュアル データ センター設計では、マルチノードの会議ノードを使用する WebEx Scheduling モデルにより、リージョンごとにアクティブ/アクティブ フェールオーバーが提供されます。または、他のリージョンへのオーバーフローも設定できます。お客様の要件に応じて、複数データ センターでのアクティブ/アクティブ ロード シェアリング用に最大 14 の会議ノードを配置した環境で、4 つのリージョンと、リージョンごとに 2 つのサイトがサポートされます。会議ノードに障害が発生した場合、音声コールはドロップされ、ユーザがダイヤルして戻ったとき、または会議室から WebEx コールバック GUI 機能を使用したときに、会議はキャパシティのあるアクティブ ノードで自動的に開始されます。コールを分配するのにリージョン内のすべての会議ノードを使用でき、別のリージョンへのオーバーフローはオプションのシステム管理設定に基づいて行われます。

Unified MeetingPlace Scheduling モデルでは、Unified MeetingPlace アプリケーション サーバのフェールオーバーが IP WAN 上の地理的に異なる場所で発生します。また、アクティブとスタンバイのアプリケーション サーバが地理的に離れていますが、両方のサーバを同じ VLAN に接続して適切なフェールオーバー動作を保証する必要があります。この種の展開では、スタンバイ アプリケーション サーバを冗長な Unified MeetingPlace Hardware Media Server と同じ場所に設置して、それらと同期させる必要があります。スタンバイ データ センター内で Unified MeetingPlace メディア サーバの音声ブレードとビデオ ブレードの数が異なる場合は、スタンバイ アプリケーション サーバがアクティブ サーバに昇格されるフェールオーバー シナリオでシステム キャパシティが減少する可能性があります。

Unified MeetingPlace メディア サーバ

Express Media Server は Unified MeetingPlace アプリケーション サーバ自体にあるソフトウェア内で実行されるため、マルチノード展開モデルでは、追加の会議を開くのにリージョン内の任意の会議ノードを使用できます。サイトごとに最大で 4 つのサーバ、リージョンごとに 2 つのサイト、および 4 つのリージョンを展開して、グローバルな分散型アーキテクチャを実現できます。

Express Media Server は Unified MeetingPlace アプリケーション サーバ自体にあるソフトウェア内で実行されるため、スタンバイのアプリケーション サーバへのフェールオーバーによって、スタンバイ サーバの EMS 機能が使用されます。EMS では、他の EMS インスタンスへのカスケーディングまたはクラスタリングはサポートされません。最大で 1 つのプライマリおよび 1 つのフェールオーバー Unified MeetingPlace アプリケーションおよび EMS サーバが、Unified MeetingPlace Scheduling または WebEx Scheduling 展開モデルを使用した Unified MeetingPlace ソリューションでサポートされます。アクティブな RSNA フェールオーバーは WebEx 統合ではサポートされません（スタンドアロンの音声/ビデオ配置だけ）。

Unified MeetingPlace アプリケーション サーバは、システム内の代替 HMS（音声ブレードまたはビデオ ブレード）へのフェールオーバーを自動的に実行します。たとえば、音声ブレードとの接続断を検出した場合、アプリケーション サーバは、以降の音声セッションがアクティブな音声ブレードに接続されるように、そのブレードをアクティブな音声ブレードのリストから削除します。音声またはビデオ ブレードの障害時に Unified MeetingPlace メディア サーバのキャパシティが減少しないようにするための 1 つの方法は、ソリューションに HMS 音声およびビデオ ブレードを追加することです。アプリケーション サーバはライセンスされたセッション数を超えることはありません。もう 1 つの方法は、専用の HMS を備えたスタンバイの Unified MeetingPlace アプリケーション サーバに戻すことです（デュアル データ センター設計と同様）。この 2 つの方法は二者択一ではありません。専用の HMS を備えたスタンバイの Unified MeetingPlace アプリケーション サーバは、音声またはビデオ ブレードを追加することで、さらに冗長性を高めることができます。

Hardware Media Server のフェールオーバーの詳細については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

Unified MeetingPlace Web サーバ

Unified MeetingPlace Scheduling モデルでは、レコーディングや Web スケジューリング インターフェイス用に音声だけを設定した Web サーバを 1 つだけ使用します。既存のお客様が WebEx 統合を使用して Unified MeetingPlace 8.5（以降のリリース）に移行し、引き続き Unified MeetingPlace Scheduling モデルを使用する場合は、DMZ 内に配置されたその他の Web サーバを使用してください。各 Cisco Unified MeetingPlace システムは、WebEx 統合だけを使用する場合、最大で 1 つの内部 Web サーバと 1 つの DMZ 内 Web サーバを保持できます。これらのサーバに冗長性オプションはありません。Unified MeetingPlace Web サーバは、Unified MeetingPlace Scheduling インターフェイスが組み込まれたソリューションに対してだけ実装されます。Unified MeetingPlace の Lotus Notes または Jabber 統合も冗長にすることはできません。

MCS または ASR 向け WebEx ノード

Unified MeetingPlace ソリューションでは、最大 4 つの MCS 向け WebEx ノードがサポートされます。ASR 向け WebEx ノードを使用する場合、ノード数の制限はありません。会議のカスケードは、MCS 向け WebEx ノードおよび WebEx Collaboration Cloud にわたってサポートされます。MCS または ASR 向け WebEx ノードは、1 つのノードで障害が発生した場合に、冗長性レベルをそれぞれ自動的に提供します。会議ゾーン URL のリストを受信したあと、クライアントはすべての会議ゾーン URL に ping し、最も近いノードを判別します。あるノードが応答しない場合、このノードに接続するクライアントはありません。すべての内部ユーザ（リモート ロケーションから VPN を使用するユーザも含む）は、MCS サーバ向け WebEx ノードのいずれかに接続できます。

会議をホストしている MCS または ASR 向け WebEx ノードが使用できなくなった場合、次に使用可能な MCS または ASR 向け WebEx ノードが自動的に引き継ぎます。共有およびレコーディングは停止され、ユーザは会議の共有およびレコーディングを再開する必要があります。お客様の複数の MCS または ASR 向け WebEx ノードが会議内でアクティブであり、各ノードにユーザのサブセットがある場合、コンテンツは MCS または ASR 向け WebEx ノード間でカスケードされます。同じ会議内で 3 つ以上の MCS 向け WebEx ノードがアクティブである場合、カスケードは、ホストが存在する MCS 向け WebEx ノードを中心とした星として表されます。ノードに障害が発生した場合、クライアントはクライアント エントリ会議ウィンドウで WebEx から提示されたリストを使用して他のノードに自動的に再度参加します。エンド ユーザへの影響はほとんど、またはまったくありません。外部のスケジュールされた会議では、内部ユーザも WebEx クラウドに接続できます。内部のスケジュールされた会議は、他の冗長 WebEx ノード上で常に内部のままとなります（ノードは、お客様のネットワーク設計要件に応じて、分散させることも同じ場所に設置することもできます）。音声コールは、オンプレミスの Unified MeetingPlace システム上でそのまま保持されます。

WebEx クラウド内の冗長性の詳細については、「ハイ アベイラビリティ」（P.22-9）を参照してください。

呼制御

Unified MeetingPlace では、Cisco Unified CM コール処理用のサブスクライバをポイントする、複数の SIP 発信ダイヤル接続を定義できます。冗長性を確保するには、Unified CM クラスタ内のコール処理サブスクライバにコールを転送するように複数の SIP プロキシ サーバを設定する必要があります。これらのコール処理サブスクライバは、Unified CM 内の Unified MeetingPlace コールについて設定された SIP トランクの Unified CM Group と関連している必要があります。Unified MeetingPlace アプリケーション サーバからは、SIP プロキシ サーバ 1 との接続が失われないかぎり、発信コールが SIP プロキシ サーバ 1 だけに送信され、SIP プロキシ サーバ 2 には送信されないことに注意してください。接続が失われた場合にだけ、Unified MeetingPlace から、リストで次に使用可能なコール処理エージェントに SIP INVITE メッセージが送信されます。コール処理エージェントの失敗が既存のコールに影響を与えないようにする必要があります。ユーザが切断すると、既存のメディア接続が失われます。

（注）　SIP プロキシ サーバという用語は、単に Unified MeetingPlace アプリケーション サーバの設定ページに見られる用語であり、すべての SIP プロキシ サーバとの統合がサポートされることを意味するものではありません。

着信コールの場合は、設定済み Unified CM Group 内で見つかった最大 3 つのコール処理サブスクライバによって、Unified CM 内の単一の設定済み SIP トランクを処理できます。Unified CM Group 内のプライマリ Unified CM コール処理サブスクライバがオフラインの場合、2 番めのコール処理サブスクライバが Unified MeetingPlace システムに対するコールの開始を引き継ぎます。詳細については、「Cisco Unified CM トランク」（P.14-1）を参照してください。EMS を使用した Unified MeetingPlace Scheduling 展開の場合、コール送信に冗長性を持たせるには複数の Cisco IOS SIP ゲートウェイが必要です。

キャパシティ プランニング

特定の Unified MeetingPlace ソリューションのキャパシティは、Unified MeetingPlace Meeting Director、EMS または HMS を使用するアプリケーション サーバ、または MCS または ASR サーバ向け WebEx ノードがインストールされるプラットフォーム、および展開される Unified MeetingPlace メディア サーバのキャパシティによって異なります。たとえば、Cisco MCS 7845-I3（または同等の Hewlett-Packard）サーバにインストールされた Unified MeetingPlace アプリケーション サーバでは、音声会議は単一のシステムまたは会議ノードで EMS の場合 1,200 ポート（G.711）、HMS の場合 2,000 ポート（G.711）になります。

Unified MeetingPlace アプリケーション サーバと共存インストールされるため、EMS のキャパシティはコーデックとビデオ帯域幅に直接関係します。Unified MeetingPlace アプリケーション サーバが Cisco MCS 7835-H2/I2 サーバ上にインストールされる場合、全体的なシステム キャパシティは EMS 展開と HMS 展開の両方で減少します。ビデオと G.729 および G.722 音声コーデックはすべて、EMS システムのキャパシティに影響します。キャパシティの詳細な数字については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

Express Media Server

EMS では、System Resource Unit（SRU; システム リソース ユニット）という概念が導入されます。この概念では、システム キャパシティ（つまり、合計 SRU 値）は、Unified MeetingPlace アプリケーション サーバが存在するハードウェア プラットフォームのタイプと、そのシステムのプロセッサの速度および数に基づきます。システムは、通常の動作でこれらの SRU の一部を合計から直接消費し、残りのリソースを SRU プールに置いて、拡張音声 / ビデオ機能で使用できるようにします。表 22-8 に、拡張音声 / ビデオで使用できる合計 SRU 数を、サポートされるプラットフォームごとに示します。

表 22-8　サポートされるプラットフォームごとの合計 SRU

プラットフォーム	拡張音声 / ビデオの合計 SRU
Cisco MCS 7835-H2/I2	500
Cisco MCS 7845-H2/I2	1,000
Cisco MCS 7845-I3	1,200
Cisco UCS B シリーズまたは C210 シリーズ	1,200（Meeting Director が共存する場合またはしない場合）
Cisco UCS C200 シリーズ	最大 250（冗長性のある 2 ノード）

表 22-9 に、さまざまな音声コーデックおよびビデオ帯域幅で消費される SRU 数を示します。

表 22-9　音声 / ビデオ セッションごとに使用されるシステム リソース ユニット

セッション タイプ	使用される SRU 数
G.711 音声ポート 1 個	1
G.729 または G.722 音声ポート 1 個	5
ビデオ ポート 1 個（320 kbps）[1]	1
ビデオ ポート 1 個（384 kbps）	1
ビデオ ポート 1 個（768 kbps）	2
ビデオ ポート 1 個（1,200 kbps）	4
ビデオ ポート 1 個（1,500 kbps）	5
ビデオ ポート 1 個（2,000 kbps）	6

1. ビデオ ライセンスに対して保証される最低レートは 320 kbps です。

表 22-8 および表 22-9 で示したように、G.711 音声コールだけを処理する MCS 7845-I3 サーバでは、EMS は 1,200 音声セッションをサポートします。または、最大 384 kbps で 650 ビデオ セッションを G.711 音声とともにサポートします（ビデオ セッションは音声セッション用にも SRU を消費します）。

Unified CM では、Unified MeetingPlace へのコール送信に使用される SIP トランクのリージョン設定を、EMS に送信されるコールの音声コーデックおよびビデオ帯域幅を制御するために設定できます。Unified MeetingPlace にダイヤルインするエンドポイントの性質と機能を理解することが、正しい設計のために重要です。EMS キャパシティ プランニングの詳細については、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

Hardware Media Server

HMS では、EMS とは異なる設定をいくつか使用します。Unified MeetingPlace Application Administration のグローバル音声モード設定は、Unified MeetingPlace HMS 音声ブレードの音声容量に直接影響します。グローバル音声モードは次のいずれかの方法で設定できます。

- LEC を使用しない G.711 および G.729

  この設定では、HMS 内の 1 つの音声ブレードで最大 250 個の音声ポートがサポートされます。サポートされるシステムの最大限度である 2,000 の同時音声セッションに達するには、8 つの音声ブレードが必要となります。

- LEC を使用する G.711、G.722、iLBC、または G.729

  この設定では、1 つの音声ブレードで最大 166 個の音声ポートがサポートされます。8 つの音声ブレードの場合、これらの追加コーデックを使用してサポートされる同時音声セッションの最大数は 1,328 です。

Unified MeetingPlace Application Administration のグローバル ビデオ モード設定は、Unified MeetingPlace HMS ビデオ ブレードのビデオ容量を決定します。グローバル ビデオ モードは次のいずれかの方法で設定できます。

- 標準レート（最大 384 kbps のビデオ コール スピード）

  このモードでは、HMS 内のビデオ ブレードは最大 40 個のビデオ ポートをサポートできます。

- 高レート（最大 2,048 kbps のビデオ コール スピード）

  このモードでは、ビデオ ブレードは最大 20 個のビデオ ポートをサポートできます。

Unified MeetingPlace でサポートされるビデオ形式の全リストについては、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html

Unified MeetingPlace Hardware Media Server は、Cisco Unified MeetingPlace 3515 または Cisco Unified MeetingPlace 3545 シャーシにすることができます。Unified MeetingPlace 3515 は、1 つの音声ブレードと 1 つのビデオ ブレードがプレインストールされた固定プラットフォームです。Unified MeetingPlace 3545 は、4 つの音声ブレードまたはビデオ ブレードのさまざまな組み合せをサポートするシャーシで構成されたモジュール式プラットフォームです。

仮想カスケーディング

Unified MeetingPlace 3545 に複数の音声ブレードとビデオ ブレードがインストールされている場合は、メディア サーバで仮想カスケーディングを使用して、ある音声ブレードまたはビデオ ブレードから別の音声ブレードまたはビデオ ブレードへ、オーディオ ストリームとビデオ ストリームがオーバーフローされます。音声ブレードには、音声セッション容量を減少させないカスケーディング ポートが組み込まれています。単一のビデオ ブレードを Unified MeetingPlace システムに展開することによって、すべてのビデオ ポートがビデオ会議に使用できます。複数のビデオ ブレードを展開した場合は、メディア サーバによって自動的にカスケーディング用のビデオ ポートが予約されます。標準レート ビデオの場合は、カスケーディング用に 8 個のビデオ ポートが予約され、40 個のビデオ ポートが他の目的に使用できます。高レート ビデオの場合は、カスケーディング用に 4 個のビデオ ポートが予約され、20 個のビデオ ポートが他の目的に使用できます。次の 2 つの例は、カスケーディング時の音声ポートとビデオ ポートの使用方法を示しています。

例 22-1　Unified MeetingPlace 音声会議

Unified MeetingPlace 3545 メディア サーバが、2 つの音声ブレードおよび 2 つのビデオ ブレードと一緒に配置されます。会議が 350 個の音声ポートを使用してスケジュールされ、グローバル音声モードが LEC を使用する G.711 用に設定されます。この場合、次のように計算します。

- メディア サーバで、最初の音声ブレードから 251 個のポートが割り当てられます。そのうちの 250 個のポートが音声参加者用に使用され、1 個のポートがビデオ カスケーディングまたは 2 番めの音声ブレードとの接続に使用されます。
- メディア サーバで、2 番めの音声ブレードから 101 個のポートが割り当てられます。そのうちの 100 個のポートが音声参加者用に使用され、1 個のポートがビデオ カスケーディングに使用されます。

例 22-2　Unified MeetingPlace ビデオ会議

Unified MeetingPlace 3545 メディア サーバが、2 つの音声ブレードおよび 2 つのビデオ ブレードと一緒に配置されます。この例では、会議が 65 個のビデオ ポートでスケジュールされ、グローバル ビデオ モードが標準レート ビデオ用に設定されます。この場合、次のように計算します。

- メディア サーバで、最初のビデオ ブレードから 41 個のポートが割り当てられます。そのうちの 40 個のポートがビデオ参加者用に使用され、1 個のポートがビデオ カスケーディングまたは 2 番めのビデオ ブレードとの接続に使用されます。
- メディア サーバで、2 番めのビデオ ブレードから 26 個のポートが割り当てられます。そのうちの 25 個のポートがビデオ参加者用に使用され、1 個のポートがビデオ カスケーディングに使用されます。

Unified MeetingPlace 音声会議のサイジングに関するガイドライン

Unified MeetingPlace 音声会議容量を計算するために次の方法を推奨します。

- 平均月間使用時間に基づく計算

  音声会議の平均使用時間（1 か月あたりの平均時間（分））がわかっている場合は、表 22-10 を使用して Unified MeetingPlace 音声会議容量を計算します。

表 22-10　平均月間使用時間に基づく Unified MeetingPlace 音声会議容量

平均月間使用時間（分）	ベースライン使用時間（1 か月およびユーザ ライセンスあたりの時間（分））	予想ポート数
20,000 ～ 50,000	1,500	15 ～ 35
50,000 ～ 500,000	2,000	25 ～ 250
500,000 ～ 1,000,000	3,000	165 ～ 335
1,000,000 ～ 2,000,000	3,500	285 ～ 570
2,000,000 ～ 8,000,000	4,000	500 ～ 2,000

- ユーザ数に基づく計算

  平均的使用率の 20 ユーザごとに 1 ポートを割り当てるように検討します。使用頻度の高い会議ユーザの場合は、15 ユーザごとに 1 ポートを用意します。たとえば、6000 ユーザのシステムでは、300 音声ポートを用意する必要があります。ただし、ユーザの会議使用頻度が高い場合は、400 音声ポートを検討します。

- ピーク時の使用時間に基づく計算

  一般的に、音声会議のピーク時の使用時間は、既存の音声会議システムのログまたはサービス プロバイダーの請求書から得られます。余裕をもった会議容量を確保するために、実際のピーク時使用時間よりも 30% 多い容量を用意することを推奨します。

（注）　ユーザ ライセンス（音声、Web、またはビデオ）は、個別のユーザに付与されるのではなく、Unified MeetingPlace システムを使用しているすべてのユーザで共有されるシステム全体のリソースに付与されます。

システム サイジングに影響する要素

次の要素は、システム ベースライン ポート要件に関する前述の方式で算出される見積もりに加えて、システム サイジングにも影響します。

- 「オペレータ スケジュール」モデルから Cisco Unified MeetingPlace 上のユーザ スケジュール モデルまたは予約不要モデルに移行する場合は、ベースラインに 20% 上積みしなければならない可能性があります。
- 平均規模の会議のデフォルトは、1 会議あたり 4.5 人の発信者です。デフォルトと異なる場合は、自分のケースに応じた値を使用してください。
- 次の条件が当てはまる場合は、それに応じてベースライン見積もりを増やします。

  （1 日あたりの予想会議数）X（予想ユーザ数）＞ベースラインの 80%
- 最大規模の会議が予想容量の 20% を超えている場合は、それに応じて見積もりを増やします。
- 専用ポートを使用して会議を連続して行う場合は、追加のポート（（会議数）X（専任発信者数））をベースラインに加算する必要があります。

総ポート数には、上記要素のすべてとベースラインが含まれます。

Unified MeetingPlace の容量拡張を考慮する場合は、次の条件がシステムに当てはまるかどうかを検討します。

- 総予想ポート容量が、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンに記載された最大サポート ポート数の 80% を超えている。

  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html
- G.711 以外の音声コーデックが望ましい。ただし、会議で他のコーデック タイプの最大容量を達成する必要がある場合は、Cisco Integrated Services Router（ISR; サービス統合型ルータ）をベースにしたトランスコーダを使用できます。
- Line Echo Cancellation（LEC; 回線エコー キャンセレーション）は、エコー キャンセレーション機能を備えた Unified MeetingPlace ではなく、ISR などの外部デバイスが提供する。

Unified MeetingPlace ビデオ会議のサイジングに関するガイドライン

Unified MeetingPlace ビデオ会議容量を計算するために次の 3 つの方法を推奨します。

- ナレッジ ワーカの数に基づく計算

  40 人のナレッジ ワーカごとに 1 つのビデオ UL を用意することを推奨します。
- 音声会議 UL 数に基づく計算

  既存の音声 UL 数の 17 ～ 25% の範囲のビデオ会議容量を用意することを推奨します。この割合は、ビデオ会議に関するビジネス要件と Unified MeetingPlace システムの規模によって異なります。

- 既存のビデオ MCU に基づく計算

  既存のビデオ会議システムをそのまま置き換えることを推奨します。既存のシステムのビデオ会議ライセンスは、Unified MeetingPlace UL で置き換えることができます。

Unified MeetingPlace Web サーバ

Unified MeetingPlace Web サーバは、会議のスケジューリングと参加のための Unified MeetingPlace Scheduling 展開と Lotus Notes 統合だけに必要です。これらのサーバにキャパシティ プランニングに関する考慮事項はありません。大規模な Unified MeetingPlace 展開にも Cisco MCS 7835 サーバで十分ですが、MCS 7845 サーバを使用することもできます。

MCS 向け WebEx ノード

MCS 向け Cisco WebEx ノードをオプションで使用する Web 会議は、MCS 向け WebEx ノードが存在するハードウェアのタイプに応じて、最大 500 の Web セッションに対応できます。ソリューションごとに最大 4 つの MCS 向け WebEx ノードを展開でき、ASR 向け WebEx ノードを使用する場合は展開できるノード数が無制限になるので、冗長性を備えたオンプレミスでの最大 2,000 の Web セッションのスケーラビリティが可能です。WebEx ノードはお客様のネットワーク内の任意の場所に分散できますが、大きい Web ユーザ グループの近くに展開することを推奨します。MCS または ASR 向け WebEx ノードでの Web セッションを使用できるのは内部ユーザだけです。外部ユーザは常にクラウドに接続します。MCS または ASR 向け Cisco WebEx ノードの詳細なキャパシティについては、次の Web サイトで入手可能な『*Planning Guide for Cisco Unified MeetingPlace*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html

ネットワーク トラフィック プランニング

Unified MeetingPlace コラボレーションのネットワーク トラフィック プランニングは、次の要素で構成されます。

- 呼制御帯域幅

  呼制御帯域幅は非常に狭いですが、重要です。Unified MeetingPlace アプリケーション サーバと Unified CM を同じ場所に設置することによって、呼制御に伴う問題の回避が容易になります。離れた場所に設置する場合は、信頼できる動作を保証するための適切な QoS プロビジョニングが必要になります。

- リアルタイム トランスポート プロトコル（RTP）トラフィック帯域幅

  RTP トラフィックは、音声とビデオのトラフィックで構成されます。Unified MeetingPlace メディア サーバは、音声コーデックとして G.711、G.729、G.722、および iLBC をサポートし、幅広いビデオ コーデックおよび帯域幅をサポートします。コーデックの種類別の推定帯域幅については、「ネットワーク インフラストラクチャ」（P.3-1）と「IP ビデオ テレフォニー」（P.12-1）の章を参照してください。

- Web コラボレーション帯域幅

  Unified MeetingPlace ソリューションの Web コラボレーション帯域幅は、WebEx SaaS ソリューションの場合と同じ方法で見積もることができます。「ネットワーク トラフィック プランニング」（P.22-10）を参照してください。

設計上の考慮事項

Unified MeetingPlace の展開には、次の設計上の考慮事項が適用されます。

- WebEx サイトごとに、サポートされる Unified MeetingPlace システムは 1 つだけです。
- Unified MeetingPlace ソリューションのコンポーネントがネットワーク ファイアウォールで分離されるシナリオでは、必要なすべてのトラフィックに対して適切なピンホールが開かれていることが不可欠です。詳細なポート リストについては、次の Web サイトで入手可能な最新バージョンの『*System Requirements for Cisco Unified MeetingPlace*』で、ネットワーク要件の情報を参照してください。

  http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html
- 通常、コラボレーティブ会議システムによって、正時のコール処理の負荷が大きくなります。Unified MeetingPlace 用の特定のパラメータを設定したキャパシティ プランニング ツールは、シスコ代理店と従業員が使用できる機能であり、大規模構成の Cisco Unified Communications システムのキャパシティの計算に役立ちます。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を http://tools.cisco.com/cucst で入手できます。
- シスコのさまざまなコラボレーティブ クライアント製品の詳細と、それらがコラボレーティブ会議ソリューションにどのように適しているかについては、「Cisco Collaboration クライアントおよびアプリケーション」（P.24-1）を参照してください。
- Unified MeetingPlace を使用したコール アドミッション制御は、Unified CM によって実行されます。ロケーションベースのコール アドミッション制御では、Unified CM は、Unified MeetingPlace 固有の SIP トランクを一定量の音声 / ビデオ帯域幅が許可されたロケーションに置くことによって、Unified MeetingPlace システムへの帯域幅を制御できます。また、Unified CM は、コール アドミッション制御も提供可能な Resource Reservation Protocol（RSVP; リソース予約プロトコル）の使用をサポートします。コール アドミッション制御戦略の詳細については、「コール アドミッション制御」（P.11-1）の章を参照してください。
- Unified MeetingPlace は、RFC 2833 および KPML DTMF という標準的な Dual-Tone Multi-Frequency（DTMF; デュアルトーン マルチ周波数）送信方式をサポートします。Unified CM は RFC 2833 をサポートし、これは DTMF リレーの推奨方式です。
- Unified MeetingPlace アプリケーション サーバからの SIP シグナリング トラフィックは、CS3（DSCP 0x18）とマークされます。ただし、Unified MeetingPlace アプリケーション サーバからのその他のトラフィック（Unified MeetingPlace Web サーバ、メディア サーバ、または WebEx サイトとの通信など）は、ベストエフォート（DSCP 0x00）とマークされます。このトラフィックのいずれかが低速で通過しているか輻輳したリンクである場合、QoS に関する考慮事項に注意する必要があります。
- デフォルトで、Unified MeetingPlace メディア サーバからのオーディオ ストリームは EF（DSCP 0x2E）とマークされ、ビデオ ストリームは AF41（DSCP 0x22）とマークされます。これらの値は Unified MeetingPlace 管理から設定可能です。
- Web 会議トラフィックは SSL で暗号化され、常にベストエフォート（DSCP 0x00）とマークされます。
- Unified MeetingPlace Meeting Director TSP コンポーネントは、WebEx サイトへのデュアル発信 TCP ポート 443 接続を開始し、SOCKS プロキシ サーバ サポートも提供します。
- Unified MeetingPlace の MCS または ASR 向け WebEx ノードは、WebEx サイトへの発信 TCP ポート 443 接続を開始しますが、HTTPS プロキシ サーバをサポートしません。MCS または ASR 向け WebEx ノードは、WebEx サイトへのプロキシを使用しない直接接続を許可されている必要があります。

Cisco Unified Videoconferencing

ビデオが広く配置されるにつれて、会議用ビデオを使用した会議が一般的になっています。Cisco Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）は、ビデオ会議に使用されます。Cisco Unified CM は、ビデオ会議に MCU を使用するために、Cisco Unified CM に登録された IP Phone とエンドポイントを有効にできます。ただし、会議とは、ユーザが音声およびビデオ会議を使用するだけでなく、コラボレーションを有効にするためにデスクトップ画面またはデスクトップ上のアプリケーションを共有できるということも意味する場合があります。

さまざまなソリューションでこの機能が提供されます。Cisco Unified Videoconferencing ソリューションには、次の重要な機能があります。

- 音声会議
- ビデオ会議用の高解像度
- H.239 プロトコルを使用したユーザのデスクトップおよびアプリケーションの共有
- Web ベースの軽量クライアントを使用したユーザのデスクトップおよびアプリケーションの共有
- モデレータとしての会議制御
- ファイアウォールおよび NAT を越えた非信頼ネットワークからの外部参加者

Cisco Unified Videoconferencing コラボレーション ソリューションは、次の要素で構成されます。

- Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）

  MCU は、IP Phone またはエンドポイントからオーディオ ストリームとビデオ ストリームを受信し、それらを混合して会議を形成する会議デバイスです。MCU はその DSP を使用してこの機能を実行します。MCU は、Skinny Client Control Protocol（SCCP）、H.323、SIP などのさまざまなコール シグナリング プロトコルをサポートします。IP Phone とエンドポイントは、さまざまなシグナリング プロトコルを使用して、Unified CM などの呼制御サーバのサポートを受けて MCU でコールを終端します。

- Cisco Unified Videoconferencing Manager

  Cisco Unified Videoconferencing Manager は、社内のさまざまなビデオ リソースおよび MCU の管理に役立つサーバです。H.323 ゲートキーパー機能を提供します。Cisco Unified Videoconferencing Manager は、次の 2 つの部分で構成されます。

  - Resource Manager

    Resource Manager は、Cisco MCU、Cisco ゲートキーパー、H.320 ゲートウェイ、端末、Cisco Unified Videoconferencing Desktop Server 接続などのリソースを管理します。また、MCU 上の会議のデフォルトも管理します。Cisco Unified Videoconferencing Manager は、仮想 MCU 機能を提供します。この機能は、外部では単一の MCU として表示され、内部ではロケーション、帯域幅、遅延などの最適化基準に基づいて MCU のカスケーディングを使用し、MCU ポートと会議を自動的に管理します。これにより、組織で十分に利用されない可能性がある MCU ポートを最適に使用できます。また、Resource Manager は、MCU ポートなどのリソースを予約できるように、スケジューリング機能も提供します。

  - Network Manager

    Network Manager は、Cisco ゲートキーパーやエンドポイント端末などのさまざまなデバイスの設定を管理します。デバイスのアラームやコールまたは会議のステータスをモニタするためのツールを管理者に提供します。

- Cisco Unified Videoconferencing Desktop Server

  Cisco Unified Videoconferencing Desktop Server は、H.323 ビデオ会議に参加する機能を Web ベースのユーザに提供します。デスクトップ クライアントは Desktop Server と通信します。Desktop Server は、コール シグナリングのために Cisco Unified Videoconferencing Manager と通

信し、コールおよび会議メディアのために MCU と通信します。Desktop Server は、デスクトップ クライアントから H.239 へ、およびその逆のインターワーキングを提供します。また、Desktop Server は、Quicktime で表示できる会議をストリームすることもできます。

- Cisco Unified Videoconferencing Recording Server

  Cisco Unified Videoconferencing Recording Server は、会議をレコーディングします。レコーディングされた会議を保存し、アクセスするメカニズムを企業に提供します。単一画面表示では、レコーディングによって、音声、ビデオ、および会議中に行われたデスクトップ共有またはアプリケーション共有が取り込まれます。

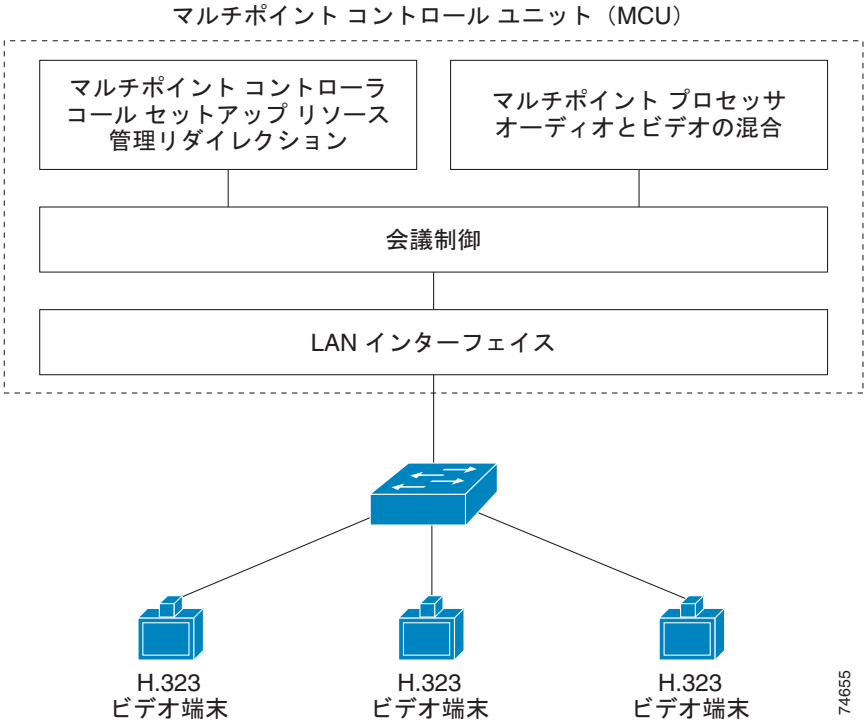
- H.239 ベースのデータ共有

  H.323 エンドポイントは、データ共有のために H.239 をサポートします。このメカニズムでは、エンドポイントは H.323 コールを使用して、音声およびビデオ以外にメディア チャネルを追加します。この追加チャネルは、エンドポイントによるデータ送信に使用されます。エンドポイントに接続されたラップトップまたはデスクトップの画面は、VGA 画像解像度をビデオ コーデックなどにエンコードし、このデータ チャネルによって遠端エンドポイントのディスプレイに表示されるように送信します。ほとんどの会議コラボレーション方法とは異なり、デスクトップまたはアプリケーションの共有データは、ビデオ コールの一部であるメディア チャネルで送信されます。

アーキテクチャ

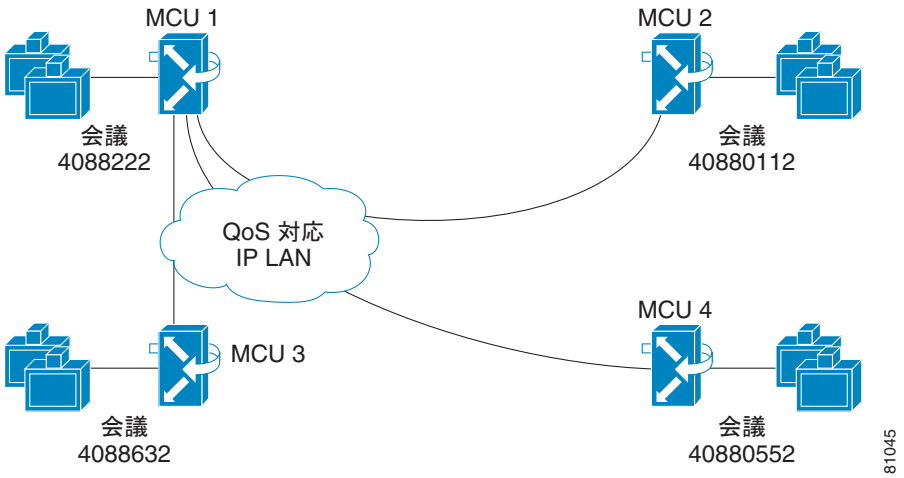
ビデオ会議設計の中心的な要素は MCU であり、MCU が実際の会議を実行します。MCU は、図 22-10 に示すように、シグナリングのためにマルチポイント コントローラと対話し、音声およびビデオ ミキシングのためにマルチポイント プロセッサと対話する会議制御ブロックで構成されます。

図 22-10　MCU の機能コンポーネント



MCU 間で会議をカスケードできます。参加者が会議に追加されたが、1 つの MCU では参加者すべてのためのキャパシティがない場合、別の MCU を使用して会議を拡張できます。2 つの MCU は、図 22-11 に示すように、会議が両方の MCU に存在できるようにするカスケード リンクを持ちます。

図 22-11　　カスケードされた MCU 会議

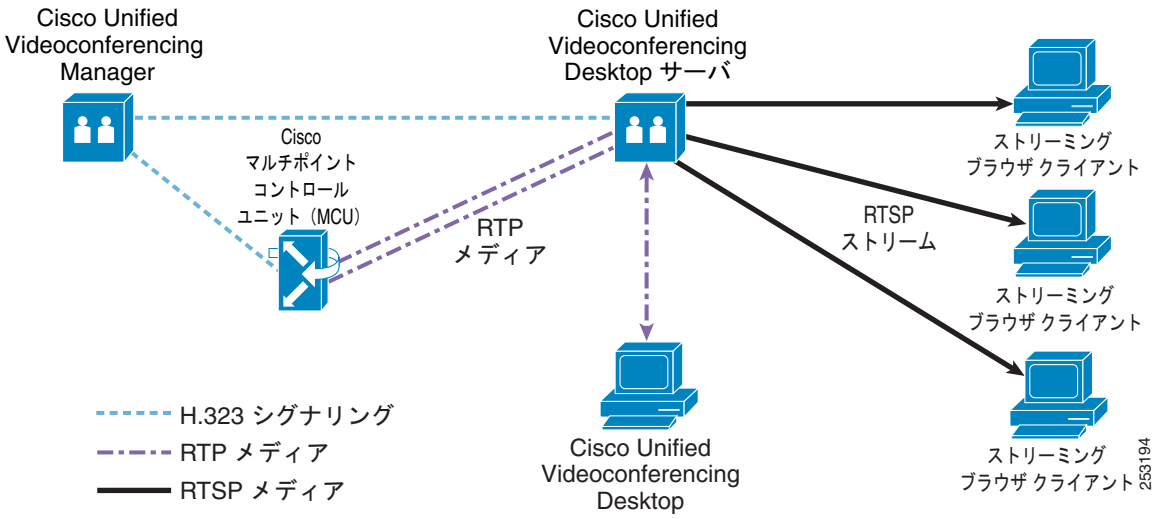


H.323 エンドポイントでは、H.323 エンドポイントが登録できる Cisco IOS ゲートキーパーなどの個別のゲートキーパー デバイスが必要です。Unified CM トランクは、ダイヤル プランに基づいてコール ルーティングを提供できます。Unified CM H.323 トランクは電話会議をゲートキーパーに送信でき、ゲートキーパーはコールを Cisco Unified Videoconferencing Manager にルーティングできます。

（注） SIP ベースのデスクトップ共有は、H.239 に似ており、Binary Flow Control Protocol（BFCP）によってサポートされます。ただし、Cisco Unified Videoconferencing Manager および Unified Videoconferencing MCU は BFCP をサポートしません。そのため、会議コラボレーションにデータ共有機能が必要な場合は、Unified Videoconferencing Manager との統合に Unified CM SIP トランクの使用は推奨しません。

Unified Videoconferencing Manager は、MCU を管理し、Cisco Unified Videoconferencing Desktop Server を使用するデスクトップ クライアントへのコール接続を提供するために使用されます。図 22-12 に、ビデオ会議ソリューションのさまざまなコンポーネントとそれらの相互接続の方法を示します。

図 22-12　Cisco Unified Videoconferencing ソリューション



MCU は会議のメディアを処理します。H.239 では、エンドポイントによって追加メディア チャネルが送信されます。それを使用して、デスクトップ共有または画面共有を会議に送信でき、すべての参加者がそれぞれのエンドポイント画面で表示できます。Cisco Unified Videoconferencing Manager は、MCU および MCU によって会議に追加されるコールを制御します。MCU は Cisco Unified Videoconferencing Manager の内部ゲートキーパーに登録できます。このことにより、Cisco Unified Videoconferencing Manager は MCU と MCU 上の会議を詳細に制御できます。

Cisco Unified Videoconferencing Manager には、企業ユーザ データベースがあります。ユーザは、Cisco Unified Videoconferencing Manager で設定するか、LDAP 統合によって企業 LDAP ディレクトリからインポートできます。そのあとで、ユーザは Cisco Unified Videoconferencing Manager で使用できるスケジューリング機能によって会議をスケジュールできます。会議をスケジュールすることで、会議用の MCU ポートも予約されます。

Cisco Unified Videoconferencing Desktop Server は、Cisco Unified Videoconferencing Manager ゲートキーパーに H.323 エンドポイントとして登録します。このことにより、Desktop Server は MCU 上の会議に参加できます。デスクトップが会議クライアントと連携すると、デスクトップは会議参加者として MCU へのコールを開始し、デスクトップはデスクトップ音声、ビデオ、およびプレゼンテーション共有を使用するコールに参加できます。デスクトップは MCU および Cisco Unified Videoconferencing Manager に対して H.323 クライアントをシミュレートしますが、デスクトップは HTTP/HTTPS で Desktop Server と通信します。デスクトップを追加するたびに別のコールが MCU に追加されるため、そのポート リソースが使用されます。この場合、Desktop Server はデスクトップからの HTTP/HTTPS 接続を、追加データ チャネル用の H.239 を伴う MCU への H.323 コールに変換します。

ユーザは、Real Time Streaming Protocol（RTSP）によるストリーミングを使用して、会議に参加することもできます。デスクトップ（ユーザが音声とビデオを使用して参加でき、デスクトップを共有できる）とは異なり、ストリーミングは会議を参照する機能だけをユーザに提供します。ユーザは、会議に参加したり、カンファレンス ブリッジで発言したりすることはできません。ストリーミングは、ユーザの PC 上の一般的なメディア プレーヤーを使用して実行できます。会議のストリーミングによって、Desktop Server は MCU 上の会議に参加し、ストリーミング会議をリッスンするユーザ数に関係なく 1 つの MCU ポートだけを使用します。

Unified Communications の統合は、ビデオ会議ネットワークと IP ビデオ テレフォニー ネットワークを統合する方法を企業に提供します。Cisco Unified Videoconferencing Manager は、H.323 トランクを使用して Unified CM または他のシステムに接続できる H.323 ゲートキーパーです。このゲートキー

パーは、Unified Communications エンドポイントによって呼び出される付加サービスを提供するために、Empty Capabilities Set（ECS）をサポートします。外部ネットワークへの接続は、Cisco Unified Border Element を両者間のトポロジ隠蔽ゲートウェイとして使用して実行できます。

Desktop Server は、Recording Server にもなります。会議のレコーディングでは、会議モデレータのデスクトップを使用して、会議の音声およびビデオだけでなくデスクトップ共有またはアプリケーション共有もレコーディングします。

Cisco Unified Videoconferencing を WebEx と統合することもできます。H.323、SIP、または ISDN ベースのビデオ コールを行える企業のルームタイプ会議システムまたはデバイスによる標準ベースのビデオを使用する配置には、この統合が有用です。また、音声およびビデオ会議を WebEx 会議用の企業ネットワーク内にとどめる必要がある企業は、この統合を使用できます。

WebEx 会議は、クラウドを使用してデスクトップおよびデータ共有機能を提供します。一方、音声およびビデオは MCU および Cisco Unified Videoconferencing Desktop Server によって処理されます。Cisco Unified Videoconferencing Desktop Server は、デスクトップ クライアントを WebEx 会議内のビデオ パネルとして提供します。

重要な設計上の考慮事項およびソリューションの統合方法の詳細については、次の Web サイトで入手可能な『*Integration Note for Enabling Cisco Unified Videoconferencing Manager and Cisco WebEx*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps7088/prod_installation_guides_list.html

ハイ アベイラビリティ

企業システムには高い可用性が必要であり、ビデオ会議ソリューションでは、すべてのコンポーネントに高い可用性が必要です。

Cisco IOS ゲートキーパーのハイ アベイラビリティのために、HSRP またはゲートキーパー クラスタリングを使用できます。ゲートキーパーは、ゲートキーパー機能を実行する Cisco IOS ルータであり、エンドポイントはこのデバイスに登録します。

ホット スタンバイ ルータ プロトコル（HSRP）

Cisco IOS ルータは、Hot Standby Router Protocol（HSRP; ホット スタンバイ ルータ プロトコル）をサポートします。このプロトコルは、冗長なデバイスに 1 つの仮想アドレスを指定します。アクティブなデバイスが使用できなくなった場合、スタンバイ デバイスが機能を引き継ぐことができます。2 つのデバイスの設定は同一である必要があります。エンドポイントは、使用可能なゲートキーパーに登録し、コールを処理します。

ゲートキーパーの HSRP の詳細については、次の Web サイトで入手可能な『*H.323 VoIP Gatekeeper for Cisco Access Platforms*』を参照してください。

http://www.cisco.com/en/US/docs/routers/access/as5300/software/notes/0042gk.html

Gatekeeper Update Protocol（GUP）

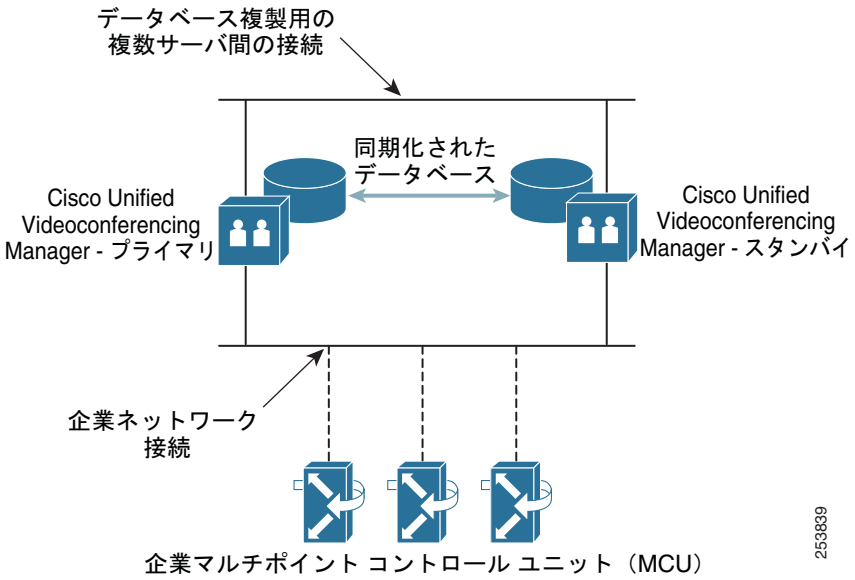
複数の Cisco IOS ゲートキーパーをクラスタリングして、1 つの大きなクラスタにできます。クラスタ内の要素は、エンドポイント登録およびコールで情報を交換します。これにより、登録およびアクティブ コールのフェールオーバーが提供されます。ただし、ゲートキーパー クラスタに登録するエンドポイントおよびトランクは、代替ゲートキーパー機能をサポートしている必要があります。

Cisco Unified Videoconferencing Manager

Cisco Unified Videoconferencing Manager は、同一サーバの追加によるハイ アベイラビリティをサポートしています。プライマリ サーバの IP アドレスは、スタンバイ デバイスによって使用されますが、非アクティブのままです。Cisco Unified Videoconferencing Manager は、別のネットワーク接続を使用して、データベースを設定およびスケジューリングの更新と同期します。プライマリ サーバに障害が発生した場合、2 番めのサーバ上でサービスを有効にすることによって、2 番めのサーバを手動でアクティブにできます。データベースの同期によって、スケジューリングの損失と設定を復元するためのオーバーヘッドが減少します。

図 22-13 に、2 つのネットワークを持つサーバを示します。1 つはサーバ データベースを同期するデータベース レプリケーション用、もう 1 つは企業接続用です。

図 22-13　Cisco Unified Videoconferencing Manager の冗長性



ハイ アベイラビリティと冗長性の詳細については、次の Web サイトで入手可能な『*Configuration Guide for Cisco Unified Videoconferencing Manager*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps7088/products_installation_and_configuration_guides_list.html

MCU

MCU デバイスにハイ アベイラビリティを持たせるには、同一の MCU ポートを使用可能にする必要があります。ただし、MCU ポートを用意するだけでは、会議リソースにハイ アベイラビリティを持たせることはできません。仮想 MCU は Cisco Unified Videoconferencing Manager によって管理されるため、仮想 MCU によって、必要なハイ アベイラビリティが実現されます。使用可能な MCU キャパシティに基づいて、必要なポートが会議に自動的に提供されます。MCU にサービス プレフィックスが設定されている場合（サービス プレフィックスは MCU の会議機能を Cisco Unified Videoconferencing Manager に移すために MCU によって使用されます）、Cisco Unified Videoconferencing Manager は、MCU に障害が発生した場合に会議を使用可能な MCU に拡張します。障害が発生した MCU 上のユーザは、会議に再度参加するために再接続する必要があります。

Cisco Unified Videoconferencing Desktop Server

Desktop Server の冗長性は、別々のサーバを保持することで提供されます。これらのサーバは、ゲートキーパーを実行している Cisco Unified Videoconferencing Manager に登録されます。Desktop Server に障害が発生した場合、ユーザは次の使用可能な Desktop Server にリダイレクトされます。会議は Cisco Unified Videoconferencing Manager によって管理され、MCU 上にあるため、会議の既存のユーザが会議を継続するには再度参加する必要があります。Desktop Server はデータ共有についてハイ アベイラビリティをサポートしないため、デスクトップ共有を再開する必要があります。H.239 を使用してデスクトップを共有していたエンドポイントは、Cisco Unified Videoconferencing Desktop の障害による影響を受けません。ストリーミング会議はデスクトップ クライアントと同じ影響を受けます。両方の機能に同じサーバが使用されるためです。

Cisco Unified Videoconferencing Recording Server

ハイ アベイラビリティのサポートは、Recording Server では使用できません。Desktop Server が使用できない場合、レコーディングは発生しません。2 番めの Desktop Server が使用される場合、レコーディングはこのサーバによって実行できます（その機能が有効な場合）。ただし、レコーディングされる会議にハイ アベイラビリティを持たせるには、Recording Server がアクセス可能な、可用性が高いネットワーク ストレージ デバイスにレコーディングを保存することを推奨します。

キャパシティ プランニング

数多くのエンドポイント登録およびコールがゲートキーパーによってサポートされます。Cisco Unified Communications Sizing Tool では、ゲートキーパーのプラットフォームに基づいてゲートキーパーのキャパシティが計算されます。サイジング ツールは、（有効なログイン認証を持つ）シスコ代理店と従業員が http://tools.cisco.com/cucst で入手できます。

MCU のキャパシティについては、次の Web サイトで入手可能な製品データ シートを参照してください。

- http://www.cisco.com/en/US/products/ps10463/products_data_sheets_list.html
- https://www.cisco.com/en/US/products/hw/video/ps1870/products_data_sheets_list.html

（注）　MCU カスケーディングは、必要に応じてブレードまたはデバイスごとに 1 つのポートを使用します。

MCU のポート数に関する Cisco Unified Videoconferencing Manager のキャパシティおよびその他のサーバ キャパシティについては、次の Web サイトで入手可能な Cisco Unified Videoconferencing Manager データ シートを参照してください。

http://www.cisco.com/en/US/products/ps7088/products_data_sheets_list.html

設計上の考慮事項

適切な Cisco Unified Videoconferencing ソリューションを構築するには、次の設計上の考慮事項が役立ちます。

- MCU は重要な要素であり、MCU の物理ロケーションは重要な設計上の考慮事項です。MCU は、会議トラフィックが最大のロケーションにある必要があります。このことにより、メディア トラフィックのほとんどを同じロケーション内にし、その他の少数の参加者だけが他のロケーションから WAN 経由で参加することで、会議は最適化されます。中央ロケーションには、会議をカスケードできる MCU のプールが必要です。

- Cisco Unified Videoconferencing Manager は、サーバの冗長性を使用して配置する必要があります。サーバの冗長性では、障害の際の切り替え時間を最小にするために、データベース同期を有効にする必要があります。
- Cisco IOS ゲートキーパーの冗長性を使用します。エンドポイントが単一の IP アドレスに到達する必要がある場合、HSRP を使用する必要があります。エンドポイントが RAS による代替ゲートキーパーをサポートする場合、異なるゲートキーパー デバイス間のロード バランシングが必要な場合、およびデバイス障害があってもゲートキーパーが予約およびコール情報を維持する必要がある場合は、ゲートキーパー クラスタリングを使用する必要があります。
- 動的カスケーディングによって会議の WAN ストリームが効率的になるように、Cisco Unified Videoconferencing Manager の仮想 MCU 機能を使用します。
- 会議メディア ストリームの遅延を最小にするために、MCU の近くに Desktop Server を配置する必要があります。
- Cisco Unified Videoconferencing Manager は、LDAP による統合を提供します。企業は、LDAP 統合を使用して、単一のユーザ リストを維持する必要があります。ただし、ユーザ情報の損失を防ぐために、LDAP 同期の前の Cisco Unified Videoconferencing Manager の既存ユーザを、LDAP ディレクトリに移行する必要があります。Cisco Unified Videoconferencing Manager には、企業 LDAP ユーザ以外に維持される、アプリケーション ユーザおよび管理者の別のリストがあります。
- Cisco Unified Videoconferencing Desktop は、MCU とのセッション用に H.235 をサポートします。クライアントと Desktop Server 間のセッションがセキュアになるようにクライアントからサーバへの HTTPS セッションをサポートするには、Cisco Unified Videoconferencing Desktop Server を有効にする必要があります。
- 外部ユーザが Desktop Server または Recording Server にアクセスする必要がある場合、ファイアウォールなどのセキュリティ デバイスは必要なピンホールを提供する必要があります。
- 統合されたスケジューリング メカニズムをユーザに提供するには、Outlook プラグインまたは Lotus Notes 統合などのスケジューリング統合を利用する必要があります。
- 企業ビデオ システムを呼び出して会議に参加できるように外部 H.323 エンドポイントを接続する場合は、Cisco Unified Border Element を使用する必要があります。
- Cisco Unified Videoconferencing Manager、Desktop Server、Recording Server などの複数の機能を 1 台のサーバで実現する場合は、サーバのスケーラビリティを考慮します。

CHAPTER 23

Cisco Unified Presence

Cisco Unified Presence は、Cisco Unified Communications システムの価値を高める多くのコンポーネントから構成されています。このソリューションの主要なプレゼンス コンポーネントは Cisco Unified Presence サーバです。このサーバは Jabber Extensible Communications Platform を備えており、ユーザの連絡可能ステータスとコミュニケーション手段に関する情報を収集する SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）をサポートしています。ユーザの可用性ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。ユーザの通信能力は、ビデオ会議、Web コラボレーション、インスタント メッセージング、基本オーディオなど、ユーザが使用できる通信の種類を示します。

Cisco Unified Presence サーバによって取り込まれた集約されたユーザ情報は、Cisco Unified Personal Communicator、Cisco Unified Communications Manager アプリケーション、およびサードパーティ製のアプリケーションがユーザの生産性を高めるのに役立ちます。これらのアプリケーションは、最も効果的な通信形態を判断することにより、ユーザ間のコミュニケーションの効率性を高めます。

この章では、Cisco Unified Communications システムにおけるプレゼンスとインスタント メッセージングの基本概念を説明し、プレゼンスおよびインスタント メッセージング ソリューションのさまざまなコンポーネントを最適に配置するためのガイドラインを示します。Cisco Unified Presence は、Cisco Unified Communications Manager（Unified CM）5.*x* 以降のリリースと一緒に配置する必要があります。Cisco Unified CM 4.*x* 以前のリリースは Cisco Unified Presence をサポートしていません。

この章では、次のトピックについて取り上げます。

この章の新規情報

表 23-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 23-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
カレンダー統合	「Cisco Unified Presence のカレンダー統合」（P.23-32） 「Outlook Web Access カレンダー統合」（P.23-33） 「Exchange Web Services カレンダー統合」（P.23-35）	2011 年 1 月 31 日
WAN を介したクラスタリング	「WAN を介したクラスタリング」（P.23-23）	2011 年 1 月 31 日
ハイ アベイラビリティ配置	「Cisco Unified Presence クラスタ」（P.23-11） 「Cisco Unified Presence サーバのハイ アベイラビリティ」（P.23-14） 「Cisco Unified Presence の配置モデル」（P.23-14）	2011 年 1 月 31 日
インスタント メッセージング ストレージの要件	「インスタント メッセージング ストレージの要件」（P.23-31）	2011 年 1 月 31 日
AOL を使用したドメイン間フェデレーション	「フェデレーション配置」（P.23-24）	2011 年 1 月 31 日
インスタント メッセージング専用配置	「インスタント メッセージング専用の Cisco Unified Presence 配置」（P.23-17） 「インスタント メッセージング専用配置」（P.23-27）	2010 年 7 月 23 日
Bidirectional-streams Over Synchronous HTTP（BOSH）インターフェイス	「Extensible Messaging and Presence Protocol インターフェイス」（P.23-40）	2010 年 4 月 2 日
Extensible Messaging and Presence Protocol（XMPP）	この章の各項で説明	2010 年 4 月 2 日
インスタント メッセージング	「Cisco Unified Presence の企業インスタント メッセージング」（P.23-29）	2010 年 4 月 2 日
Jabber Extensible Communications Platform（XCP）	「Cisco Unified Presence のアーキテクチャ」（P.23-10）	2010 年 4 月 2 日
Cisco Unified Presence 7.*x* から 8.*x* への移行	「Cisco Unified Presence の移行」（P.23-28）	2010 年 4 月 2 日

プレゼンス

*プレゼンス*とは、ユーザが特定のデバイス セットで通信する能力とその意志を意味します。プレゼンスでは、次の段階またはアクティビティが実行されます。

- ユーザ ステータスのパブリッシュ

  ユーザ ステータスの変化は、ユーザによるキーボード操作、電話機の使用、またはデバイスのネットワーク接続が認識されてへのデバイス接続などが認識されることで自動的にパブリッシュされます。

- このステータスの収集

  パブリッシュされた情報は、すべての利用可能なソースから収集され、プライバシー ポリシーが適用され、現在のステータスが集約および同期されてから、保存されたうえで消費されます。

- 情報の消費

  デスクトップ アプリケーション、カレンダー アプリケーション、およびデバイスが、ユーザ ステータス情報を使用して、エンド ユーザにリアルタイムの更新情報を提供します。これにより、エンド ユーザは、適切な通信方法を判断できるようになります。

ステータス情報は、デバイスやユーザが実行可能な機能（音声、ビデオ、インスタント メッセージング、Web コラボレーションなど）と、デバイスやユーザの状態（連絡可能、ビジー、通信中など）の両方を示します。プレゼンス ステータスは、クライアントへのログインや電話機のオフフックなどの自動イベントによって決定されるか、またはユーザがステータス変更ピックリストから [Do Not Disturb] を選択したなどのユーザによるステータス変更の明示的な通知イベントによって決定されます。

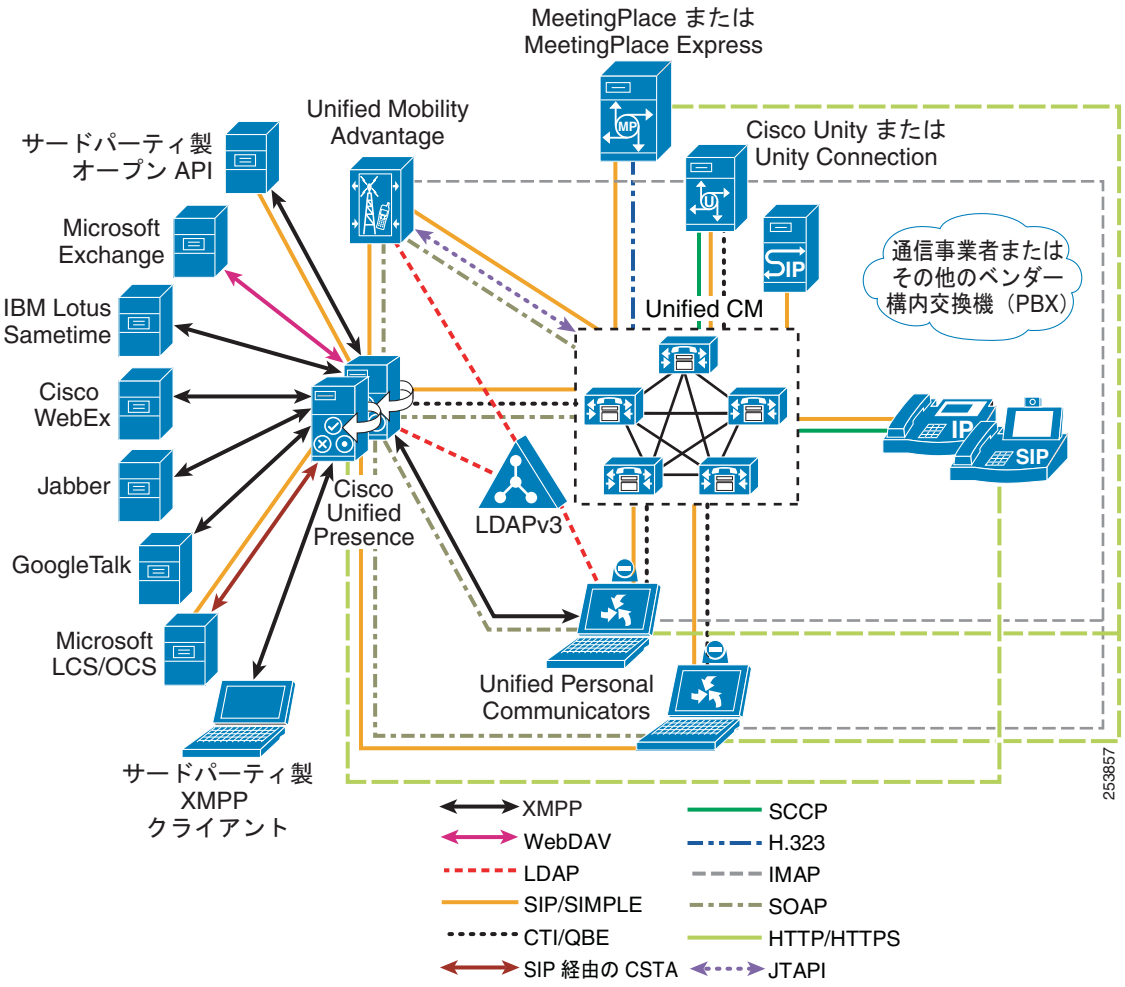
プレゼンスに関する用語として、ウォッチャ、プレゼンス エンティティ（*presentity*）、およびプレゼンス サーバがあります。プレゼンス エンティティは、SIP/SIMPLE クライアントの場合は PUBLISH または REGISTER メッセージを、XMPP クライアントの場合は XML プレゼンス スタンザを使用して、自身の現在のステータスをプレゼンス サーバにパブリッシュします。プレゼンス エンティティは、通信クラスタ内外の Directory Number（DN; ディレクトリ番号）または SIP の Uniform Resource Identifier（URI; ユニフォーム リソース識別子）です。*ウォッチャ*（デバイスまたはユーザ）は、プレゼンス サーバにメッセージを送信することにより、プレゼンス エンティティに関するプレゼンス ステータスを要求します。これに対しプレゼンス サーバは、要求されたプレゼンス エンティティの現在のステータスが含まれたメッセージをウォッチャに返します。

Cisco Unified Presence のコンポーネント

Cisco Unified Presence には、次のコンポーネントが含まれています（図 23-1 を参照）。

- Cisco Unified Presence サーバ
- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified Personal Communicator
- Cisco Unified MeetingPlace または MeetingPlace Express
- Cisco Unity または Unity Connection
- Cisco Unified Videoconferencing または Cisco Unified MeetingPlace Express VT
- Lightweight Directory Access Protocol（LDAP）Server v3.0
- Cisco Unified IP Phone
- サードパーティ製のプレゼンス サーバ
- サードパーティ製の XMPP クライアント
- サードパーティ製アプリケーション

図 23-1　Cisco Unified Presence のコンポーネント



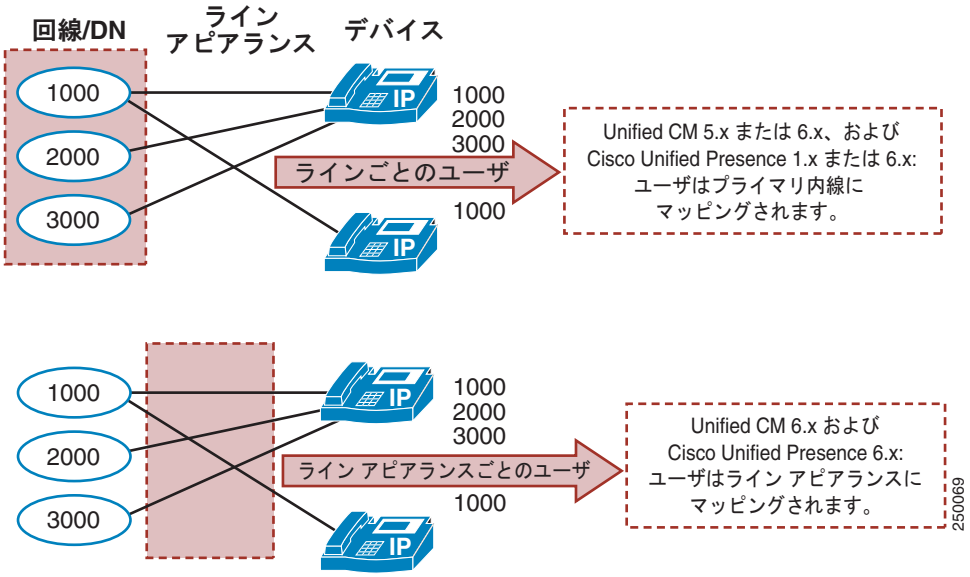
Cisco Unified Presence ユーザ

ユーザのプレゼンスは通常、ユーザのプレゼンス ステータス、システム上のユーザ数、またはユーザのプレゼンス機能で示されます。

Cisco Unified Presence での定義のとおり、ユーザは Cisco Unified CM でデフォルトでエンド ユーザとして指定されており、プライマリ内線が設定されている必要があります。ユーザは実質的にディレクトリ番号に結合されているので、プレゼンス ステータスは、ユーザのプライマリ内線の状態を反映し、ユーザが関連付けられているデバイスの状態は反映されません（図 23-2 を参照）。

Cisco Unified CM でエンド ユーザとして指定されたユーザには、プライマリ内線の設定や、ライン アピアランスの関連付けが可能です。Unified CM で CUP PUBLISH Trunk サービス パラメータを使用する場合は、ユーザにプライマリ内線を設定するだけでなく、ライン アピアランスと関連付ける必要があります。ライン アピアランスに関連付けることによって、ユーザは実質的にライン アピアランス（特定のデバイスのディレクトリ番号）に結合されるので、より詳細できめ細かいプレゼンス情報を集約できます。ユーザを複数のライン アピアランスにマップすることも、各ライン アピアランスに複数のユーザ（最大 5 人）を割り当てることも可能です。エンド ユーザをライン アピアランスに関連付けることを推奨します（図 23-2 を参照）。

図 23-2　プライマリ内線またはライン アピアランスに関連付けられたエンド ユーザ



この章では、*プレゼンス ユーザ*という概念が随所で使用されます。Cisco Unified Presence で定義されるユーザの意味を常に念頭に置いてください。

Unified CM Presence

ユーザのテレフォニー プレゼンス要求は、クラスタ内かクラスタ外かに関係なく、すべて Cisco Unified CM で処理されます。

ウォッチャが、プレゼンス エンティティと同じ Unified CM クラスタ内にある場合、要求を送信した Unified CM ウォッチャは、プレゼンス ステータスなどの応答を直接受信します。

プレゼンス エンティティがクラスタ外にある場合、Unified CM は、SIP トランク経由で外部のプレゼンス エンティティに照会します。ウォッチャが、SUBSCRIBE コーリング サーチ スペースとプレゼンス グループ（いずれも「Unified CM のプレゼンス ポリシー」（P.23-8）の章を参照）に基づいて外部プレゼンスをモニタする権限を持つ場合、SIP トランクはプレゼンス要求を外部プレゼンス エンティティに転送し、外部プレゼンス エンティティからの応答を待って、現在のプレゼンス ステータスをウォッチャに返します。

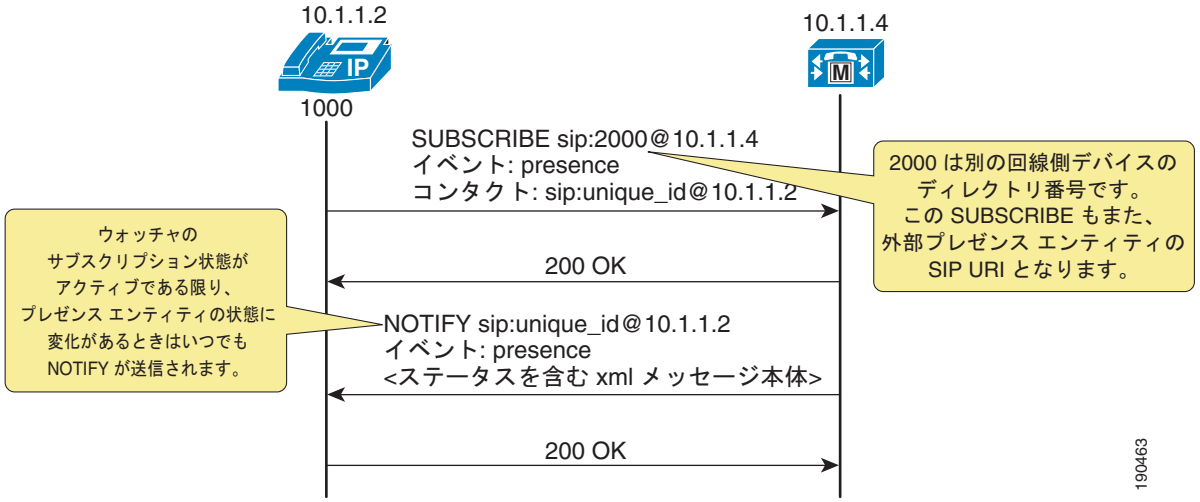
Unified CM クラスタ外のウォッチャは、プレゼンス要求を SIP トランクに送信します。Unified CM がそのプレゼンス エンティティをサポートしている場合、現在のプレゼンス ステータスを応答として返します。Unified CM がそのプレゼンス エンティティをサポートしていない場合、SIP エラー応答によってプレゼンス要求を拒否します。

SIP を使用した Unified CM Presence の配置

Unified CM で、*SIP 回線*という用語は、Unified CM に直接接続され、登録されている SIP 対応のエンドポイントを表し、*SIP トランク*という用語は、SIP をサポートするトランクを表します。プレゼンス ウォッチャとして動作する SIP 回線側エンドポイントは、指定されたプレゼンス エンティティのプレゼンス ステータスを要求する SIP SUBSCRIBE メッセージを Unified CM に送信します。

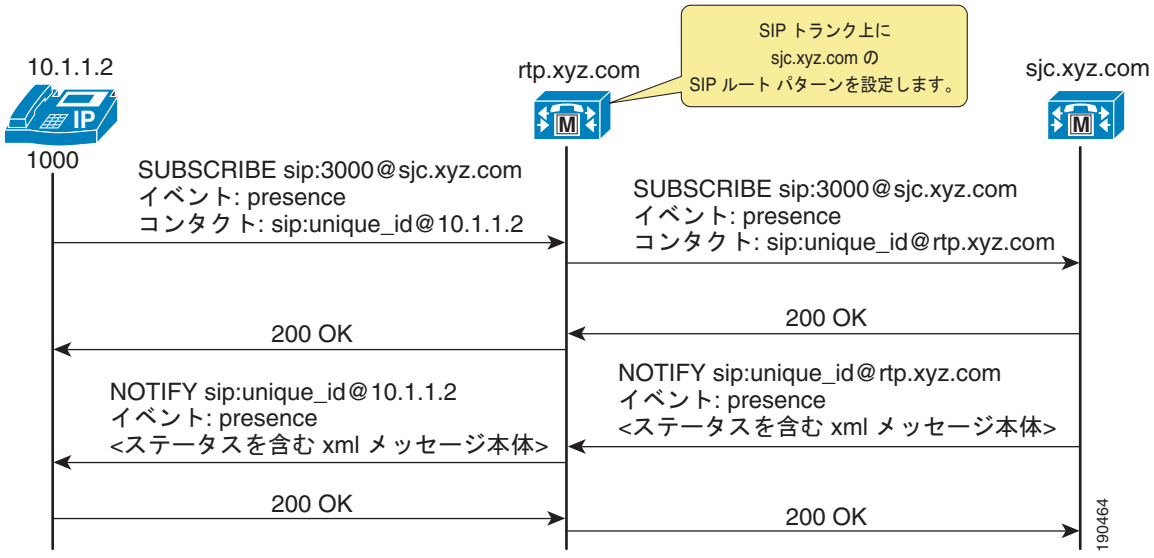
そのプレゼンス エンティティが Unified CM クラスタ内にある場合、Unified CM は、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに応答として送信します（図 23-3 を参照）。

図 23-3　SIP 回線の SUBSCRIBE/NOTIFY の交換



そのプレゼンス エンティティが Unified CM クラスタ外にある場合、Unified CM は、SUBSCRIBE コーリング サーチ スペース、プレゼンス グループ、および SIP ルート パターンに基づいて、SUBSCRIBE 要求を外部の適切な SIP トランクにルーティングします。Unified CM は、プレゼンス エンティティのステータスを示す SIP NOTIFY 応答をトランクで受信すると、SIP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SIP NOTIFY メッセージをプレゼンス ウォッチャに送信して応答します（図 23-4 を参照）。

図 23-4　SIP トランクの SUBSCRIBE/NOTIFY の交換



Unified CM クラスタの外側にあるディレクトリ番号または SIP URI に対する SUBSCRIBE メッセージは、Unified CM 内の SIP トランク上で送受信されます。SIP トランクは、別の Unified CM とのインターフェイスとして動作するか、Cisco Unified Presence サーバとのインターフェイスとして動作できます。

SCCP を使用した Unified CM Presence

Unified CM では、Skinny Client Control Protocol（SCCP）回線側エンドポイントがプレゼンス ウォッチャとして動作できます。SCCP トランクは存在しません。SCCP エンドポイントは、Unified CM に SCCP メッセージを送信して、指定したプレゼンス エンティティのプレゼンス ステータスを要求できます。

そのプレゼンス エンティティが Unified CM クラスタ内にある場合、Unified CM は、SCCP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SCCP メッセージをプレゼンス ウォッチャに送信して応答します

そのプレゼンス エンティティが Unified CM クラスタ外にある場合、Unified CM は、SUBSCRIBE コーリング サーチ スペース、プレゼンス グループ、および SIP ルート パターンに基づいて、SUBSCRIBE 要求を外部の適切な SIP トランクにルーティングします。Unified CM は、プレゼンス エンティティのステータスを示す SIP NOTIFY 応答をトランクで受信すると、SCCP 回線側プレゼンス要求に対し、プレゼンス エンティティの現在のステータスを示す SCCP メッセージをプレゼンス ウォッチャに送信して応答します。

Unified CM のスピード ダイヤルのプレゼンス

Unified CM は、Busy Lamp Field（BLF; ビジー ランプ フィールド）スピード ダイヤルを使用したスピード ダイヤルのプレゼンス機能をサポートしています。BLF スピード ダイヤルは、スピード ダイヤルとプレゼンス インジケータの両方の機能を備えています。ただし、BLF スピード ダイヤルを設定できるのは管理者のみで、システム ユーザは BLF スピード ダイヤルを設定できません。

管理者は、対象のディレクトリ番号に対し、宛先の Unified CM クラスタまたは SIP トランク内のディレクトリ番号に解決可能な BLF スピード ダイヤルを設定する必要があります。SIP URI に対して、BLF スピード ダイヤル用に、BLF SIP 回線側エンドポイントを設定することもできますが、SCCP 回線側エンドポイントの設定はできません。BLF スピード ダイヤルのインジケータは、回線レベルのインジケータであり、デバイス レベルのインジケータではありません。

BLF スピード ダイヤルをサポートしている電話機モデルのリストについては、http://www.cisco.com/ で入手可能な Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

図 23-5 では、電話機のさまざまなタイプの BLF スピード ダイヤルのインジケータを示しています。

図 23-5　スピード ダイヤルのプレゼンスのインジケータ

状態	アイコン	LED
アイドル		
ビジー		
不明		

190465

Unified CM の履歴のプレゼンス

Unified CM は、コール履歴リストに関するプレゼンス機能をサポートしています（電話機の Directories ボタン）。コール履歴リストのプレゼンス機能は、Unified CM Administration 内の **BLF for Call Lists** エンタープライズ パラメータによって制御されます。**BLF for Call Lists** エンタープライズ パラメータは、電話機の Directories ボタンを使用するすべてのページ（不在着信、着信履歴、発信履歴、個人ディレクトリ、社内ディレクトリ）に影響を及ぼし、グローバルに設定されます。

コール履歴リストのプレゼンス機能をサポートしている電話機モデルのリストについては、http://www.cisco.com/ で入手可能な Cisco Unified IP Phone のアドミニストレーション ガイドを参照してください。

コール履歴リストのプレゼンス インジケータには、図 23-5 のアイコン列と同じインジケータが使用されます。LED インジケータはありません。

Unified CM のプレゼンス ポリシー

Unified CM には、プレゼンス ステータスを要求するユーザに対して、ポリシーを設定する機能があります。このポリシーを設定するには、まずプレゼンス ステータスに関する SIP SUBSCRIBE メッセージを特にルーティングするコーリング サーチ スペースを設定します。次に、ユーザを関連付けることのできるプレゼンス グループを設定し、そのグループに対し、他のグループのユーザのプレゼンス ステータスを表示するためのルールを指定します。

Unified CM の SUBSCRIBE コーリング サーチ スペース

Unified CM のプレゼンス ポリシーの第 1 の側面は、SUBSCRIBE コーリング サーチ スペースです。Unified CM は、SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ（電話機またはトランク）から送信されるプレゼンス要求（Event フィールドが Presence に設定された SUBSCRIBE メッセージ）のルーティング方法を決定します。SUBSCRIBE コーリング サーチ スペースは、ウォッチャに関連付けられ、ウォッチャが「確認」できるパーティションをリストします。このメカニズムによって、プレゼンス SUBSCRIBE 要求を通常のコール処理コーリング サーチ スペースから独立してルーティングするという詳細な制御が可能になります。

SUBSCRIBE コーリング サーチ スペースは、デバイス別またはユーザ別に割り当てることができます。ユーザがエクステンション モビリティを使用してデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにユーザ設定が適用されます。

SUBSCRIBE コーリング サーチ スペースを <None> に設定すると、BLF スピード ダイヤルとコール履歴リストのプレゼンス ステータスが機能しなくなり、サブスクリプション メッセージが「user unknown」として拒否されます。有効な SUBSCRIBE コーリング サーチ スペースを指定すると、インジケータが動作し、SUBSCRIBE メッセージが受け入れられて、適切にルーティングされます。

（注）　<None> と定義されたままのコーリング サーチ スペースを残さないでください。コーリング サーチ スペースを <None> に設定したままにすると、プレゼンス ステータスやダイヤル プランの動作が予測困難になる可能性があります。

Unified CM のプレゼンス グループ

Unified CM のプレゼンス ポリシーの第 2 の側面は、プレゼンス グループです。プレゼンス グループには、デバイス、ディレクトリ番号、およびユーザを割り当てることができます。すべてのユーザは、デフォルトで Standard Presence Group に割り当てられています。プレゼンス グループは、定義済みのプレゼンス グループとのユーザのアソシエーションに基づいて、ウォッチャがモニタできる対象を制御します（たとえば、Contractors（派遣社員）から Executives（エグゼクティブ）のモニタは禁止するが、逆は許可するなど）。ユーザがエクステンション モビリティ経由でデバイスにログインするか、管理によってデバイスに割り当てられると、開始されるサブスクリプションにプレゼンス グループのユーザ設定が適用されます。

複数のプレゼンス グループが定義されている場合は、Inter-Presence Group Subscribe Policy サービス パラメータが使用されます。1 つのグループと別のグループとの関係が、許可や禁止ではなく Use System Default 設定による場合、このサービス パラメータの値が有効になります。Inter-Presence Group Subscribe Policy サービス パラメータが **Disallowed** に設定されている場合、SUBSCRIBE コーリング サーチ スペースが許可していても、Unified CM は要求をブロックします。Inter-Presence Group Subscribe Policy サービス パラメータは、コール履歴リストがあるプレゼンス ステータスにのみ適用され、BLF スピード ダイヤルには使用されません。

依存関係レコードを有効にすると、プレゼンス グループは、関連付けられたすべてのディレクトリ番号、ユーザ、およびデバイスをリストできます。依存関係レコードを使用することで、管理者はグループレベルの設定に関する特定の情報を検索できます。ただし、Dependency Record Enterprise パラメータを有効にすると、CPU の使用量が大きくなるので注意してください。

Unified CM のプレゼンス ガイドライン

システム管理者は、Unified CM で Unified CM Administration の中から、ユーザの電話機の状態のプレゼンス機能の設定と制御が可能です。Unified CM 内でプレゼンスを設定する場合は、次のガイドラインに従ってください。

- ユーザの電話機の状態のプレゼンス ステータスを表示できる適切なモデルの Cisco Unified IP Phone を選択します。
- プレゼンス ユーザのプレゼンス ポリシーを定義します。
  - SUBSCRIBE コーリング サーチ スペースを使用して、ウォッチャ プレゼンスベースの SIP SUBSCRIBE メッセージが正しい宛先にルーティングされるように制御します。
  - プレゼンス グループを使用して同類のユーザのセットを定義し、他のユーザ グループのプレゼンス ステータスの更新を許可するか禁止するかを定義します。
- コール履歴リストのプレゼンス機能はグローバルに有効になりますが、プレゼンス ポリシーを使用してユーザ ステータスをセキュリティ保護できます。
- BLF スピード ダイヤルは管理制御され、プレゼンス ポリシー設定の影響を受けません。

（注）　Cisco Unified Communications Manager Business Edition（Unified CMBE）は、Unified CM によってユーザ プレゼンス機能を設定および制御する場合とほぼ同じ方法で使用できます。詳細については、「コール処理」（P.8-1）の章を参照してください。

Cisco Unified Presence のアーキテクチャ

Cisco Unified Presence サーバは、標準ベースの SIP、SIP for Instant Messaging and Presence Leveraging Extensions（SIMPLE）、および Extensible Messaging and Presence Protocol（XMPP）を使用して、クライアントおよびアプリケーションを Cisco Unified Communications システムに統合するための共通の境界ポイントを提供します。また、Cisco Unified Presence は、Simple Object Access Protocol（SOAP）経由の設定インターフェイス、Representational State Transfer（REST）経由のプレゼンス インターフェイス、および JabberWerx AJAX 経由のプレゼンス、インスタント メッセージング、および参加者管理インターフェイスを備えた HTTP インターフェイスを提供します。JabberWerx AJAX インターフェイスは、Cisco Unified Presence 内の Extensible Communications Platform 上の Bidirectional-streams Over Synchronous HTTP（BOSH）インターフェイスと通信します。Cisco Unified Presence サーバは、これらの標準ベースの SIP、SIMPLE、XMPP、および HTTP インターフェイスを使用して、ユーザの能力と属性を収集、集約、および配布します。

シスコ製またはサードパーティ製のアプリケーションにプレゼンスを統合することによって、エンドユーザ エクスペリエンスと効率性を向上させるサービスを提供できます。Cisco Unified Presence サーバの中心となるコンポーネントは、プレゼンス、インスタント メッセージング、参加者、ルーティング、ポリシー、およびフェデレーション管理を処理する Jabber Extensible Communications Platform（XCP）、プレゼンス ステータス収集、ネットワーク ベースの高度なプレゼンス構成、プレゼンス対応ルーティング機能を処理する高度なプレゼンス サービス、アドホック グループ チャットの保管のサポート、外部データベースへの永続的なチャットとメッセージのアーカイブのサポートです。永続的なチャットが有効になっていると、アドホック チャットが開かれている間、アドホック ルームのログが外部の PostgreSQL データベースに保存されます。これにより、ルームのオーナーは、アドホック チャットを永続的なチャットにエスカレーションできます。エスカレーションしないと、アドホック チャットは、チャット終了時に PostgreSQL からパージされます。永続的なチャットが無効の場合、アドホック チャットは、チャットの期間中揮発性メモリに保管されます。

アプリケーション（シスコ製またはサードパーティ製）にプレゼンスを統合することによって、エンドユーザ エクスペリエンスと効率性を向上させるサービスを提供できます。Cisco Unified Presence サーバには、Cisco Unified IP Phone でインスタント メッセージングとプレゼンス ステータスを利用するための IP Phone Messenger アプリケーションがデフォルトで含まれています。Cisco Unified Presence サーバによってサポートされるクライアント、Cisco Unified Personal Communicator というクライアント、インスタント メッセージングとプレゼンス ステータスを統合します。

また、Cisco Unified Presence サーバは、Microsoft Live Communications Server 2005、Microsoft Office Communications Server 2007、および Unified CM に接続された Cisco Unified IP Phone 用の Microsoft Office Communicator クライアントとの相互運用性もサポートしています。Microsoft Office Communicator クライアントの相互運用性には、クリックツーダイヤル機能、電話制御機能、および Cisco Unified IP Phone のプレゼンス ステータスが含まれます。

Cisco Unified Presence クラスタ

Cisco Unified Presence サーバで使用される基礎となるアプリケーション モデルおよびハードウェアは、Unified CM や Cisco Unified Computing System（UCS）プラットフォーム上の Unified CM で使用されるものと同じです（同様の管理インターフェイスなど）。サポートされるプラットフォームの詳細については、次の Web サイトで入手可能な『*Cisco Unified Presence Server Administration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/prod_maintenance_guides_list.html

Cisco Unified Presence は、6 台のサーバで構成され、そのうち 1 つはパブリッシャに指定されています。これは、Unified CM のパブリッシャおよびサブスクライバと同じアーキテクチャ概念を採用しています。Cisco Unified Presence クラスタ内の各サーバをグループ化して、サブクラスタを構成できます。サブクラスタには、最大で 2 台のサーバを関連付けることができます。図 23-6 は Cisco Unified Presence クラスタの基本的なトポロジを示し、図 23-7 は可用性の高いトポロジを示しています。また、Cisco Unified Presence クラスタには、2 台のサーバが設定されたサブクラスタと、1 台のサーバが設定されたサブクラスタを混合して配置することもできます（図 23-8 を参照）。Cisco Unified Presence サーバは独自のクラスタを形成し、Unified CM クラスタの一部として正式に統合されているわけではありません。

図 23-6　Cisco Unified Presence の基本的配置

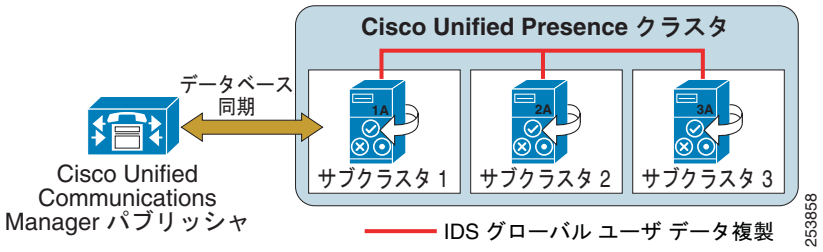


図 23-7　Cisco Unified Presence のハイ アベイラビリティ配置

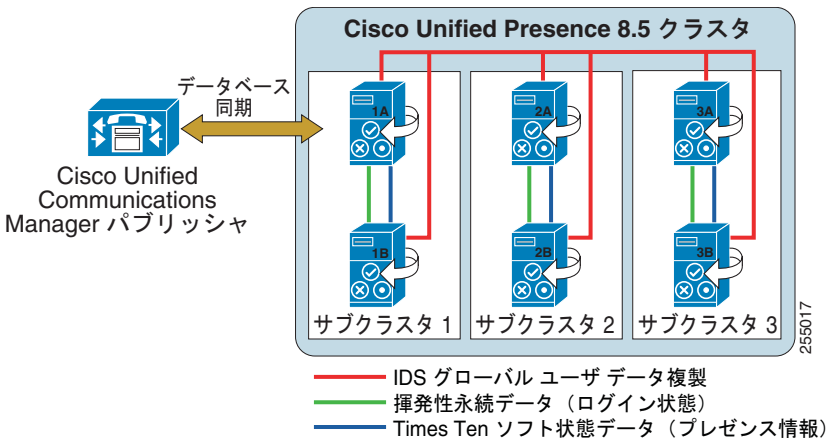
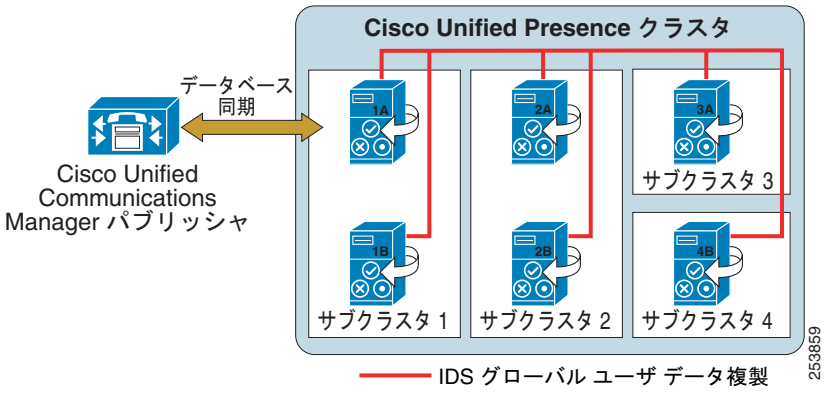


図 23-8　Cisco Unified Presence の混合配置



Cisco Unified Presence パブリッシャは、ユーザ情報とデバイス情報を共有することによって、Unified CM パブリッシャが使用するデータベースを利用し、それを拡張します。Cisco Unified Presence クラスタは、1 つの Unified CM クラスタのみをサポートするので、Cisco Unified Presence のすべてのユーザは、同じ Unified CM クラスタ内で定義する必要があります。

クラスタ内トラフィックは、Cisco Unified Presence と Unified CM の間、および Cisco Unified Presence パブリッシャとサブスクライバ サーバの間に非常に低いレベルで加わります。両方のクラスタは、共通のホスト ファイルを共有し、IPTables を使用した強力な信頼関係を備えています。これらは、データベースとサービスのレベルでは別個の異なるクラスタであり、それぞれの Cisco Unified Presence サーバと Unified CM クラスタは別々に管理する必要があります。現在、クラスタ内トラフィックには、Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）や IPSec は使用されていません。

Cisco Unified Presence サーバの外部システムとのインターフェイスでは、UDP、TCP、TLS 経由で SIP および XMPP トラフィックが送信されます。TLS 相互認証には、Cisco Unified Presence サーバと外部システムの間の証明書のインポートとエクスポートが必要です。TLS サーバ認証（Cisco Unified Presence サーバが、検証用の TLS 証明書をクライアント デバイスに提示）では、ダイジェスト認証によってエンド ユーザを検証します。

Cisco Unified Presence パブリッシャは、ユーザ情報とデバイス情報を共有することによって、Simple Object Access Protocol（SOAP）インターフェイスを使用して、AVVID XML Layer Application Program Interface（AXL API）経由で Unified CM パブリッシャと直接通信します。最初の設定時に、Cisco Unified Presence パブリッシャは、Unified CM ユーザおよびデバイス データベース全体の初期同期を実行します。すべての Cisco Unified Presence ユーザは、Unified CM End User 設定で設定されます。同期の際、Cisco Unified Presence は、Unified CM データベースからこれらのユーザをそれ自体のデータベースに入力しますが、その管理インターフェイスからエンド ユーザ設定を提供することはありません。

Unified CM から最初に Cisco Unified Presence データベースを同期する場合、少し時間がかかることがあります。所要時間は、データベース内の情報量と現在システムにかかっている負荷によって異なります。それ以降は、新しいユーザ情報やデバイス情報が Unified CM に追加されたときに、Unified CM から Cisco Unified Presence へのデータベースの同期がリアルタイムで実行されます。プランニング用には、1 つの Cisco Unified Presence パブリッシャを使用して、Unified CM との初期データベース同期を実行する場合のガイドラインとして、表 23-2 の値を使用してください。

（注）　Cisco Unified Presence は、最大 60,000 ユーザの同期をサポートします（Unified CM と同等）。ただし、Cisco Unified Presence クラスタに対してライセンスされたプレゼンス ユーザの最大数は 15,000 です。

表 23-2　Cisco Unified Presence パブリッシャの同期の所要時間

サーバ プラットフォーム	ユーザ数	同期の所要時間
Cisco MCS 7816	500	5 分
Cisco MCS 7825	1,000	5 分
Cisco MCS 7835	1,000	5 分
	10,000	25 分
Cisco MCS 7845	1,000	5 分
	10,000	20 分
	30,000	70 分

（注）　Cisco Unified Computing System（UCS）プラットフォームの場合の数値は、MCS 7835 の数値（1 基の CPU、2 GB の RAM、2 台の 160 GB ドライブ）および MCS 7845 の数値（2 基の CPU、4 GB の RAM、4 台の 160 GB ハード ドライブ）と同じです。

プランニング用には、1 つの Cisco Unified Presence パブリッシャとサブスクライバ サーバを使用して、Unified CM との初期データベース同期を実行する場合のガイドラインとして、表 23-3 の値を使用してください。

表 23-3　Cisco Unified Presence パブリッシャとサブスクライバ サーバの同期の所要時間

サーバ プラットフォーム	ユーザ数	同期の所要時間
Cisco MCS 7816	500	5 分
Cisco MCS 7825	1,000	10 分
Cisco MCS 7835	1,000	10 分
	10,000	50 分
Cisco MCS 7845	1,000	10 分
	10,000	40 分
	30,000	140 分

（注）　Cisco Unified Presence サーバによる Unified CM からの初期データベース同期の際、同期エージェントがアクティブな間は、管理作業を一切行わないでください。

データベース エントリが更新中でないか、または Sync Agent サービスが停止している場合は、Real-Time Monitoring Tool（RTMT）を使用してクリティカル アラーム **Cisco Unified Presence ServerSyncAgentAXLConnectionFailed** をモニタすることによって、同期エージェントとの接続が切断されていないかを確認できます。

Cisco Unified Presence サーバのハイ アベイラビリティ

Unified CM は、オプションとして、次の冗長性設定から選択できます。

- 2:1 冗長性方式：プライマリ サブスクライバ 2 台ごとに、1 つの共用バックアップ サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ サブスクライバごとに、1 つのバックアップ サブスクライバを設置します。

Unified CM の冗長性の詳細については、「コール処理」（P.8-1）の章を参照してください。

Cisco Unified Presence クラスタは、最大 6 台のサーバで構成されていますが、これを複数のサブクラスタ（最大 3 つのサブクラスタ）に構成してハイ アベイラビリティを実現ができます。サブクラスタには最大 2 台のサーバが含まれ、フェールオーバー イベントの発生時には、サブクラスタの片方のサーバに関連付けられたユーザが、自動的にサブクラスタの他方のサーバを使用できるようになります。Cisco Unified Presence はサブクラスタ間のフェールオーバー機能を提供しません。

Cisco Unified Presence クラスタをハイ アベイラビリティを確保して配置する場合、フェールオーバーの発生時にサブクラスタ内の 1 台のサーバに対してオーバーサブスクリプションにならないよう、1 台のサーバあたりの最大ユーザ数を考慮する必要があります。Cisco Unified Presence クラスタを配置する場合は、クラスタ内のすべてのサーバに同等のハードウェアを使用してください。

Cisco Unified Presence の配置モデル

Unified CM では、次の配置モデルを選択できます。

- 単一サイト
- 集中型コール処理を使用するマルチサイト WAN
- 分散型コール処理を使用するマルチサイト WAN
- WAN を介したクラスタリング

Cisco Unified Presence は、すべての Unified CM 配置モデルでサポートされます。ただし、初期ユーザ データベース同期のために、Cisco Unified Presence パブリッシャを Unified CM パブリッシャと共存させることを推奨します。すべての Cisco Unified Presence サーバは、次の場合を除き、Cisco Unified Presence クラスタ内に共存する必要があります。

- データセンターの地理的冗長性と WAN を介したクラスタリング

  詳細については、「WAN を介したクラスタリング」（P.23-23）を参照してください。

- Cisco Unified Customer Voice Portal（Unified CVP）

  Cisco Unified Presence クラスタは、Cisco Unified Customer Voice Portal 配置の要件に従い、2 つのサイト間に最大 2 台のサーバ（各サイトに 1 台ずつのサーバ）を置いて単一のクラスタを構成し、SIP プロキシ機能のみ（プレゼンス機能なし）を提供できます。この配置では、5 Mbps 以上の帯域幅を確保し（主としてインストールおよび設定用）、遅延を 80 ms Round-trip Tme（RTT; ラウンド トリップ時間）以下に抑える必要があります。Unified CVP の詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『*Cisco Unified Customer Voice Portal SRND*』を参照してください。

Unified CM の配置モデルの詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

Cisco Unified Presence の配置は、ハイ アベイラビリティの要件、合計ユーザ数、および使用するサーバ ハードウェアに依存します。Cisco Unified Presence クラスタの各サーバには、類似したハードウェアを使用することを推奨します。詳細な設定および配置の手順については、次の Web サイトで入手可能な『*Deployment Guide for Cisco Unified Presence*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

可用性が高い Cisco Unified Presence クラスタには、1 つのサブクラスタごとに 2 台のサーバが必要です。これにより、ユーザはサブクラスタ内のサーバ間でフェールオーバーを実行できますが、サポートされる合計ユーザ数とフェールオーバー時間は、有効にする機能、連絡先リストの平均サイズ、およびサーバ上のトラフィック レートによって異なります。Cisco Unified Presence サブクラスタは、2 台のサーバ構成にすると、常にハイ アベイラビリティ構成として動作します。ハイ アベイラビリティは、アクティブ/スタンバイ モデルまたはアクティブ/アクティブ モデルを使用して配置できます。これらのモードは、Sync Agent サービス パラメータの User Assignment Mode によって制御されます。デフォルトで、すべてのユーザはクラスタ内のすべてのサーバに均等に割り当てられます。このパラメータはデフォルト値のままにすることを推奨します。

Cisco Unified Presence でアクティブ/スタンバイ モード（User Assignment Mode を **None** に設定）を実現するには、手動でユーザをサブクラスタの最初のサーバに割り当て、2 番めのサーバにユーザを 1 人も割り当てずにすべての処理を同期させ、サブクラスタの最初のサーバに障害が発生した場合のフェールオーバーに備えます。たとえば、図 23-7 では、最初のユーザをサーバ 1A、2 番めのユーザをサーバ 2A、3 番めのユーザをサーバ 3A、4 番めのユーザをサーバ 1A、5 番めのユーザをサーバ 2A、6 番めのユーザをサーバ 3A、というように割り当てています。これにより、ユーザは、クラスタのすべての「A」サーバに均等に割り当てられます。

Cisco Unified Presence のアクティブ/アクティブ モード（User Assignment Mode を **balanced** に設定）では、自動的にユーザがサブクラスタ内のすべてのサーバに均等に割り当てられます。各サーバは同期され、サブクラスタ内の他のサーバの障害時には、フェールオーバーが可能です。たとえば、図 23-7 では、最初のユーザをサーバ 1A、2 番めのユーザをサーバ 2A、3 番めのユーザをサーバ 3A、4 番めのユーザをサーバ 1B、5 番めのユーザをサーバ 2B、6 番めのユーザをサーバ 3B、というように割り当てます。ユーザは、クラスタ内のすべてのサーバに均等に割り当てられます。

User Assignment Mode を balanced に設定した Cisco Unified Presence のアクティブ/アクティブ配置では、使用される機能、ユーザの連絡先リストのサイズ、および生成されるトラフィック（ユーザ データ プロファイル）に応じた柔軟な冗長構成が可能です。Cisco Unified Presence の完全な冗長性モードのアクティブ/アクティブ配置では、機能に関係なく、サポートされる合計ユーザ数を半分にする必要があります（たとえば、Cisco MCS 7845 サーバをバランス型のハイ アベイラビリティ冗長構成で配置する場合、1 つのサブクラスタでサポートされるユーザ数は、最大 5,000 人になります）。Cisco Unified Presence の非冗長モードのアクティブ/アクティブ配置では、使用される機能、ユーザの連絡先リストの平均サイズ、および生成されるトラフィックをさらに詳細に検討する必要があります。たとえば、プレゼンスとインスタント メッセージングを有効にし、カレンダーとモビリティ統合を無効にした配置で、連絡先リストが平均 30 ユーザ、ユーザ データ プロファイルが少数のプレゼンスとインスタント メッセージングの更新の場合、1 つのサブクラスタあたり 5,000 以上のユーザをサポートできます（Cisco MCS 7845 サーバを使用している場合）。

ハイ アベイラビリティ構成でない Cisco Unified Presence クラスタ配置の場合、サブクラスタの各サーバは、ユーザの最大数までをサポートできます。サブクラスタに別のサーバを追加した後でも、サブクラスタはハイ アベイラビリティ配置と同様に動作しますが、オンライン サーバが容量の上限（有効な Cisco Unified Presence 機能、ユーザの連絡先リストの平均サイズ、およびユーザによって生成されるトラフィック量に基づく）に達すると、サーバに障害が発生した場合にフェールオーバーが成功しないことがあります。

Cisco Unified Presence の配置例

例 23-1　単一の Unified CM クラスタで Cisco Unified Presence を使用

配置要件

- 4,000 ユーザから 13,000 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- インスタント メッセージのロギングおよびコンプライアンスへの準拠が不要
- ハイ アベイラビリティが不要

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 3 つの単一サーバのサブクラスタ、User Assignment Mode = balanced に設定

例 23-2　2 つの Unified CM クラスタ、Cisco Unified Presence を使用

配置要件

- 11,000 ユーザから 24,000 ユーザまで拡張可能
- 2 つの Cisco Unified Communications Manager クラスタ
- インスタント メッセージのロギングおよびコンプライアンスへの準拠が不要
- ハイ アベイラビリティが不要

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 2 つの Cisco Unified Presence クラスタ（各 Cisco Unified Communications Manager クラスタに 1 つずつ）、各クラスタに 3 つのサブクラスタ、各サブクラスタに 1 つずつサーバがあり、すべて User Assignment Mode = balanced に設定

例 23-3　単一の Unified CM クラスタで Cisco Unified Presence を使用

配置要件

- 500 ユーザから 2,500 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager クラスタ
- インスタント メッセージのアーカイブが必要
- ハイ アベイラビリティが必要

ハードウェア：

- Cisco MCS 7835 サーバ

配置：

- **balanced** に設定された User Assignment Mode を使用している 2 台のサーバから構成される 1 つのサブクラスタとクラスタ用の 1 つの PostgreSQL データベース インスタンス

例 23-4　単一の Unified CMBE クラスタと Cisco Unified Presence

配置要件

- 100 ユーザから 500 ユーザまで拡張可能
- 単一の Cisco Unified Communications Manager Business Edition（Unified CMBE）
- インスタント メッセージのアーカイブと永続的なチャットが必要
- ハイ アベイラビリティが必要

ハードウェア：

- Cisco MCS 7825 サーバ

配置：

- **balanced** に設定された User Assignment Mode を使用している 2 台のサーバから構成される 1 つのサブクラスタと、永続的なチャット機能を実現するためのクラスタ内の各サーバに対する一意の PostgreSQL データベース インスタンス

例 23-5　複数の Unified CM Clusters で Cisco Unified Presence を使用

配置要件

- 5,000 ユーザから 40,000 ユーザまで拡張可能
- 複数の Cisco Unified Communications Manager クラスタ
- インスタント メッセージのコンプライアンス準拠が必要
- ハイ アベイラビリティが必要

ハードウェア：

- Cisco MCS 7845 サーバ

配置：

- 各クラスタ間にクラスタ間ピアが設定された複数の Cisco Unified Presence クラスタを設定する必要があります。各 Cisco Unified Presence クラスタに最大 5,000 ユーザに対応する、2 台のサーバから構成される単一サブクラスタを最初に設定し、次に既存の Cisco Unified Presence クラスタにサブクラスタを追加します。単一の Cisco Unified Presence クラスタ内に多数のユーザを割り当てる場合は、User Assignment Mode サービス パラメータを **balanced** に設定します。各 Cisco Unified Presence クラスタの各サーバでインスタント メッセージングのコンプライアンスに準拠するために、サードパーティ製のコンプライアンス サーバを設定します。

インスタント メッセージング専用の Cisco Unified Presence 配置

Cisco Unified Presence クラスタは、Unified CM が特定のユーザの呼制御のために配置されてはいない環境でのエンタープライズ クラスのプレゼンスとインスタント メッセージングを提供するようには配置できません。Unified CM は、やはり手動または LDAP 同期を通じて入力されるユーザ アカウントを確立する必要があります。Cisco Unified Presence のインスタント メッセージング専用配置は、Unified CM から得たユーザ情報を、完全な Unified Communications 配置で行われるのと同じように同期化します。Unified CM は配置されていない場合、および既存の配置済み Unified CM がインスタントメッセージングだけに使用されるわけではない場合のために、プリロードされた Unified CM ソフトウェアを持つ Cisco MCS 7816 メディア コンバージェンス サーバがオプションとして与えられます。

Unified CM クラスタがすでに配置されている既存の Cisco Unified Presence 配置では、インスタントメッセージング専用モードで使用するためのユーザを追加することもできます。これにより、エンドユーザ ライセンス契約書に従ったうえで、インスタント メッセージング専用のユーザに加えて、完全な Unified Communications ユーザも混在させることができます。

Cisco Unified Presence サーバのパフォーマンス

Cisco Unified Presence サーバ クラスタは、シングル サーバとマルチ サーバの両方の構成をサポートします。ただし、複数のサーバを使用する場合、各サーバは、パブリッシャ サーバと同じタイプのサーバ プラットフォームを使用する必要があります。

表 23-4 は、Cisco Unified Presence サーバのハードウェア プラットフォーム要件と、プラットフォームごとにサポートされる最大ユーザ数を示します たとえば、3 台の Cisco MCS 7825 サーバを含む Cisco Unified Presence クラスタを配置し、それぞれのサーバが独自のサブクラスタを構成する場合、合計 3,000 ユーザがサポートされます。1 つの Cisco Unified Presence クラスタでサポートされる最大ユーザ数は 15,000 です。

表 23-4　Cisco Unified Presence サーバ プラットフォームとサポートされるユーザ数

サーバ プラットフォーム	完全 Unified Communications モードでプラットフォームごとにサポートされるユーザ数	インスタント メッセージング専用モードでプラットフォームごとにサポートされるユーザ数
Cisco MCS 7816	500	1,500
Cisco MCS 7825	1,000	3,000
Cisco MCS 7835 または Cisco UCS B シリーズ ブレード サーバ（2 基の vCPU、4 GB の RAM、80 GB ドライブ、1 つの vNIC）	2,500	7,500
Cisco MCS 7845 または Cisco UCS B シリーズ ブレード サーバ（4 基の vCPU、4 GB の RAM、2 台の 80 GB ドライブ、1 つの vNIC）	5,000	15,000

ハードウェア仕様の詳細については、次の Web サイトで入手可能な Media Convergence Server の資料を参照してください。

http://www.cisco.com/en/US/products/hw/voiceapp/ps378/prod_models_home.html

Cisco Unified Presence のライセンス

ユーザ プレゼンス機能は、Unified CM Administration で、Licensing Capabilities Assignment を使用して割り当てます。ユーザは Unified CM からプレゼンス機能をライセンスされるので、Cisco Unified Presence を Cisco Unified CM と統合する必要があります。

チェックボックスは、Unified Presence 用と Unified Personal Communicator 用に 1 つずつ用意されています。ユーザがプレゼンス メッセージの更新を送受信できるようにするには、そのユーザに対して Unified Presence のチェックボックスをオンにする必要があります。そうでない場合は、そのユーザに関するプレゼンス メッセージやステータスの更新が許可されません。Cisco Unified Personal Communicator を使用できるようにするには、そのユーザに対して Unified Personal Communicator のチェックボックスをオンにする必要があります。

Unified CM のライセンスの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Administration Guide*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Unified CM は、複数のデバイスを使用するプレゼンス ユーザに対して、付加ライセンスを使用できる機能を提供します。この機能により、すでに Cisco Unified IP Phone を使用しているプレゼンス ユーザは、Cisco Unified Personal Communicator または Cisco IP Communicator を共有できます。付加ライセンスを有効にするには、Unified CM で Cisco Unified Personal Communicator の Primary Phone オプションを使用します。プライマリ Phone が Cisco Unified Personal Communicator に関連付けられている場合、付加ライセンスが有効になり、ライセンス ユニット計算に反映されます。

Cisco Unified Presence の配置

Cisco Unified Presence は、次のいずれかの構成で配置できます。

- 「シングルクラスタ配置」（P.23-19）
- 「マルチクラスタ配置」（P.23-21）
- 「WAN を介したクラスタリング」（P.23-23）
- 「フェデレーション配置」（P.23-24）
- 「インスタント メッセージング専用配置」（P.23-27）

シングルクラスタ配置

図 23-9 に、Cisco Unified Presence、LDAP サーバ、および Cisco Unified Communications Manager 間で基本的な機能に使用される通信プロトコルを示します。Cisco Unified Presence の管理と設定の詳細については、次の Web サイトで入手可能な Cisco Unified Presence のインストール、管理、および設定に関するマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6837/tsd_products_support_series_home.html

図 23-9　Cisco Unified Presence コンポーネント間の対話

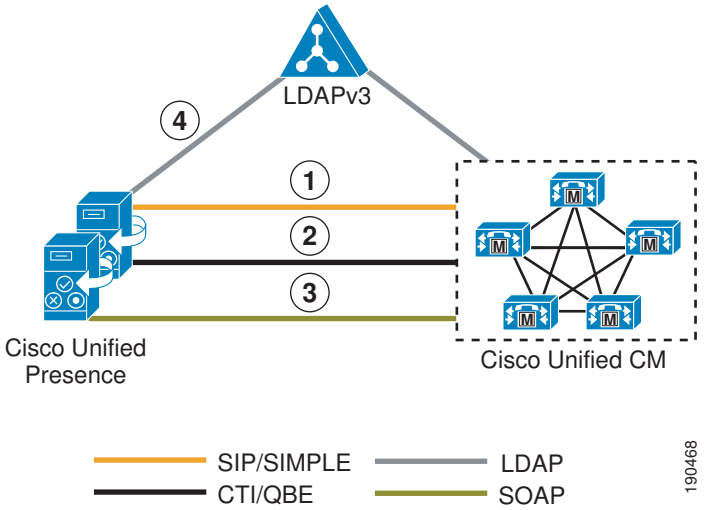


図 23-9 は、Cisco Unified Presence コンポーネント間の次の対話を示します。

1. Cisco Unified Presence サーバと Unified CM 間の SIP 接続は、すべての電話機の状態のプレゼンス情報の交換を処理します。

a. Unified CM の設定では、Cisco Unified Presence サーバをアプリケーション サーバとして Unified CM に追加する必要があります。また SIP トランクが Cisco Unified Presence サーバを指す必要があります。SIP トランクに設定するアドレスは、Cisco Unified Presence サーバに対して解決される Domain Name System（DNS; ドメイン ネーム システム）サーバ（SRV）の Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）、または個別の Cisco Unified Presence サーバの IP アドレスです。Cisco Unified Presence 7.0(3) 以降のリリースは、管理者が Cisco Unified Presence の管理ページからシステム トポロジ ページにノードを追加すると、Cisco Unified Communications Manager アプリケーション サーバ エントリの設定を AXL/SOAP で自動的に処理します。

b. Cisco Unified Presence の設定は、Unified CM Presence Gateway で行われ、Unified CM とプレゼンス情報が交換されます。設定されるのは次の情報です。

Presence Gateway: *server_fqdn*:5070

（注） *server_fqdn* は、Unified CM パブリッシャの FQDN、Unified CM サブスクライバ サーバに解決される DNS SRV FQDN、または IP アドレスです。

ネットワーク内の DNS の可用性が非常に高く、DNS SRV の利用が可能な場合、Cisco Unified Presence パブリッシャとサブスクライバの DNS SRV FQDN を使用して、Unified CM 上に SIP トランクを設定します。また、Unified CM サブスクライバの DNS SRV FQDN を同等の重み付けで使用し、Cisco Unified Presence サーバ上に Presence Gateway を設定します。この設定により、プレゼンス情報の交換に使用するすべてのサーバ間でプレゼンス メッセージングが均等に振り分けられます。

DNS がハイ アベイラビリティでない場合、またはネットワーク内で信頼できるオプションでない場合は、IP アドレスを使用する。IP アドレスを使用すると、単一のサブスクライバが指されるので、プレゼンス メッセージング トラフィックを複数の Unified CM サブスクライバ間で均等に振り分けることはできません。

Unified CM では、PUBLISH メソッド（SUBSCRIBE/NOTIFY ではなく）を設定し、Cisco Unified Presence への SIP トランク インターフェイス上で使用できるようにする CUP PUBLISH Trunk というサービス パラメータによって、通信をさらに簡素化し、使用帯域幅を削減します。CUP PUBLISH Trunk サービス パラメータを有効にした場合、ユーザをプライマリ内線だけでなく、ライン アピアランスと関連付ける必要があります。

2. Cisco Unified Presence と Unified CM との間の Computer Telephony Integration Quick Buffer Encoding（CTI-QBE）接続は、Cisco Unified Presence のプレゼンス対応ユーザが、Unified CM に登録済みの各自に関連付けられた電話機を制御するために使用するプロトコルです。この CTI 通信は、Cisco Unified Personal Communicator が Desk Phone モードで Click to Call を行う場合、または Microsoft Office Communicator が Microsoft Live Communications Server 2005 または Office Communications Server 2007 によって Click to Call を行う場合に実行されます。

a. Unified CM の設定では、ユーザを CTI Enabled グループに関連付け、そのユーザに割り当てられたプライマリ内線で CTI 制御を有効にする必要があります（[Directory Number] ページのチェックボックス）。CTI Manager Service もまた、Cisco Unified Presence パブリッシャおよびサブスクライバとの通信に使用される各 Unified CM サブスクライバ上でアクティブにする必要があります。Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合には、Unified CM で、CTI Enabled グループと役割を使用して、アプリケーション ユーザを設定する必要があります。

b. Cisco Unified Personal Communicator と連携して使用するための Cisco Unified Presence の CTI 設定（CTI サーバおよびプロファイル）は、Unified CM とのデータベースの同期時に自動的に作成されます。すべての Cisco Unified Personal Communicator CTI 通信は、Cisco Unified Presence サーバ経由ではなく、直接 Unified CM で実行されます。

Microsoft Live Communications Server 2005 または Office Communications Server 2007 と連携して使用するための Cisco Unified Presence の CTI 設定（Desktop Control Gateway）では、Desktop Control Gateway の アドレス（Cisco Unified Communications Manager のアドレス）とプロバイダー（Unified CM で以前に設定されたアプリケーション ユーザ）を設定する必要があります。スケーラビリティを拡大させるため、最大 8 個の Cisco Unified Communications Manager アドレスをプロビジョンできます。Cisco Unified Presence サーバ の Desktop Control Gateway の設定で使用できるのは、IP アドレスのみです。

3. AXL/SOAP インターフェイスは、Unified CM からのデータベースの同期を処理して、Cisco Unified Presence データベースにデータを入力します。
   a. Unified CM では、その他の設定は必要ありません。
   b. Cisco Unified Presence セキュリティ設定では、AXL 設定内の Unified CM AXL アカウントのユーザとパスワードを設定する必要があります。

      Sync Agent サービス パラメータである User Assignment をデフォルトの [balanced] に設定すると、Cisco Unified Presence クラスタ内のすべてのサーバに対して、すべてのユーザが均等にロードバランスされます。管理者は、User Assignment サービス パラメータを [None] に変更して、Cisco Unified Presence クラスタ内の特定のサーバに手動でユーザを割り当てられます。
4. LDAP インターフェイスは、ログイン時に、Cisco Unified Personal Communicator ユーザの LDAP 認証に使用します。LDAP 同期と認証の詳細については、「LDAP ディレクトリ統合」（P.16-1）の章を参照してください。

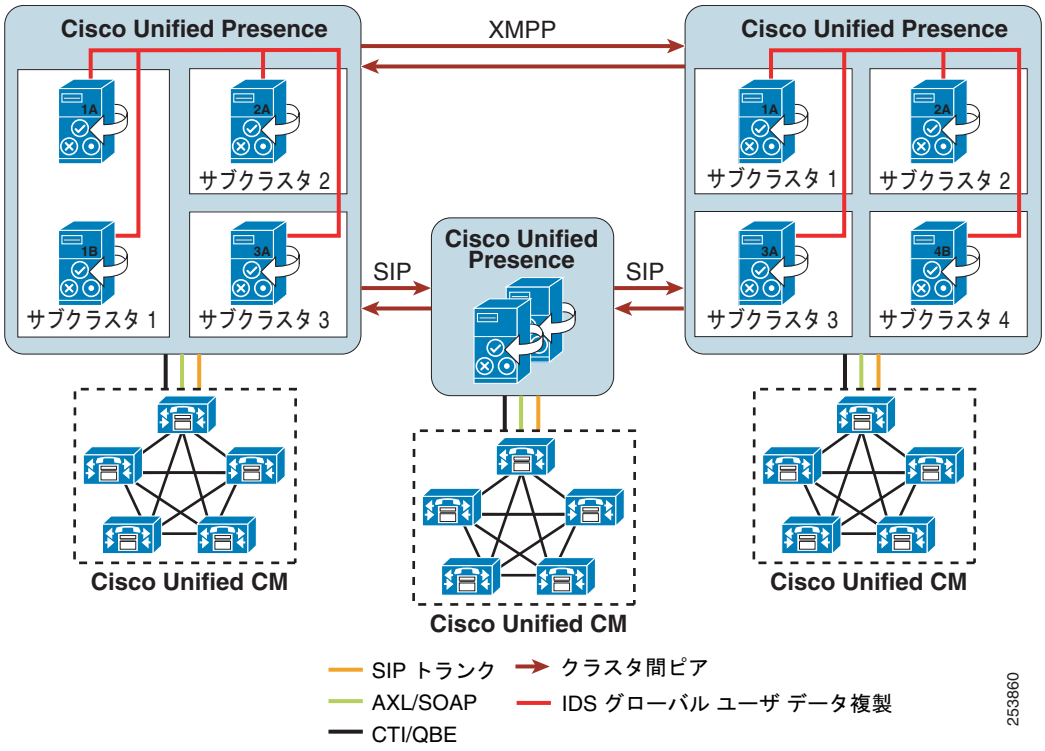
   Unified CM は、手動設定によるすべてのユーザ エントリまたは LDAP からの直接の同期を処理し、Cisco Unified Presence がすべてのユーザ情報を Unified CM から同期させます。Cisco Unified Personal Communicator ユーザが Cisco Unified Presence サーバにログインし、Unified CM で LDAP 認証が有効な場合、Cisco Unified Presence は直接 LDAP に移動し、Bind 操作によって Cisco Unified Personal Communicator ユーザを認証します。Cisco Unified Personal Communicator の認証が完了すると、Cisco Unified Presence は情報を Cisco Unified Personal Communicator に転送してログインを続行します。

   Microsoft Active Directory を使用する場合は、パラメータの選択を慎重に考慮してください。大規模な Active Directory 実装が存在し、設定で Domain Controller が使用されている場合、Cisco Unified Presence で十分なパフォーマンスが得られないことがあります。Active Directory の応答時間を改善するために、場合によっては、ドメイン コントローラをグローバル カタログに追加し、LDAP ポートを 3268 に設定する必要があります。

マルチクラスタ配置

前の項まででは、単一の Cisco Unified Presence クラスタが、単一の Unified CM クラスタと通信する配置トポロジについて説明しました。しかし単一のクラスタ内だけの通信では、プレゼンスやインスタント メッセージングの機能には限りがあります。そこで、プレゼンスとインスタント メッセージングの能力と機能を拡張できるよう、これらのスタンドアロンのクラスタにピア関係を設定することで、同じドメイン内の複数のクラスタ間で通信できるようになります。図 23-10 は、複数のクラスタやサイトを相互接続した場合の Cisco Unified Presence クラスタ間のピア関係を示します。この機能により、1 つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。

図 23-10　Cisco Unified Presence のマルチクラスタ配置



フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco Unified Presence クラスタと、同じドメイン内の個々の Cisco Unified Presence クラスタとの間に、個別のピア関係が設定されている必要があります。このクラスタ間ピアに設定されているアドレスは、リモートの Cisco Unified Presence クラスタ サーバに対して解決される DNS SRV FQDN、または単純に Cisco Unified Presence クラスタ サーバの IP アドレスです。

各 Cisco Unified Presence クラスタ間のインターフェイスには、AXL/SOAP インターフェイスとシグナリング プロトコル インターフェイス（SIP または XMPP）の 2 つが使用されます。AXL/SOAP インターフェイスは、ホーム クラスタ アソシエーションのためにユーザ情報の同期を処理しますが、これは完全なユーザ同期ではありません。シグナリング プロトコル インターフェイス（SIP または XMPP）は、サブスクリプション トラフィックと通知トラフィックを処理し、ユーザが同じドメイン内のリモート Cisco Unified Presence クラスタで検出された場合は、転送前に URI のホスト部分を書き換えます。

Cisco Unified Presence をマルチクラスタ環境に配置する場合、プレゼンス ユーザ プロファイルを決定する必要があります。プレゼンス ユーザ プロファイルは、マルチクラスタ プレゼンス配置の規模とパフォーマンスおよびサポート可能なユーザ数の決定に役立ちます。プレゼンス ユーザ プロファイルによって、一般的なユーザの連絡先（バディ）の数、およびそれらの連絡先の多くがローカル クラスタのユーザか、リモート クラスタのユーザかが確定します。

Cisco Unified Presence クラスタ間で生成されるトラフィックは、プレゼンス ユーザ プロファイルの特徴に直接比例します。たとえば、プレゼンス ユーザ プロファイル A は、30 個の連絡先を持ち、その 20% がローカルの Cisco Unified Presence クラスタのユーザで、80% がリモートの Cisco Unified Presence クラスタのユーザだとします。またプレゼンス ユーザ プロファイル B は、30 個の連絡先を持ち、その 50% がローカルの Cisco Unified Presence クラスタのユーザで、50% がリモートの Cisco Unified Presence クラスタのユーザだとします。この場合、プレゼンス ユーザ プロファイル B は、リモート クラスタ トラフィック量が小さいので、ネットワーク パフォーマンスが若干高く、帯域幅利用率が小さくなります。

WAN を介したクラスタリング

Cisco Unified Presence クラスタは、Wide Area Network（WAN; ワイド エリア ネットワーク）を介して配置されたサブクラスタのノードの 1 つを使用して配置できます。これにより、サイトをまたがるノード間でサブクラスタの地理的冗長性とユーザのハイ アベイラビリティが実現します。次のガイドラインは、Cisco Unified Presence の配置と WAN を介したクラスタリングの計画時に使用する必要があります。

- データセンターの地理的冗長性とリモート フェールオーバー

  Cisco Unified Presence クラスタは、単一サブクラスタ トポロジで 2 つのサイト間に配置できます。このトポロジでは、サブクラスタの一方のサーバが 1 つの地理的サイトに置かれ、サブクラスタの他方のサーバが別のサイトに置かれます。残りのサブクラスタ（これらのサブクラスタ内のノード）はすべて、Cisco Unified Presence パブリッシャと共存したままにする必要があります。この配置では、5 Mbps 以上の帯域幅を確保し、遅延を 80 ms Round-Trip Time（RTT; ラウンド トリップ時間）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。

- ハイ アベイラビリティと規模

  Cisco Unified Presence のハイ アベイラビリティにより、サブクラスタ内の 1 つのノードのユーザは、サブクラスタ内の別のノードに自動的にフェールオーバーされます。最大 2 つのノードで構成される Cisco Unified Presence サブクラスタでは、リモート フェールオーバーは基本的に 2 つのサイト間（各ノードに 1 つのサイト）で行われます。スケーラブルなハイ アベイラビリティの Cisco Unified Presence クラスタでは、最大 3 つのサブクラスタを構成できます。したがって、スケーラブルなハイ アベイラビリティのリモート フェールオーバー トポロジは、次のような 2 つのサイトで構成されます。

  - サイト A : サブクラスタ 1 ノード A、サブクラスタ 2 ノード A、およびサブクラスタ 3 ノード A
  - サイト B : サブクラスタ 1 ノード B、サブクラスタ 2 ノード B、およびサブクラスタ 3 ノード B

  この配置では、1 つのサブクラスタごとに 5 Mbps 以上の帯域幅を確保し、遅延を 80 ms Round-Trip Time（RTT; ラウンド トリップ時間）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。この配置に追加される新しい各サブクラスタには、データベースと状態の複製を処理するために、さらに 5 Mbps の専用帯域幅が必要です。

- ローカル フェールオーバー

  2 つのサイト間の Cisco Unified Presence クラスタ 配置では、1 つのサイトごとに 1 つのサブクラスタ トポロジ（単一ノードまたはハイ アベイラビリティ構成のデュアル ノード）を構成することもできます。この場合、一方のサブクラスタを 1 つの地理的サイトに置き、他方のサブクラスタを別の地理的サイトに置きます。このトポロジにより、ユーザは、異なるサイトまたは場所にフェールオーバーせずに、（ハイ アベイラビリティまたはハイ アベイラビリティでない）ローカル サイトに残ることができます。この配置では、それぞれのサイトの各サブクラスタ間に 5 Mbps 以上の専用帯域幅を確保し、遅延を 80 ms Round-Trip Time（RTT; ラウンドトリップ時間）以下に抑え、TCP によるメソッド イベント ルーティングを行う必要があります。

- 帯域幅と遅延に関する考慮事項

  WAN を介してノードが分割されたトポロジを持つ Cisco Unified Presence クラスタでは、ユーザのクライアント内の連絡先数が、帯域幅の要件や配置の基準に影響を及ぼす可能性があります。Cisco Unified Presence のクラスタ内およびクラスタ間で生成されるトラフィックは、プレゼンス ユーザ プロファイルの特性や配置に必要な帯域幅に直接関係します。帯域幅が小さい（10 Mbps 以下）環境のクライアントでは、リモート連絡先を 25% 以下にすることを推奨します。最大ラウンドトリップ遅延は、常に 80 ms 以下にする必要があります。

- 永続的なチャットとコンプライアンス ロギングに関する考慮事項

  Cisco Unified Presence で永続的なチャット、メッセージ アーカイブ、またはコンプライアンス ロギングが有効であり、サブクラスタが WAN を介して分割されている場合、外部データベース サーバは外部データベース サーバを使用する Cisco Unified Presence サーバと同じ WAN 側に存在する必要があります。単一サーバで複数のデータベース インスタンスをサポートする機能と外部データベース サーバを同じ WAN 側に存在させる要件により、Cisco Unified Presence クラスが WAN を介して分割された場合は、2 つの外部データベース サーバが必要です。

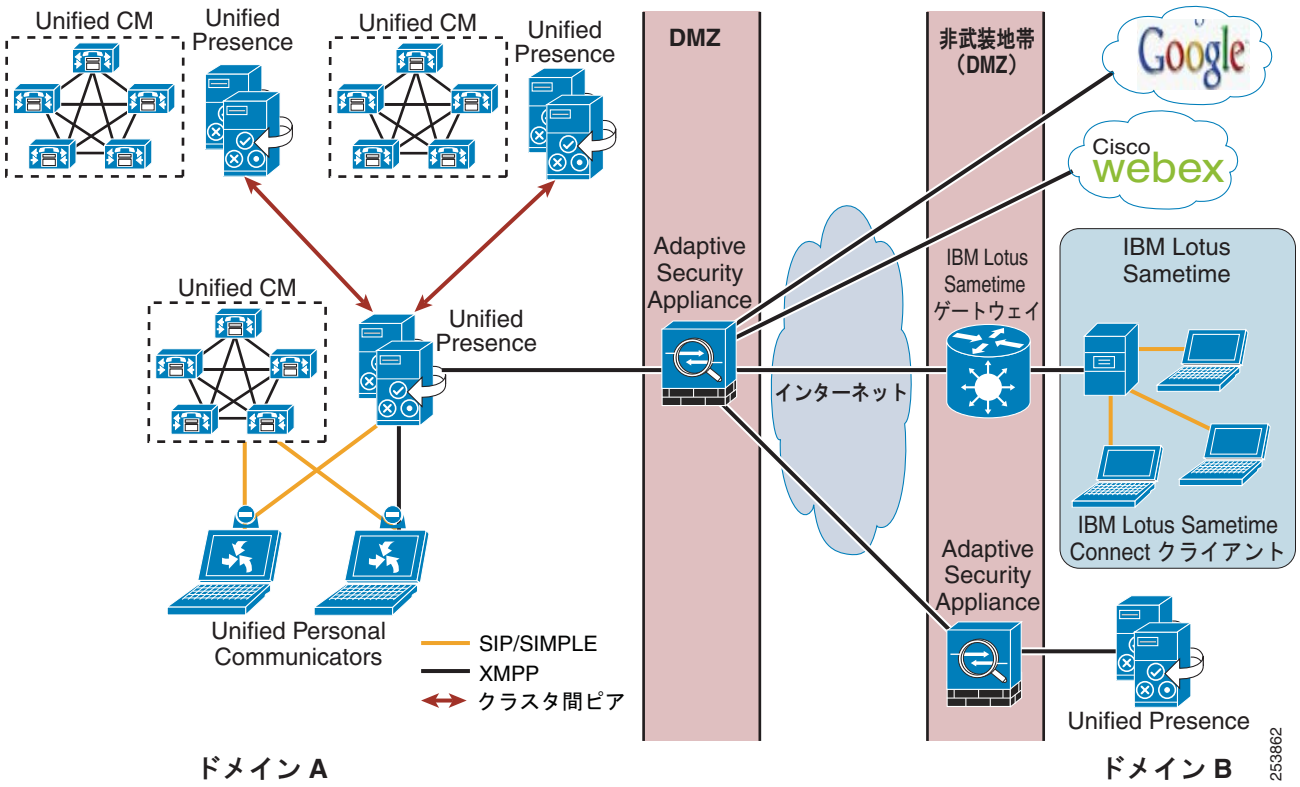
フェデレーション配置

Cisco Unified Presence は企業間通信に対応するため、異なるドメイン間でプレゼンス情報やインスタント メッセージング通信を共有するドメイン間フェデレーションを搭載しています。ドメイン間フェデレーションの構築には、2 つの明示的な DNS ドメインを設定し、さらに DMZ にセキュリティ アプライアンス（Cisco Adaptive Security Appliance）を置いて、フェデレーション接続を企業で終端させる必要があります。フェデレーション ドメインが同じ信頼性境界内に存在する場合（配置では単一データセンター内にすべてのコンポーネントが含まれます）は、Adaptive Security Appliance を使用する必要がありません。ドメイン間フェデレーションについては、次の Web サイトで入手可能な『*Integration Guide for Configuring Cisco Unified Presence Interdomain Federation*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

図 23-11 は、ドメイン A とドメイン B という 2 つの異なるドメインの間の、基本的なドメイン間フェデレーション配置を示します。DMZ の Adaptive Security Appliance（ASA）は、社内への境界として使用されます。XMPP トラフィックはそのまま通過しますが、SIP トラフィックは検査されます。フェデレーションのすべての着信および発信トラフィックは、フェデレーション ノードとして有効化された Cisco Unified Presence サーバ経由でルーティングされ、内部ではユーザがいるクラスタの適切なサーバにルーティングされます。マルチクラスタ配置では、クラスタ間ピアはトラフィックをドメイン内の適切なホーム クラスタに伝達します。大企業での配置においては、複数のノードをフェデレーション ノードとして有効化できます。その場合、各要求は、DNS SRV ルックアップから返されるデータのラウンドロビン実装に基づいてルーティングされます。

図 23-11　Cisco Unified Presence XMPP フェデレーション（ドメイン間）



また、Cisco Unified Presence では、Microsoft と AOL とのドメイン間フェデレーションを行えるように SIP からの設定も提供されます（図 23-12 を参照）。Cisco Unified Presence は、Microsoft Office Communications Server（OCS）および Live Communications Server（LCS）とのドメイン間フェデレーションによって、基本プレゼンス（応対可能、不在、ビジー、オフライン）とポイントツーポイントのインスタント メッセージングを提供します。高度なプレゼンス機能（通話中、会議中、休暇中など）や高度なインスタント メッセージング機能はサポートされていません。Cisco Unified Presence による AOL とのドメイン間フェデレーションにより、AOL パブリック コミュニティ（aim.com、aol.com）のユーザ、AOL によりホストされたドメインのユーザ、および AOL とのフェデレーションを行う遠端企業のユーザ（つまり、AOL はクリアリング ハウスとして使用されます）とのフェデレーションが可能になります。

（注）　Cisco Unified Presence では、AOL ネットワーク（ホストされたネットワークとパブリック コミュニティの両方から構成されます）の各ドメインに対して SIP フェデレーション（ドメイン間と AOL）を設定する必要があります。ホストされた一意のドメインをそれぞれ設定する必要がありますが、AOL ネットワークではユーザを user@aol.com または user@aim.com と指定できるため、単一の aol.com パブリック コミュニティだけを指定する必要があります。

ドメイン間フェデレーション設定では、図 23-12 に示すように、Cisco Unified Presence と Microsoft Office Communications Server（OCS）の間の特定のフェデレーションも可能です。Cisco Unified Presence は、Microsoft Office Communications Server（OCS）または Live Communications Server（LCS）とのドメイン間フェデレーションによって、基本プレゼンス（応対可能、不在、ビジー、オフライン）とポイントツーポイントのインスタント メッセージングを提供します。高度なプレゼンス機能（通話中、会議中、休暇中など）や高度なインスタント メッセージング機能はサポートされていません。

図 23-12　Cisco Unified Presence SIP フェデレーション（ドメイン間）

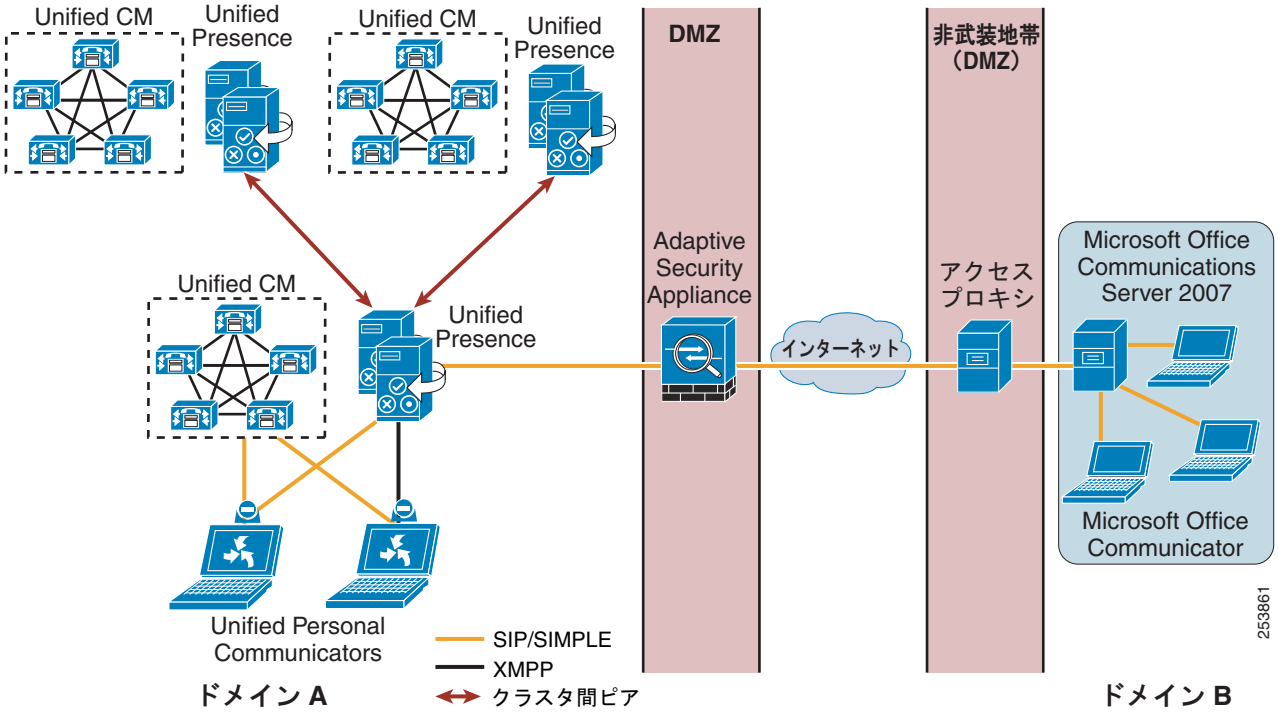


表 23-5 は、Cisco Unified Presence と Microsoft Office Communications Server の間の状態のマッピングを示します。

表 23-5　プレゼンス ステータスのマッピング

シスコでのステータス	シスコのランプの色	Microsoft Office Communications Server でのステータス	AOL に対するステータス
不在	赤	退席中	退席中
割込不可	赤	取り込み中	退席中
取り込み中	赤	取り込み中	退席中
電話中	黄色	取り込み中	退席中
会議中	黄色	取り込み中	退席中
退席中	黄色	退席中	退席中
応対可能	緑	応対可能	応対可能
応対不可 / オフライン	グレー	オフライン	オフライン

（注）　Cisco Unified Presence は、他のドメインが、DNS SRV によって Cisco Unified Presence サーバを検出できるように、ドメインに関する DNS SRV レコードをパブリッシュする必要があります（SIP、XMPP、および各テキスト会議ノード）。Microsoft Office Communications Server または Live Communications Server 配置では、Cisco Unified Presence が Access Edge サーバ上の Public IM Provider として設定されているので、このようなパブリッシュが必要です。Cisco Unified Presence サーバが DNS SRV を使用している Microsoft ドメインを検出できない場合、Cisco Unified Presence で外部ドメインの静的ルートを設定する必要があります。

Cisco Unified Presence のフェデレーション配置は、Adaptive Security Appliance と Cisco Unified Presence サーバ間にロード バランサを使用することで、冗長性のある構成にできます。または、冗長構成の Adaptive Security Appliance によって冗長性を実現することもできます。

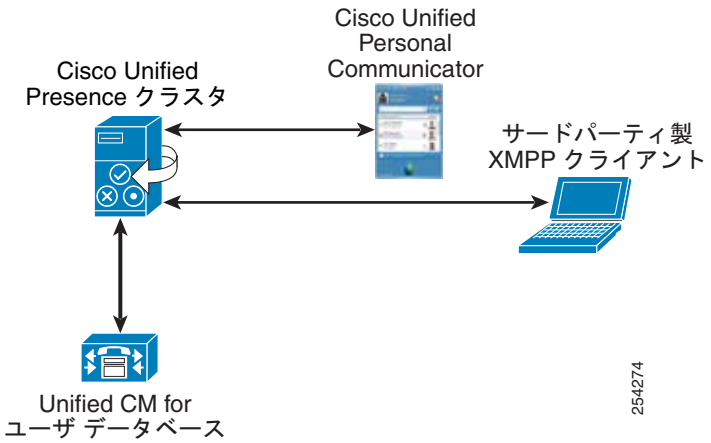
フェデレーション配置に関するその他の設定と配置上の考慮事項については、次の Web サイトで入手可能な『*Integration Guide for Configuring Cisco Unified Presence for Interdomain Federation*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

インスタント メッセージング専用配置

Cisco Unified Presence では、エンタープライズ クラスのインスタント メッセージング専用のソリューションが可能です。このソリューションでは、まだ完全な Unified Communications 配置が提供されていないケースで配置するために、「Cisco Unified Presence の企業インスタント メッセージング」（P.23-29）に定義されているとおりのプレゼンスとインスタント メッセージングの完全なサポートが提供されます。インスタント メッセージング専用の環境に配置された Cisco Unified Presence クラスタは、1 つのクラスタ内で最大 3 台のサーバをサポートします（図 23-13 を参照）。Cisco Unified Presence 上のインスタント メッセージング専用ユーザも、LDAP 同期を利用するか、または手動のプロビジョニングによって、AXL/SOAP インターフェイスを通じて Unified CM からプロビジョニングできます。Cisco Unified Personal Communicator 8.0 とサードパーティ製 XMPP クライアントが、Cisco Unified Presence のインスタント メッセージング専用配置でサポートされるクライアントです。これ以外は、Cisco Unified Presence のその他の設計ガイドラインがすべて当てはまります。

図 23-13　　インスタント メッセージング専用ユーザ モードの配置



Cisco Unified Presence の移行

Cisco Unified Presence の配置のリリース 8.*x* への移行は、Cisco Unified Presence 7.*x* からだけサポートされています。バージョン 7.*x* から 8.*x* に移行した場合、Cisco Unified Presence クラスタ上のユーザ割り当てはサーバ単位で維持されます。

Cisco Unified Presence の移行には、次のガイドラインが適用されます。

- 複数のクラスタを使用した Cisco Unified Presence 7.*x* の配置では、Cisco Unified Presence 8.*x* にアップグレードする前に、クラスタ内の各サーバでプレゼンス エンジンを非アクティブにする必要があります。非アクティブにしたプレゼンス エンジンは、すべてのサーバを Cisco Unified Presence 8.*x* にアップグレードしてから再アクティブ化してください。
- 複数のクラスタを使用した Cisco Unified Presence 7.x の配置では、すべてのクラスタを同時に Cisco Unified Presence 8.*x* にアップグレードすることを推奨します。
- Cisco Unified Presence の配置をバージョン 8.*x* に移行すると、別の標準プロトコル XMPP が導入され、Jabber XCP アーキテクチャが追加されます。Cisco Unified Personal Communicator 7.*x*、Microsoft Office Communications Server とのドメイン間フェデレーション、およびサードパーティ製のアプリケーションのすべてで、SIP/SIMPLE サブスクリプションが作成されます。アクティブな SIP/SIMPLE サブスクリプションの数は、Real-Time Monitoring Tool（RTMT）の Active Subscription カウンタを使用して参照できます。Cisco Unified Presence 8.*x* では、これらのサブスクリプションは SIP Federation Connection Manager を使用して管理されます。アクティブな SIP/SIMPLE サブスクリプションの数が非常に多い場合（20,000 を超える場合）や、アップグレード後にサブスクリプションが失敗するようになった場合は、SIP Federation Connection Manager のサービス パラメータ **Pre-allocated SIP stack memory (bytes)** を現在のデフォルト値の 2 倍の値に設定することを推奨します。

Cisco Unified Presence サーバのポリシー

Cisco Unified Presence サーバのポリシーは、管理者ではなく、ユーザが設定します。ユーザがポリシー ルールに変更を加えなければ、すべてがオープンで利用可能なデフォルトのルールが適用されます。すべてのポリシー設定は、https://<*cup_server_address*>/cupuser/ の Cisco Unified Presence ユーザ ページにある [User Options] 領域で制御できます。

ユーザは、これらのルールが適用されるウォッチャのアクセス コントロール リスト（ACL）が入ったルール セットを設定できます。各ルール セットには、次の 3 種類のルールがあります。

- 表示ルール
  - ブロック：ウォッチャに対して応対不可のプレゼンス ステータスが表示され、ユーザのデバイス ステータスは表示されません。
  - Reachability Only：ウォッチャに対して全体のプレゼンスだけが表示され、デバイスの詳細情報は表示されません。
  - すべての状態（デフォルト）：ウォッチャに対して全体のプレゼンスに加え、フィルタリングされていないデバイス ステータス情報がすべて表示されます。
- プレゼンス ルール
  - 優先順位ベースのルール（最初に一致した項目）に従ってプレゼンス（away、available、busy、unavailable、do not disturb、unknown）が表示されます。
  - デバイス タイプ、メディア タイプ、カレンダー ベースのルール（たとえば、携帯電話が busy またはカレンダーが busy の場合は、全体のプレゼンスを busy とする。インスタント メッセージング デバイスのいずれかが do-not-disturb の場合、全体のプレゼンスを do-not-disturb とする）。電話から設定された do-not-disturb はクライアント デバイスに伝達されません。

- フィルタリング ルール
  - 特定のデバイス タイプ、メディア タイプ、またはカレンダーのプレゼンス ステータスを除外します。

フィルタリング ルールはプレゼンスの判定に先立って適用されるので、フィルタリングされたデバイスのステータスが、ユーザのプレゼンス ステータスに影響を与えることはありません。ユーザはまた、プレゼンス ルールとフィルタリング ルールに使用するデバイス タイプ（たとえば、携帯電話、オフィスの電話など）を定義できます。

プライバシー リストはサブスクリプションに基づくため、連絡先リストのユーザは常にユーザのプレゼンスを確認することを許可されます。ユーザの連絡先リストに存在するユーザをブロックするには、ブロックするユーザをブロック リストに明示的に追加する必要があります。

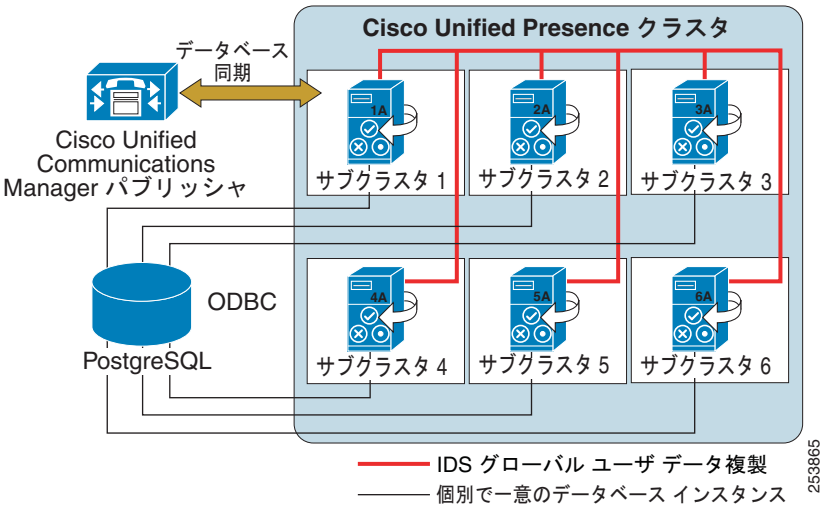
Cisco Unified Presence の企業インスタント メッセージング

Cisco Unified Presence には、Jabber Extensible Communications Platform（XCP）でサポートされている企業インスタント メッセージング機能が組み込まれています。また、マルチデバイス ユーザ エクスペリエンスのサポートを向上するためにいくつかの変更を行うことができます。Cisco Unified Presence では、Jabber XCP インスタント メッセージング ルーティング アーキテクチャが変更され、最初のインスタント メッセージが、既存の Jabber XCP インストールで行われるように最も優先順位の高いデバイスにルーティングされるのではなく、ユーザの負ではない優先順位のすべてのログイン済みデバイスにルーティングされます。Cisco Unified Presence SIP クライアントおよび XMPP クライアント間のポイントツーポイントのインスタント メッセージングの下位互換性サポートは、IM ゲートウェイによって提供されます。

マルチユーザ チャットとも呼ばれるテキスト会議は、アドホック グループ チャットおよび永続的なグループ チャットとして定義され、Jabber XCP 機能セットの一部としてサポートされます。また、オフライン インスタント メッセージング（現在オフラインであるユーザのためにインスタント メッセージを保存する機能）も Jabber XCP 機能セットの一部としてサポートされます。Cisco Unified Presence では、これらの各インスタント メッセージング機能における保存は、異なる場所で処理されます。オフライン インスタント メッセージングは、Cisco Unified Presence IDS データベースにローカルに保存されます。アドホック グループ チャットは、Cisco Unified Presence でメモリ内にローカルに保存されます。永続的なグループ チャットには、チャット ルームおよび会話を保存するための外部データベースが必要です。外部データベースとしては、PostgreSQL だけがサポートされています（http://www.postgresql.org/ を参照）。

Cisco Unified Presence では、外部データベースの基本的なインターフェイスが使用され、データベースの管理、インターフェイス フック、または設定は提供されません。Cisco Unified Presence を永続的なグループ チャットとともに配置する場合は、クラスタ内の各サーバに個別のデータベース インスタンスが必要です（図 23-14 を参照）。データベース インスタンス間で同じハードウェアを共有することはできますが、必ずしも共有する必要はありません。

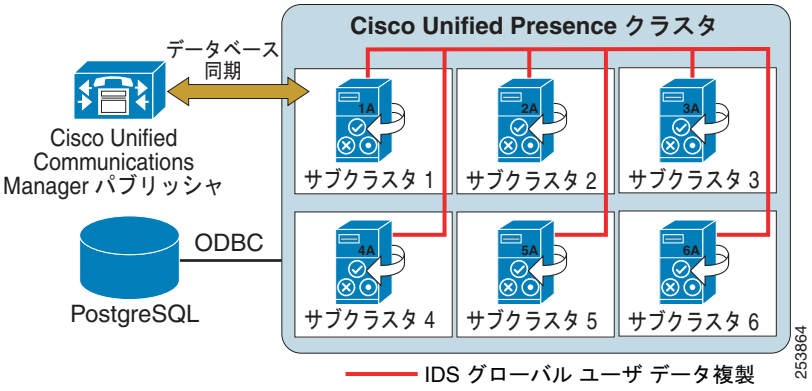
図 23-14　Cisco Unified Presence の永続的なチャット



Cisco Unified Presence のメッセージ アーカイブとコンプライアンス準拠

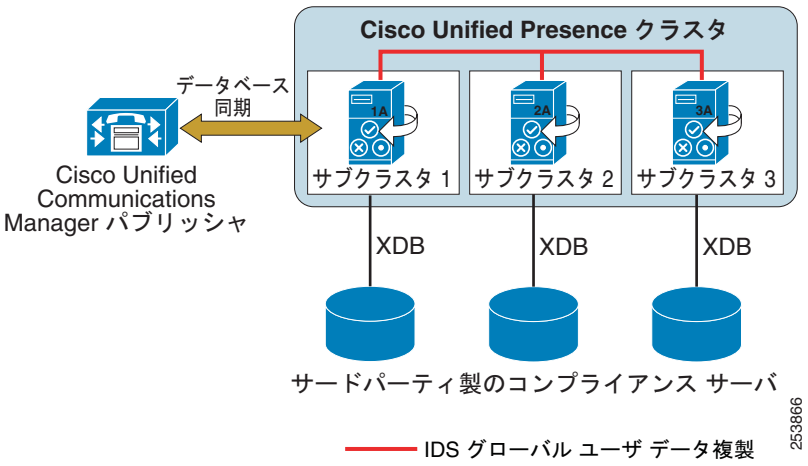
Jabber XCP アーキテクチャの一部として、Cisco Unified Presence にはメッセージ アーカイバ コンポーネントが含まれています。このコンポーネントによって、ブロックしないネイティブなコンプライアンス準拠の一部として、テキスト会議メッセージ、フェデレーション メッセージ、およびクラスタ間メッセージを外部データベースにロギングできます。Cisco Unified Presence におけるネイティブなコンプライアンス準拠およびメッセージ アーカイブには、図 23-15 に示すように、クラスタごとに PostgreSQL データベース インスタンスが必要です。同じデータベースを複数のクラスタで共有できますが、マルチクラスタ配置において多数のユーザがいる場合には、複数のデータベース サーバが必要になる可能性があります。

図 23-15　Cisco Unified Presence のネイティブなコンプライアンス準拠とメッセージ アーカイブ



メッセージのロギング、およびメッセージ配信とメッセージ内容へのポリシーの適用が可能な、サードパーティ製のブロックするコンプライアンス ソリューションは、サードパーティ製のコンプライアンス サーバ ソリューションによって提供されます。Cisco Unified Presence におけるサードパーティ製品によるコンプライアンス準拠には、図 23-16 に示すように、クラスタ内の各サーバにコンプライアンス サーバが必要となります。

図 23-16　Cisco Unified Presence におけるサードパーティ製品によるコンプライアンス準拠



インスタント メッセージング ストレージの要件

メッセージ アーカイブと永続的なチャット機能は、外部データベースを使用してメッセージをオフラインで保存します。配置のストレージ要件には、カスタマー トポロジ、データベースの調整方法、組織内でのメッセージングの使用方法などの複数の考慮事項が存在します。次の計算は、外部データベース ストレージ配置のロー データベース ストレージ要件を見積もるために使用する入力値のガイドラインを提供します。これらの計算では、シングルバイト文字データ エンコーディングを前提としています。したがって、国際化された文字セットが使用される場合は追加のストレージが必要になることがあります。

Cisco Unified Presence は SIP クライアントと XMPP クライアントの両方をサポートし、プロトコルに応じて 1 つのメッセージあたりのオーバーヘッドのサイズが若干異なります。メッセージ アーカイブの 1 つのメッセージあたりのオーバーヘッドは、実際には配置、Jabber ID/UserID サイズ、クライアント タイプ、およびスレッド ID に応じて大きくなったり、小さくなったりすることがあります。したがって、平均のオーバー サイズが使用されます。SIP ベースのメッセージの場合、平均オーバーヘッドは 800 バイトになり、XMPP メッセージの場合、平均オーバーヘッドは 600 バイトになります。

Cisco Unified Personal Communicator 7.*x* ユーザに対する 1 か月あたりのメッセージ アーカイブの最低ストレージ要件（バイト単位）は、次のように計算できます。

（ユーザ数）＊（1 時間あたりのメッセージ数）＊（1 か月あたりのビジー時間数）＊（800 +（3 ＊ 1 つのメッセージあたりの文字数））

Cisco Unified Personal Communicator 8.*x* ユーザに対する 1 か月あたりのメッセージ アーカイブの最低ストレージ要件（バイト単位）は、次のように計算できます。

（ユーザ数）＊（1 時間あたりのメッセージ数）＊（1 か月あたりのビジー時間数）＊（600 +（3 ＊ 1 つのメッセージあたりの文字数））

Cisco Unified Presence のコンプライアンス設定で **Enable Outbound Message Logging** が有効な場合は、上記のメッセージ アーカイブ要件を 2 倍にする必要があります。

Cisco Unified Personal Communicator 8.*x* ユーザに対する 1 か月あたりの永続的なチャットの最低ストレージ要件（バイト単位）は、次のように計算できます。

（ユーザ数）＊（1 時間あたりの永続的なチャット メッセージ数）＊（1 か月あたりのビジー時間数）＊（700 +（3 ＊ 1 つのメッセージあたりの文字数））

（注） 永続的なチャットは XMPP クライアントでのみサポートされ、700 バイトの平均オーバーヘッドを使用します。

これらのメッセージ アーカイブ数と永続的なチャット数は、長期の平均値に基づいた最小ストレージ要件です。したがって、非常に大きい UserID、予想よりも大きいインスタント メッセージ長、およびストレージ要件を増加させる可能性がある他の要因に対応するために、1.5（150%）のバッファ係数を使用する必要があります。表 23-6 と表 23-7 は、それぞれ Cisco Unified Personal Communicator 8.*x* と 7.*x* のストレージ要件のいくつかの例を示しています。

表 23-6　Unified Personal Communicator 8.x メッセージ ロギング ストレージ要件の例

プロファイル	ユーザ数	1 時間あたりのメッセージ数	1 か月あたりのビジー時間数	メッセージの平均サイズ	メッセージ アーカイブ ストレージの要件	永続的なチャット ストレージの要件
低	1500	10	200	100	2.7 GB	3.0 GB
中	2500	15	200	250	10.2 GB	10.9 GB
高	2500	25	200	500	26.3 GB	27.5 GB

表 23-7　Unified Personal Communicator 7.x メッセージ ロギング ストレージ要件の例

プロファイル	ユーザ数	1 時間あたりのメッセージ数	1 か月あたりのビジー時間数	メッセージの平均サイズ	メッセージ アーカイブ ストレージの要件
低	1500	10	200	100	3.3 GB
中	2500	15	200	250	11.7 GB
高	2500	25	200	500	28.8 GB

Cisco Unified Presence のカレンダー統合

Cisco Unified Presence は、Microsoft Exchange 2003、2007、または 2010 とのカレンダー モジュール インターフェイスを使用してカレンダー ステータスを取得し、それをプレゼンス ステータスに集約できます。Microsoft Exchange の統合は、Microsoft Active Directory 2003 および Active Directory 2008 と Windows Server 2003 および Windows Server 2008 でサポートされます。Microsoft Exchange 2003 または 2007 では、WebDAV プロトコル（RFC 2518）の拡張に基づいて構築された Outlook Web Access（OWA）経由で、サーバからカレンダー データを取得できます。Microsoft Exchange 2007 または 2010 では、Microsoft Exchange からの要求の送信や通知の受信を可能にする Exchange Web Services（EWS）経由で、サーバからカレンダー データを取得できます。Microsoft Exchange との統合は、カレンダー アプリケーション用の別のプレゼンス ゲートウェイによって実現されます。管理者が Outlook 対応のプレゼンス ゲートウェイを設定すると、ユーザは自分のプレゼンス ステータスをカレンダー情報に集約するかどうかを切り替えられるようになります（表 23-8 を参照）。

表 23-8　カレンダー ステータスと集約されたプレゼンス ステータス

Cisco Unified Presence のステータス	カレンダー ステータス
応対可能	空き時間 / 仮承諾
アイドル / ビジー	取り込み中
退席中	不在

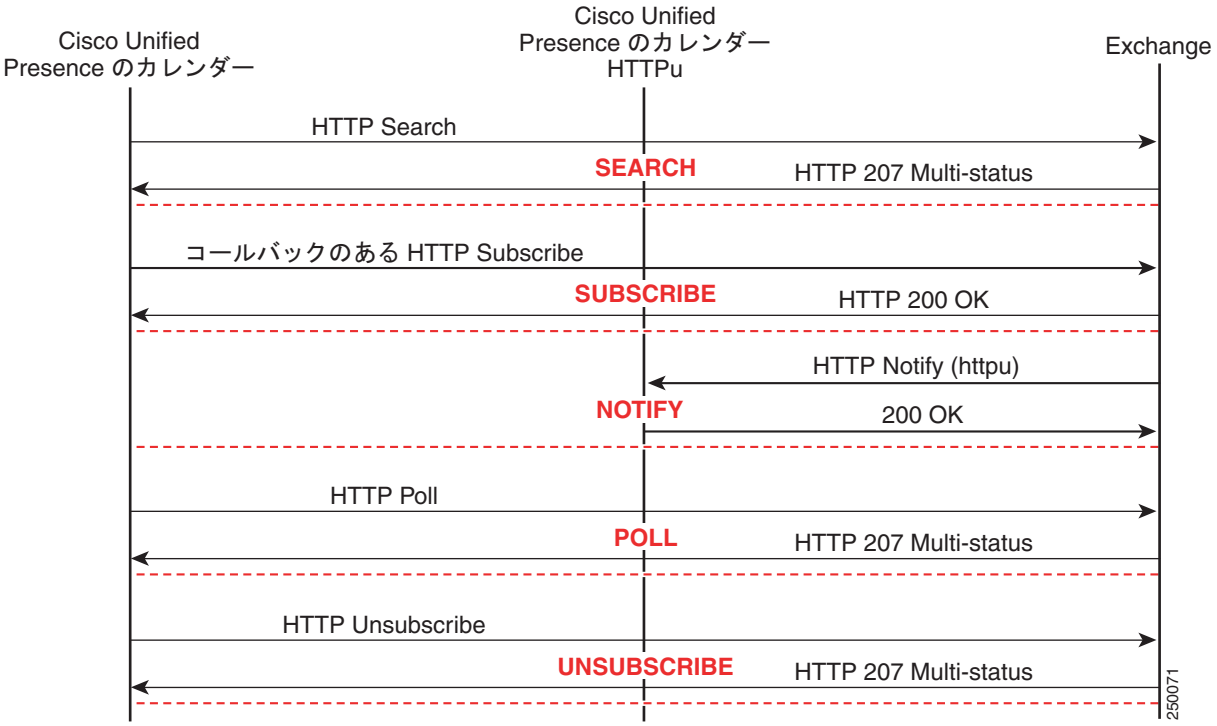
カレンダー情報の取得に使用される交換 ID は、そのユーザの LDAP 構造の電子メール ID から取得されます。電子メール ID が存在しない場合、または LDAP が使用されていない場合は、Cisco Unified Presence のユーザ ID が交換 ID としてマッピングされます。

Cisco Unified Presence サーバから Microsoft Exchange Server へのカレンダー ステータスに関するサブスクリプションによって、情報が収集されます。図 23-17 は、このやり取りを示します。

Outlook Web Access カレンダー統合

この機能には、UDP HTTP（Microsoft Exchange Notification Port）リッスン ポートのポート アドレスであるサービス パラメータが必要です。このポートは、Microsoft Exchange が、カレンダー イベントの特定のサブスクリプション識別情報に対する変更を示す通知（NOTIFY によって示される）を送信するポートです。図 23-17 を参照してください。

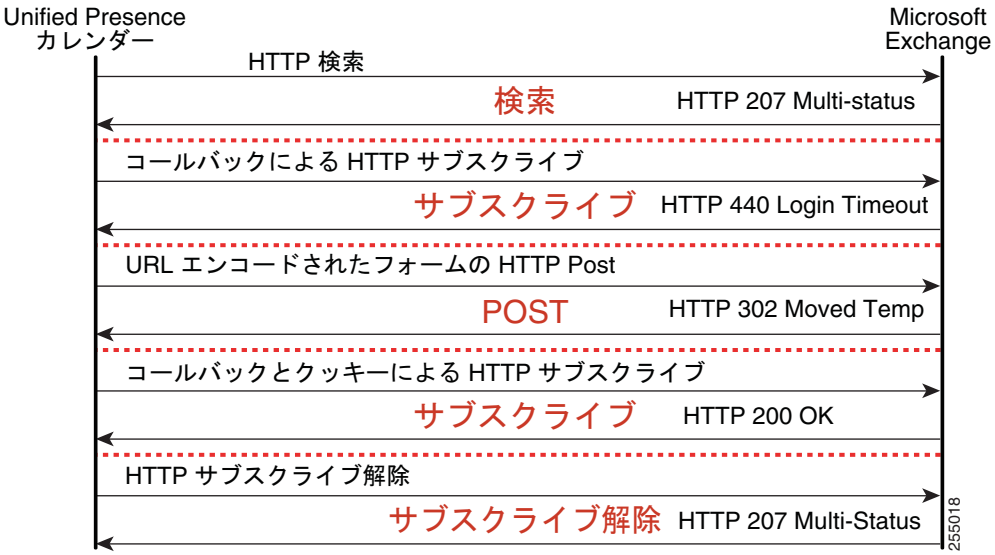
図 23-17　Cisco Unified Presence と Microsoft Exchange 間の Outlook Web Access 通信



SEARCH トランザクションは、一定の期間についてユーザのカレンダーを検索します。このトランザクションは、ユーザが、カレンダー情報をプレゼンス ステータスに含めるようにプレゼンスを設定した場合に呼び出されます。検索結果は、空き時間 / ビジー トランザクションのリストに変換されます。SUBSCRIBE メッセージは、フォルダ /exchange/user*X*/Calendar で、ユーザの空き時間 / ビジー状態に関する変更が生じた場合に通知を求めるサブスクリプションを示します。POLL メソッドは、クライアントが特定のイベントを受信したこと、またはそれに対して応答したことを確認します。UNSUBSCRIBE メッセージは、それまでの 1 つ以上のサブスクリプションを終了します。

Cisco Unified Presence Outlook Web Access 統合では、ヘッダーの一部として符号化された Exchange Server の実際の URL を含む追加の HTTP POST トランザクション要求を実行する、フォーム ベースの認証を有効にできます（図 23-18 を参照）。

図 23-18　Cisco Unified Presence カレンダーを使用したフォーム ベース認証



（注）　Cisco Unified Presence は、単一または複数の Microsoft Exchange Server とともに単一のフォレスト内にのみ配置できます。Microsoft Exchange 配置では、複数の Exchange Server で構成されるクラスタが使用できるので、Cisco Unified Presence は、Cisco Unified Presence がステータスを要求するユーザをホストしている Exchange Server への REDIRECT メッセージを受け入れます。

多言語カレンダーのサポート

カレンダー統合配置の要件で複数の言語を指定する場合は、次の設計ガイドラインに従ってください。

- Cisco Unified Presence には、Cisco Unified Communications Manager と同様に、ユーザが必要なロケールを選択できるように適切なロケールがインストールされている必要があります。
- Cisco Unified Presence は、カレンダー統合用に Unified Communications の標準ロケールをすべてサポートしています。
- エンド ユーザ用ページ、または管理用の Bulk Administration Tool によって、ユーザに目的のロケールが設定される必要があります。
- Cisco Unified Presence は、最初の照会とともに適切なロケール フォルダを送信します。照会は必要に応じて、フロントエンドまたはクライアント アクセス用 Microsoft Exchange Server の最初の応答によってリダイレクトされます。

- IP Phone Messenger および会議通知機能を使用する場合は、ユーザのロケールを、電話機の IP Phone Messenger サービスが使用されているロケールと同じに設定する必要があります。

Exchange Web Services カレンダー統合

Cisco Unified Presence では、ユーザの全体のプレゼンス ビューに集約されるカレンダー ステータス情報を Microsoft Exchange Web Services が収集することを許可するよう設定できます。ユーザ メールボックスが設定された Exchange サーバに存在する場合、Cisco Unified Presence は Exchange サーバと直接通信します。その一方で、ユーザ メールボックスが設定されたものと異なる Exchange サーバに存在する場合、Cisco Unified Presence は Exchange サーバのリダイレクションに従ってユーザ メールボックスが存在するサーバを見つけます。サーバ ファームの Exchange サーバだけが、設定された Exchange サーバとして機能できます。これらのサーバの 1 つだけをサーバ ファームから指定する必要があります。

Microsoft Exchange Web Services は、エンドユーザが使用する言語に関係なく、Exchange クライアント アクセス サーバと連携するために使用されるプロトコルを指定します。したがって、エンドユーザの言語を決定するためにロケールを使用する必要はありません。Cisco Unified Presence カレンダー統合は、単一の Microsoft Exchange フォレストでのみサポートされます。

Cisco Unified Presence Exchange Web Services カレンダー統合は、カレンダー情報のポーリング（図 23-19 を参照）とカレンダー情報のサブスクリプション/通知（図 23-20 を参照）の両方をサポートします。さまざま設定パラメータを使用して、ポーリング間隔のレート、サブスクリプション頻度、およびタイマーの耐障害性を制御します。設定の詳細については、次の Web サイトで入手可能な『*Integration Note for Configuring Cisco Unified Presence with Microsoft Exchange*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

図 23-19　Cisco Unified Presence カレンダーを使用した Exchange Web Services のポーリング

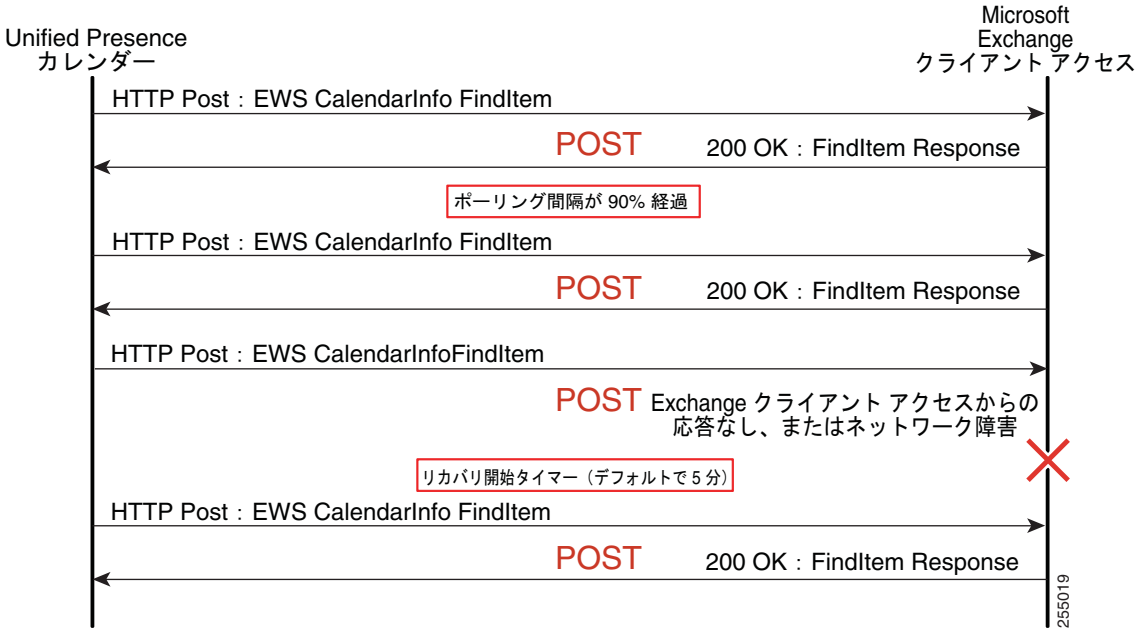
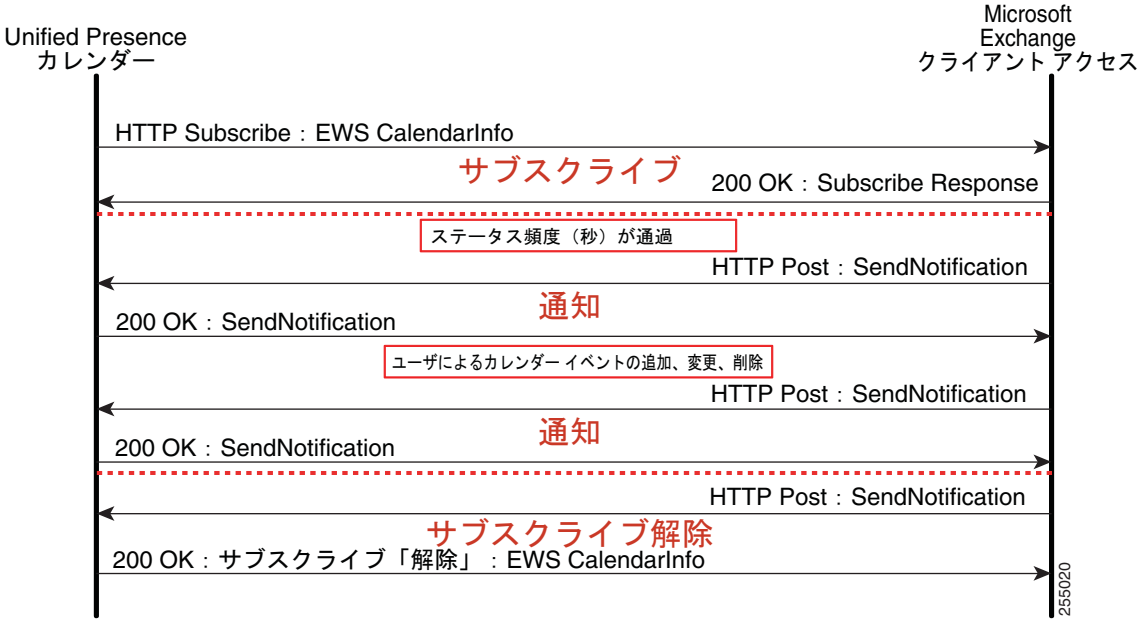


図 23-20　Cisco Unified Presence カレンダーを使用した Exchange Web Services のサブスクリプション / 通知



Client Access Server（CAS; クライアント アクセス サーバ）ロールがインストールされた各サーバに対して Service Connection Point（SCP）Active Directory オブジェクトが作成された場合は、Cisco Unified Presence で Exchange Web Services Auto Discover もサポートされます。Auto Discover では、ドメインと、ホストおよびポートの代わりにサイト（任意）を使用してカレンダー ゲートウェイが設定されます。Cisco Unified Presence は、自動検出アルゴリズムを使用して適切なクライアント アクセス サーバである Exchange Server と接続するのに使用する Exchange Web Services URL を調べます。

Cisco Unified Presence のモビリティ統合

Cisco Unified Presence は、連絡先リストとプレゼンス ステータスを Cisco Unified Mobility Advantage と Cisco Unified Mobile Communicator と統合できます。Cisco Unified Mobile Communicator は、引き続き Cisco Unified Mobility Advantage と直接通信を行いますが、Cisco Unified Mobility Advantage は、AXL/SOAP および SIP 経由で Cisco Unified Presence とやり取りします。

Cisco Unified Mobility Advantage が、Cisco Unified Presence との間で管理セッションを確立するには、その前に Cisco Unified Presence と Cisco Unified Mobility Advantage 上でアプリケーション ユーザを設定する必要があります。Cisco Unified Mobile Communicator のエンド ユーザ ログインにより、Cisco Unified Presence に対してシステム設定、ユーザ設定、連絡先リスト、プレゼンス ルール、およびアプリケーション ダイヤル ルールを求める Cisco Unified Mobility Advantage SOAP 要求が生成されます。その後、Unified Communicator Change Notifier（UCCN）設定と Presence SIP サブスクリプションが実行されます。図 23-21 は、Cisco Unified Mobility Advantage と Cisco Unified Presence の間の対話を示します。

図 23-21　Cisco Unified Mobile Communicator のコール フロー

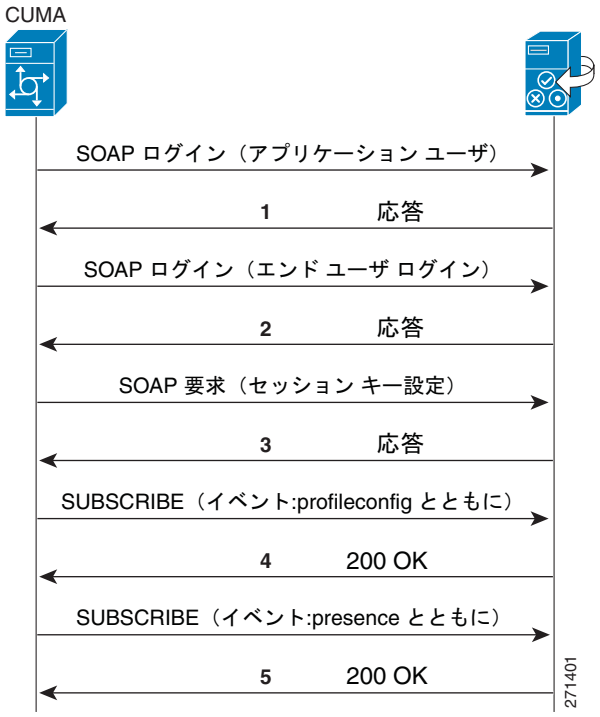


図 23-21 のコールフローは、次の一連のイベントを示しています。

1. Cisco Unified Mobility Advantage が、スーパーユーザ アプリケーション ユーザ（CCMAdministrator）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。このアプリケーション ユーザは、Cisco Unified Presence と Cisco Unified Mobility Advantage の両方で作成しておく必要があります。
2. Cisco Unified Mobile Communicator エンド ユーザがログインし、Cisco Unified Presence がセッション キーを返します。
3. Cisco Unified Mobility Advantage が、ユーザの代わりに（セッション キーを使用して）**get-all-config** SOAP 要求を開始し、システム設定、ユーザ設定、連絡先リスト、プレゼンス ルール、およびアプリケーション ダイヤル ルールを取得します。
4. Cisco Unified Mobility Advantage が、Unified Communicator Change Notifier（UCCN）サブスクリプションをユーザの **profileconfig** イベント パッケージとともに送信します。
5. Cisco Unified Mobility Advantage が、Presence サブスクリプションをユーザの **presence** イベント パッケージとともに送信します。

Cisco Unified Mobility Advantage を Cisco Unified Presence と統合する場合は、次の要件に従ってください。

- Cisco Unified Mobility Advantage は、単一の Cisco Unified Communications Manager クラスタと単一の Cisco Unified Presence クラスタに配置する必要があります。
- 1 つの Cisco Unified Mobility Advantage 配置で、1000 人を超える Cisco Unified Mobile Communicator ユーザの統合はできません。
- Cisco Unified Presence クラスタには、3 つ以上のノードを置くことはできません。

Cisco Unified Presence のサードパーティ製 Open API

Cisco Unified Presence は、SIP/SIMPLE と XMPP に加え、HTTP を介してサードパーティ製アプリケーションを統合できます。HTTP インターフェイスは、設定インターフェイスのほか、Representational State Transfer（REST）経由のプレゼンス インターフェイスを備えています。サードパーティ製の Open API は、プレゼンスへのアクセス メカニズムとして、リアルタイム イベンティング モデルとポーリング モデルの 2 つのメカニズムを持っています。

リアルタイム イベンティング モデル

リアルタイム イベンティング モデルでは、Cisco Unified Presence 上でアプリケーション ユーザを使用することにより、ユーザがそのセッション キーを使用してログインできるようになります。ユーザはログインすると、Representational State Transfer（REST）を使用してプレゼンスの更新について登録とサブスクリプションを行います。図 23-22 は、サードパーティ製の Open API のリアルタイム イベンティング モデルにおける Cisco Unified Presence との対話を示します。

図 23-22　　サードパーティ製 Open API リアルタイム イベンティング モデル

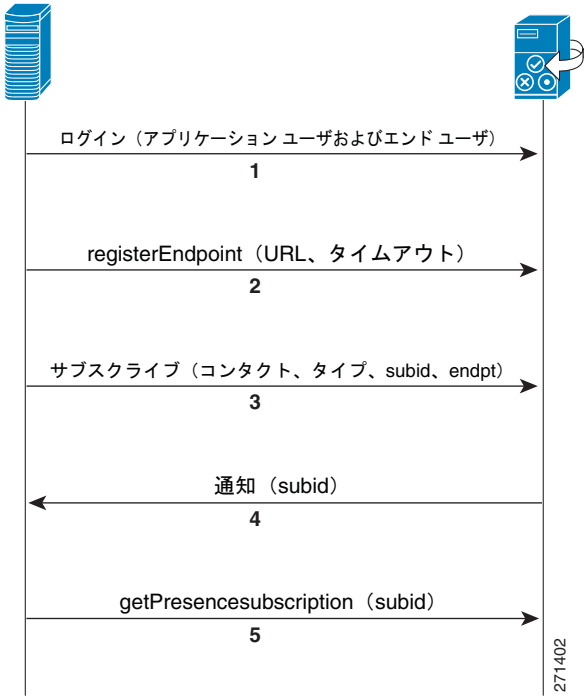


図 23-22 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンド ユーザをログインさせられるようになります（実質的には、エンド ユーザがアプリケーション経由でログインします）。
2. エンド ユーザが、アプリケーションユーザ セッション キーを使用してエンドポイントを登録します。
3. アプリケーションが、ユーザの代わりに（セッション キーを使用して）サブスクライブ要求を開始し、ユーザ情報、連絡先リスト、およびプレゼンス ルールを取得します。
4. Cisco Unified Presence が、非保護の通知を送信します。
5. アプリケーションが、ユーザのプレゼンス ステータスを要求します。

ポーリング モデル

ポーリング モデルでは、Cisco Unified Presence 上でアプリケーション ユーザを使用することにより、ユーザがそのセッション キーを使用してログインできるようになります。ユーザがログインすると、アプリケーションは、ここでも Representational State Transfer（REST）を使用して、定期的にプレゼンスの更新を要求します。図 23-23 は、サードパーティ製の Open API のポーリング モデルにおける Cisco Unified Presence との対話を示します。

図 23-23　サードパーティ製オープン API ポーリング モデル

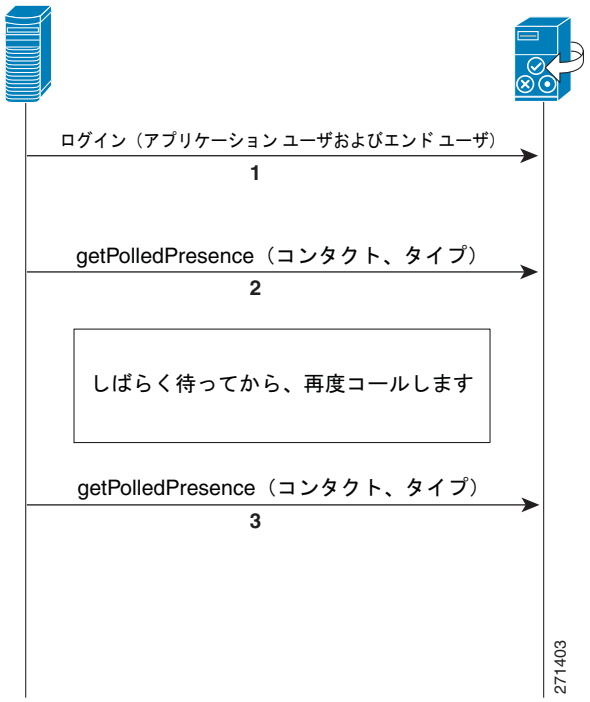


図 23-23 のコールフローは、次の一連のイベントを示しています。

1. アプリケーションが、スーパーユーザ アプリケーション ユーザ（APIUser）経由で Cisco Unified Presence に対して SOAP ログイン要求を開始し、Cisco Unified Presence がセッション キーを返します。これにより、アプリケーションはセッションキーを使用してエンド ユーザをログインさせられるようになります（実質的には、エンド ユーザがアプリケーション経由でログインします）。
2. アプリケーションがプレゼンス ステータスを要求します。イベンティング モデルは省略されます。

（注） ポーリング モデルでは、基本プレゼンスと高度なプレゼンスの両方が取得できますが、Presence サーバの負荷が大きくなります。

Extensible Messaging and Presence Protocol インターフェイス

Jabber XCP アーキテクチャでは、プレゼンス、インスタント メッセージング、および参加者管理のためのクライアント XMPP インターフェイスおよび JabberWerx AJAX インターフェイスという 2 つのオープンなインターフェイスを追加で使用できます。クライアント XMPP の機能によって、サードパーティ製の XMPP クライアントにプレゼンス、インスタント メッセージング、および参加者管理を統合できます。これは、Cisco Unified Presence における SIP/SIMPLE インターフェイスを補完するインターフェイスです。クライアント XMPP インターフェイスは、Cisco Unified Presence 内では通常の XMPP クライアントとして処理されます。そのため、インターフェイスのサイジングは、通常の XMPP クライアントとして処理する必要があります。

JabberWerx AJAX API は、Jabber XCP 機能を Web アプリケーションおよびウィジェットに統合するための Web 2.0 スタイルのインターフェイスを提供し、Cisco Unified Presence から直接利用できます。JabberWerx AJAX API は Bidirectional-streams Over Synchronous HTTP（BOSH）インターフェイスと通信するクライアント側専用の JavaScript ライブラリです。BOSH は、基本的にロングポーリング手法を使用してサーバから Web ブラウザにデータをプッシュできる XMPP over HTTP インターフェイスです。

いずれかのモデルのサードパーティ製の Open API を Cisco Unified Presence と統合する場合は、次の要件に従ってください。

- プレゼンス インターフェイスに対する証明書（sipproxy.der）と設定インターフェイスに対する証明書（tomcat_cert.der）が必要です。
- 1 つの Cisco Unified Presence 配置で、1000 人を超えるサードパーティ製の Open API ユーザの統合はできません。
- パフォーマンスの向上を図るには、サードパーティ製 Open API ユーザを Cisco Unified Presence クラスタにあるすべてのサーバに均等に振り分けてください。

Cisco Unified Presence のサードパーティ製 Open API の詳細については、次の Web サイトの Cisco Developer Services を参照してください。

http://developer.cisco.com/web/cupapi

開発者向けの情報は、Cisco Developer Community にも用意されています。次の Web サイトからログインしてアクセスしてください。

http://developer.cisco.com/

Cisco Unified Presence の設計上の考慮事項

- LDAP 統合が可能な場合、すべてのユーザ情報（番号、ID など）は、単一のソースから Unified CM との LDAP 同期を使用してプルする必要があります。ただし、LDAP server および LDAP 同期が有効でない Unified CM の両方を含む配置の場合、管理者は、ユーザのディレクトリ番号のアソシエーションの設定にあたって、Unified CM と LDAP の両方に一貫した設定を行う必要があります。
- Cisco Unified Presence は、Differentiated Services Code Point（DSCP）により、レイヤ 3 IP パケットをマーキングします。Cisco Unified Presence は、SIP プロキシの下の Differential Service Value サービス パラメータ（デフォルトは DSCP 24（PHB CS3））に基づいて、すべてのコール シグナリング トラフィックにマーキングします。
- Cisco Unified Presence のプレゼンス ポリシーは、ユーザが作成した定義されたルール セットによって、厳格に制御されます。
- Cisco Unified Presence パブリッシャとサブスクライバは、Unified CM パブリッシャと共存する必要があります。

- サービス パラメータ CUP PUBLISH Trunk を使用して、Cisco Unified Presence サーバ との SIP 通信トラフィックを簡素化します。
- Unified CM のプレゼンス ユーザは、プライマリ内線だけでなく、ライン アピアランスと関連付けます。これにより、デバイスとユーザのプレゼンス ステータスの詳細度が向上します。サービス パラメータ CUP PUBLISH Trunk を使用している場合、Unified CM 内のプレゼンス ユーザをライン アピアランスと関連付けます。
- サーバ ハードウェアとクラスタ トポロジの特性を決定する際は、プレゼンス ユーザ プロファイル（ユーザ アクティビティおよび連絡先リストの連絡先とサイズ）を考慮する必要があります。
- クラスタ全体として最高のパフォーマンスを得るには、Assignment Mode Sync Agent パラメータに、デフォルトの [balanced] を使用します。
- Cisco Unified Presence では、永続的なチャットを行う場合、クラスタ内の各サーバに外部データベース インスタンスが必要です。また、メッセージ アーカイブおよびネイティブなコンプライアンス準拠用には、クラスタごとに 1 つのデータベース インスタンスが必要です。データベース インスタンス間で同じハードウェアを共有できます。サポートされている外部データベースは、PostgreSQL だけです。
- Cisco Unified Presence では、クラスタあたり合計で 15,000 ユーザがサポートされています。ユーザのサイジングにおいては、SIP/SIMPLE ユーザの数および XMPP ユーザの数を考慮する必要があります。SIP/SIMPLE ユーザは Jabber XCP アーキテクチャへの IM ゲートウェイ機能を利用するため、XMPP ユーザの方が若干パフォーマンスがよくなります。
- バージョン 7.*x* から 8.*x* に Cisco Unified Presence の配置を移行する場合は、アップグレード前にプレゼンス エンジン サービスを非アクティブにし、すべてのサーバが 8.*x* にアップグレードされた後に再度有効化する必要があります。
- すべての eXtensible Communications Platform（XCP）通信およびロギングは GMT で実行および保管され、インストールされたロケーションに合せてローカライズされません。
- Cisco Unified Presence 8.0 は、Unified CM 6.*x*、7.*x*、および 8.*x* と互換性があります。
- Cisco Unified Communications Manager Business Edition（Unified CMBE）7.*x* 以降のリリースは、LDAP 同期をサポートしています。これは、Unified CMBE を Cisco Unified Presence と統合する場合に有効にする必要があります。

Cisco Unified Presence によって使用されるポートの完全なリストについては、次の Web サイトで入手可能な『*Port Usage Information for Cisco Unified Presence*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

サードパーティ製プレゼンス サーバ統合

Cisco Unified Presence は、SIP アプリケーションと SIMPLE アプリケーションを Cisco Unified Communications ソリューションに統合するための、SIP と SIP for Instant Messaging and Presence Leveraging Extensions（SIMPLE）に基づくインターフェイスを提供します。これにより、サードパーティ製のプレゼンス サーバやアプリケーションをこの SIP/SIMPLE と連携して設定し、統合して、プレゼンス集約やフェデレーションを提供できます。

Microsoft Communications Server

Microsoft Live Communications Server 2005 または Office Communications Server 2007、および Microsoft Office Communicator のすべてのセットアップ、設定、および配置については、次の Web サイトの資料を参照してください。

http://www.microsoft.com/

シスコは、Microsoft Communications 製品の設定、配置、またはベスト プラクティス手順は提供していませんが、Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合に関する次のガイドラインを提供しています。

シスコシステムズは、機能の相互運用性と、Cisco Unified Presence を Microsoft Live Communications Server 2005 に統合するための設定手順を示すアプリケーション ノートを作成しました。アプリケーション ノートは、次の Web サイトで入手できます。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/602270nt.pdf

シスコシステムズはまた、機能の相互運用性と、Cisco Unified Presence を Microsoft Office Communications Server 2007 に統合するための設定手順を示すアプリケーション ノートを作成しました。アプリケーション ノートは、次の Web サイトで入手できます。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/pbx/interop/notes/617030nt.pdf

http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns728/ns784/712410.pdf

シスコシステムズはまた、Cisco Unified Presence を Microsoft Office Communications Server 2007 に統合するためのガイドを作成しました。この『*Integration Note for Configuring Cisco Unified Presence with Microsoft LCS/OCS for MOC Call Control*』は、次の Web サイトで入手可能です。

http://www.cisco.com/en/US/products/ps6837/products_installation_and_configuration_guides_list.html

Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 との統合のためのガイドライン

次のガイドラインは、Cisco Unified Presence サーバを Microsoft Live Communications Server 2005 または Office Communications Server 2007 に統合する場合に適用されます。

- Cisco Unified Presence と Microsoft Live Communications Server 2005 または Office Communications Server 2007 の間の通信には、SIP/SIMPLE インターフェイスが使用されます。ただし、Microsoft Live Communications Server 2005 または Office Communications Server 2007 は、SIP 経由の Computer-Supported Telecommunications Applications（CSTA）トラフィックをトンネルします。したがって、Cisco Unified Presence サーバ上の CTI ゲートウェイは、Click to Call の電話制御のために CSTA-CTI 変換を処理するように設定する必要があります。
- リモート通話コントロール対応の Microsoft Office Communications Server 2007 または Live Communications Server 2005 と共に配置する Cisco Unified Presence は、1 対のサーバを持つ単一のサブクラスタから成る Cisco Unified Presence クラスタで構成する必要があります。

- 次の表では、プラットフォームごとのサポートされるユーザ数を示します。

Cisco Unified Presence のプラットフォーム	Cisco Unified Communications Manager のプラットフォーム	サーバごとのサポートされるユーザ数[1]	Microsoft Office Communicator のクラスタごとのサポートされるユーザ数[1]
MCS 7825、7835、または 7845	MCS 7825	900	3,600
MCS 7825、7835、または 7845	MCS 7835	2,000	8,000
MCS 7825、7835、または 7845	MCS 7845	5,000	20,000

1. これらの数は、Cisco Unified CM 7.1(3) 以降のリリースに基づいています。

- エンド ユーザ ID は、LDAP、Unified CM、および Microsoft Live Communications Server 2005 または Office Communications Server 2007 で同一に設定する必要があります。これにより、Microsoft Live Communications Server 2005 または Office Communications Server 2007 の Active Directory（AD）での認証や Unified CM のエンド ユーザ設定との競合、さらには Unified CM 上でのユーザの電話機の制御との競合を防止できます。

  Active Directory については、General、Account、および Live Communications のユーザのプロパティですべて同一の ID を使用することを推奨します。Cisco Unified Presence の全ユーザの一貫性を維持するために、Unified CM で LDAP 同期と LDAP 認証を有効にする必要があります。
- Microsoft Live Communications Server 2005 または Office Communications Server 2007 のホスト認証に Cisco Unified Presence のパブリッシャとサブスクライバを含める必要があります。
- Live Communications Server 2005 または Office Communications Server 2007 のプロパティの設定で、SIP メッセージが静的 IP アドレスによって Cisco Unified Presence にルーティングされるように設定する必要があります。
- Cisco Unified Presence サーバの発着信のアクセス コントロール リスト（ACL）で、Microsoft Live Communications Server 2005 または Office Communications Server 2007 との通信を許可する必要があります。
- Unified CM で各ユーザのプレゼンスを有効にするだけでなく、Cisco Unified Presence サーバ設定で、各ユーザに Microsoft Office Communicator の使用を許可する必要があります。
- Microsoft Office Communicator のログイン時に、Microsoft Office Communicator と Microsoft Communications Server 間での設定情報の交換や、Cisco Unified Presence サーバ CTI ゲートウェイとの初期通信のために必要となる帯域幅を考慮に入れる必要があります。
- Microsoft Office Communications Server 2007 では、必要なパラメータの名前が Live Communications Server 2005 から変更されています。Live Communications Server 2005 で定義されている TEL URI パラメータは、Office Communications Server 2007 の Line URI と同じです。また Live Communications Server 2005 の Remote Call Control SIP URI パラメータは、Office Communications Server 2007 の Server URI と同じです。
- ディレクトリ番号からそれに対応するユーザを検索するリバース ルックアップの問題に対処するには、次の Web サイトで入手可能な『*Release Notes for Cisco Unified Presence*』のガイドラインの資料を使用してください。

  http://www.cisco.com/en/US/products/ps6837/prod_release_notes_list.html

IBM Lotus Sametime

シスコ システムズでは、IBM Lotus Sametime Server と Cisco Unified Communications の最適な統合のための次のガイドラインを提供していますが、IBM Communications 製品の設定、配置、またはベスト プラクティス手順を強く推奨しているわけではありません。

IBM Lotus Sametime Server のセットアップ、設定、および配置についてのすべての情報は、次の Web サイトを参照してください。

http://www.ibm.com/

シスコは、IBM Communications 製品に関する設定、配置、またはベスト プラクティス手順は提供していませんが、IBM Lotus Sametime Server と Cisco Unified Communications システムの統合に関して次のガイドラインを提供しています。

Cisco Unified Presence と IBM Lotus Sametime Server（バージョン 7.5.1 以降）の統合のためのガイドライン

IBM Lotus Sametime クライアント内に統合されたクリックツーコールおよびクリックツー会議機能は、IBM Lotus Sametime Server 上に存在する Cisco Call Control プラグイン経由で処理されます。クリックツーコールおよびクリックツー会議機能のための Cisco Unified Communications との統合は、Unified CM との SIP トランク インターフェイス経由で処理されます。プレゼンス機能のための Cisco Unified Communications との統合は、Cisco Unified Presence との SIP/SIMPLE インターフェイス経由で処理されます。

- クリックツーコールおよびクリックツー会議機能のための Unified CM SIP トランクの Out-Of-Dialog Refer（OOD-Refer）処理ができるように設定する必要があります。IBM Lotus Sametime Server と通信する SIP トランクの [SIP Trunk Security Profile] で、[Accept Out-of-dialog REFER] チェックボックスをオンにします。
- IBM Lotus Sametime Server に存在する Cisco Call Control プラグインは、ラウンドロビン方式で使用される Unified CM の設定済みリストを保持します。このリストには、アウトオブダイアログ REFER SIP トランクで設定した Unified CM サブスクライバの IP アドレスが含まれています。

  Unified CM のリストは、DNS SRV でも設定できますが、この SRV ロジックは、冗長性のみに使用されロード バランシングには使用されないので、この設定は推奨できません。
- IBM Lotus Sametime Server を使用した配置トポロジは、これら 2 つのシステムの容量の違いから、通常、複数の Unified CM クラスタと統合されます。Unified CM のリストをラウンドロビン方式で使用するシスコのクリックツーコール プラグインを利用すると、ユーザのホーム クラスタとは異なるクラスタに、REFER が送信されることがあります。Unified CM は、このコール設定を受信すると、REFER を処理し、適切な宛先に対して、このコール設定を完了させる INVITE を生成します。
- Cisco Call Control プラグインでは、トラフィック マーキングが完全に実装されていません。次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

  http://www.cisco.com/go/designzone

サーバ間の観点から見ると、Cisco Unified Presence 8.0 は IBM Lotus Sametime 8 と XMPP インターフェイスで統合され、IBM Lotus Sametime クライアントと Cisco Unified Presence クライアントとの間のドメイン間フェデレーションが可能となります。

CHAPTER 24

Cisco Collaboration クライアントおよびアプリケーション

（注） この章は、このマニュアルの現在のリリースに向けて大幅に改訂されました。コラボレーション クライアントとアプリケーションをお使いの Cisco Unified Communications システムに配置する前に、この章全体に目を通しておくことを推奨します。

Cisco Collaboration クライアントおよびアプリケーションは統合的なユーザ エクスペリエンスを実現し、Cisco Unified Communications システムの機能と操作性を拡張します。これらのクライアントおよびアプリケーションは、オンライン会議、プレゼンス通知、インスタント メッセージング、オーディオ、ビデオ、ボイスメールなど、多数のアプリケーションを使い勝手のよい 1 つのコラボレーション クライアントに統合することにより、企業境界内外のコラボレーションを可能にします。

複数のコラボレーション クライアントおよびアプリケーションを使用でき、Cisco Unified Communications システムに統合する場合のアーキテクチャ ビュー、配置に関する考慮事項、プランニング、および設計ガイドラインがそれぞれに用意されています。この章を使用して、どのコラボレーション クライアントおよびアプリケーションが配置に最も適しているかを確認してください。

- Cisco Unified Personal Communicator

  Cisco Unified Personal Communicator は、デスクトップ（PC または Mac）上のリッチ メディア インターフェイスから音声、ビデオ、Web 会議、インスタント メッセージング、ボイスメール、およびプレゼンス情報への容易なアクセスを可能にするユーザ向けのデスクトップ アプリケーションです。Cisco Unified Personal Communicator の利用によって、チーム間の生産性は高まり、ナレッジ ワーカーは便利なユーザ インターフェイスを通じていつでもどこでも簡単にコラボレートし、通信をエスカレーションすることが可能になります。詳細については、「Cisco Unified Presence」（P.23-1）の章を参照してください。

- Cisco WebEx Connect

  Cisco WebEx Connect は、コラボレーティブな Software-as-a-Service（SaaS）型プラットフォームであり、開発者、パートナー、およびカスタマーはこれを利用して、コラボレーティブ ソリューションを経由した到達可能範囲を拡大できる強力なコラボレーティブ ビジネス ソリューションを作成できます。Cisco WebEx Connect は、企業クラスのセキュリティ、スケーラビリティ、パフォーマンス、および可用性を強制的に確立するとともに、Cisco Unified Communications ソリューションとの透過的な通信を可能にするための、拡張可能なオープン型コラボレーション プラットフォームを実現します。Cisco WebEx Connect には、Cisco WebEx Connect Client と Cisco WebEx Connect Platform の 2 つの主要コンポーネントがあります。

- Cisco UC Integration™ for Microsoft Lync

  Cisco UC Integration™ for Microsoft Lync は、一貫したユーザ エクスペリエンスを保ちつつ、Cisco Unified Client Services Framework を使用して Cisco Unified Communications の Microsoft Lync との統合を可能にします。このソリューションは、標準ベースの音声とビデオ、ユニファイド メッセージング、Web 会議、デスクトップ制御、テレフォニー プレゼンスなどの幅広い一連の Cisco Unified Communications サービスへのアクセスを提供することにより、Microsoft Lync のプレゼンスとインスタント メッセージングの機能を拡張します。

- Cisco Unified Mobile Communicator

  Cisco Unified Mobile Communicator は、携帯電話から Cisco Unified Communications アプリケーションにアクセスし、利用する機能をユーザに提供するモビリティ ソリューションです。Cisco Unified Mobile Communicator および Cisco Mobile グラフィカル クライアントは、Cisco Unified Mobility Advantage ソフトウェアを実行しているサーバと連動して、携帯電話の機能にアクセスし、制御するためのリッチ ユーザ インターフェイスを提供します。このシステムは既存の社内 LDAP ディレクトリに統合されるため、ユーザはすべてのデバイス上で単一のクレデンシャル セットを使用できます。詳細については、「モバイル ユニファイド コミュニケーション」（P.25-1）の章を参照してください。

- サードパーティ製の XMPP クライアントおよびアプリケーション

  Cisco Unified Presence では SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）がサポートされているため、サードパーティ製のクライアントおよびアプリケーションで、プレゼンスおよびインスタント メッセージングの更新を複数のクライアント間で通信することがサポートされています。サードパーティ製の XMPP クライアント、MomentIM、Adium、Spark、Pidgin などでは、さまざまなデスクトップ オペレーティング システム間での拡張された相互運用性を利用できます。また、Web ベースのアプリケーションは、SOAP、REST、または BOSH（JabberWerx AJAX API に基づく）を使用する HTTP インターフェイスを使用して、プレゼンスの更新、インスタント メッセージング、および参加者リストの更新を取得できます。サードパーティ製のオープン インターフェイスの詳細については、「Cisco Unified Presence」（P.23-1）を参照してください。

この章の新規情報

表 24-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 24-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco Unified Personal Communicator のハイ アベイラビリティ	「Cisco Unified Personal Communicator のハイ アベイラビリティ」（P.24-13）	2011 年 1 月 31 日
Microsoft Office Communicator の名前が Microsoft Lync に変更	この章の各項で説明	2011 年 1 月 31 日

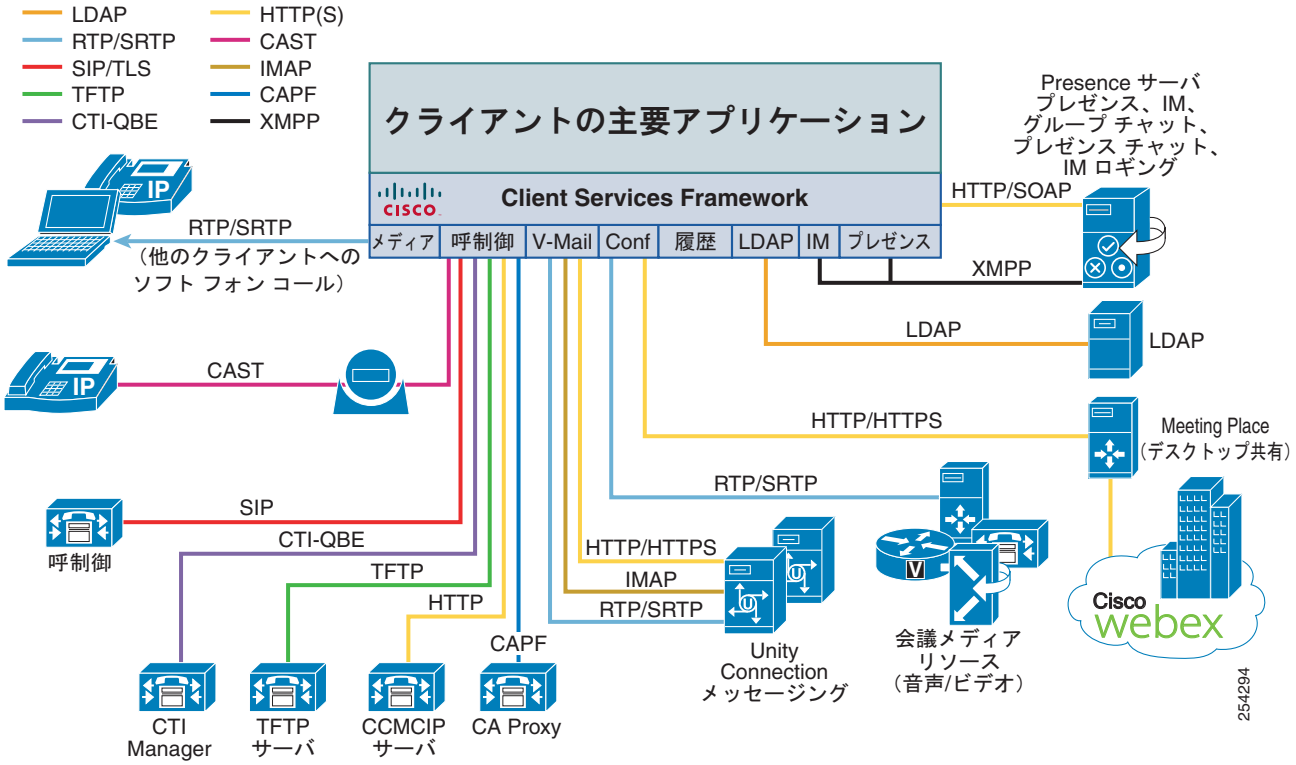
Cisco Unified Client Services Framework のアーキテクチャ

Cisco Unified Personal Communicator、Cisco WebEx Connect、および Cisco UC Integration™ for Microsoft Lync はすべて、クライアント アプリケーションの基本構築ブロックとして Client Services Framework を使用します。Cisco Unified Client Services Framework は、多数のサービスを統合クライアントと組み合せるソフトウェア アプリケーションです。音声、ビデオ、Web コラボレーション、ビジュアル ボイスメールなどの Unified Communications サービスをプレゼンスおよびインスタント メッセージング アプリケーションに統合するために、基礎となるフレームワークが提供されます。

ユーザは Cisco Unified Communications Manager（Unified CM）、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、および Lightweight Directory Access Protocol（LDAP）バージョン 3（v3）サーバにインターフェイスするさまざまな通信サーバにアクセスできます。Client Services Framework（図 24-1 を参照）は、Microsoft Lync、Cisco WebEx Connect、Cisco Unified Personal Communicator などのさまざまなデスクトップ クライアントへの統合も可能にします。

通信機能およびサービスと API を抽象化する機能（図 24-1 を参照）は、プロトコルの管理をこれらのサービスおよび API に対して調整し、イベント通知を処理し、ローカル システム リソースのための低水準の接続ロジックを制御することを可能にします。

図 24-1　Cisco Unified Client Services Framework



コンタクト管理

Client Services Framework は、ソースの階層構造を通じて、コンタクトの管理を処理します。これには、ディレクトリ統合、LDAP と LDAPS のサポート（カスタマイズ可能な属性テーブルが設定されている必要があります）、Client Services Framework キャッシュ、Local Address Book コンタクトなどが含まれます。Client Services Framework のコンタクト管理では、LDAP 照会用に最大 5 つの検索ベースを定義することができ、それがフォト取得に加えて、着信電話番号のコンタクトへのマッピングのために逆番号ルックアップを処理します。

ディレクトリ

LDAP ディレクトリの Client Services Framework との統合により、属性のマッピングと管理するコンタクトの設定が中央のディレクトリの場所から行えるようになりました。一般的なほとんどのディレクトリ属性マッピングを表 24-2 にリストします。

表 24-2　ディレクトリ属性マッピング

Client Services Framework での名前	LDAP ディレクトリでの属性
businessPhone	telephoneNumber
commonName	cn
companyName	company
displayName	displayName
email	mail
firstName	givenName
homePhone	homePhone
lastName	sn
mobilePhone	mobile
objectclassKey	objectclass
objectclassValue	person
otherPhone	otherTelephone
photoUri	photoUri
title	title
uri	msRTCSIP-PrimaryUserAddress
userAccountName	sAMAccountName / uid
userLogonName	userPrincipalName / uid

Client Services Framework のキャッシュ

Client Services Framework は、ローカルのアドレス帳だけでなく、前のディレクトリ照会から派生したコンタクト情報およびすでにリストされているコンタクトのローカル キャッシュを保持しています。

ディレクトリ検索

ローカル Client Services Framework キャッシュ内にコンタクトが見つからない場合は、LDAP または LDAPS を通じて、コンタクト情報のディレクトリ検索を行えます。Client Services Framework では、コンタクト情報が入力されるとともにローカル キャッシュを照会する予測検索が使用されます。一致

するデータがローカルに見つからなかった場合は、ユーザは、ディレクトリ検索オプションを使用できます。これは、cn、sn、uid、および givenName で一致するものを探す searchRequest を形成し、設定されている LDAP プロファイルに基づいて LDAP サーバに要求を送信できます。要求に一致したすべての結果が返され、リストされます。

呼制御

Cisco Unified Client Services Framework は、ソフトフォン モード（コンピュータ上の音声）またはデスクフォン制御モード（音声にデスクフォンを使用）の 2 つのモードで稼動できます。ソフトフォン モード（コンピュータ上の音声）の Client Services Framework は、音声とビデオの呼制御機能のために SIP エンドポイントとして直接 Unified CM に登録され、Unified CM 上で新しいデバイス タイプ、Client Services Framework として設定されます。デスクフォン制御モード（音声にデスクフォンを使用）の Client Services Framework は、Cisco Unified IP Phone を制御する一方で、CTI/JTAPI を使用してコールの開始、モニタ、終了、回線状態のモニタ、およびコール履歴の提供を行います。Client Services Framework がデバイスに関連付けられているユーザを発見するのに、Unified CM 上の CCMCIP が使用されます。

ソフトフォン モード（コンピュータ上の音声）

Client Services Framework は、ソフトフォン モード（コンピュータ上の音声）で稼動しているときには、Unified CM 上の SIP 回線側登録デバイスで、登録の設定、冗長性、リージョン、ロケーション、ダイヤル プラン管理、認証、暗号化、ユーザの関連付けなど、すべての呼制御機能と Cisco Unified IP Phone の機能を使用します。Client Services Framework は、ユーザに対して単一のライン アピアランスをサポートします。

Unified CM クラスタのサイジングの計算では、Client Services Framework の SIP 登録デバイスは、その他のあらゆる SIP 登録エンドポイントと同じく、正規の SIP エンドポイントとして考慮しなければなりません。

デスクフォン制御モード（音声にデスクフォンを使用）

デスクフォン制御モード（音声にデスクフォンを使用）で稼動しているときには、Client Services Framework は、CTI/JTAPI を使用して、Cisco Unified IP Phone を使用したコールの発信、モニタ、および受信の機能を提供します。このモードでコールが受信または発信されると、音声パスが Cisco Unified IP Phone を通過します。Client Services Framework は、Unified CM 上の CCMCIP サービスを使用して、ユーザの関連付けられているデバイスを発見します。ビデオを使用する場合、Client Services Framework と制御対象になっている Unified IP Phone が、Cisco Discovery Protocol（CDP）を使用してお互いを発見し、Cisco Audio Session Tunnel（CAST）を使用してビデオ コールのセットアップと管理を行います。Client Services Framework に使用される PC は、32 ビット オペレーティング システムでなければならず、物理的に Unified IP Phone の PC ポートに接続されていなければなりません。そして、Unified IP Phone のその PC ポートが有効になっていなければなりません。

Client Services Framework のデスクフォン制御モードを使用する場合は、CTI 規模の値を Unified CM 配置計算に組み入れてください。キャパシティ プランニングの詳細については、「コール処理」（P.8-1）を参照してください。

メディア

Client Services Framework では、低帯域幅の配置や忠実度の高い配置で使用するための標準音声 / ビデオ コーデックが多数サポートされています。音声コーデックには、G.729a、iLBC、G.711、G.722、および iSAC が含まれ、ビデオ コーデックには、H.264 ベースライン プロファイル レベル 1 ～ 3.1 のサポートを備えた H.264 AVC（Advanced Video Coding）が含まれます。サポートされるビデオ形式には、最大 30 フレーム / 秒のフレーム速度での QCIF、CIF、VGA、および 720p HD が含まれます。

Client Services Framework は、常に高品位ビデオを送受信しようとしますが、ビデオを配置する際には、考慮する必要のある多数の調整要素があります。この調整上の考慮事項には、通信相手となるデバイスのキャパシティ、PC のローカル処理能力、管理者またはユーザの設定、ローカル カメラの性能、および施行されているあらゆるコール アドミッション制御ポリシーが含まれます。

Client Services Framework がコールに使用するビデオ フレーム レートの決定に使用する決定ポイントは多数あります。重要な決定ポイントの 1 つは、使用される PC の Windows Experience Index（WEI）に基づきます（http://technet.microsoft.com/en-us/library/cc507870.aspx）。高解像度ビデオのエンコーディングとデコーディングに関する最小値として、5.9 のプロセッサ WEI エンコード値と毎秒 15 フレームで 720p の場合の 1 Mbps または毎秒 30 フレームで 720p の場合の 2 Mbps という帯域幅要件が必要です。H.264 レベルおよび WEI エンコード / デコード値に基づいたその他のビデオ フレーム レートのリストを見るには、次のアプリケーション リリース ノートを参照してください。

- Cisco Unified Personal Communicator リリース ノート
  http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- Cisco UC Integration™ for Microsoft Lync リリース ノート
  http://www.cisco.com/en/US/products/ps10317/prod_release_notes_list.html

ビデオの受信レベルは、Client Services Framework 内でビデオ設定を手動で調整することによって、または管理制御あるいはユーザ制御のいずれかによって制御できます。動作のモードと対応する H.264 レベルを手動で調整できる機能は、ビデオ ストリーム レートと Windows Experience Index の調整を可能にします。この調整上の考慮事項には、Client Services Framework と通信するデバイスのキャパシティ、PC のローカル処理能力、管理者またはユーザの設定、ローカル カメラの性能、および施行されているあらゆるコール アドミッション制御ポリシーが含まれます。Windows Experience Index とビデオ解像度の関係については、アプリケーション リリース ノートを参照してください。

Client Services Framework からの音声 / ビデオ コールの帯域幅利用率は、Unified CM リージョンおよびロケーション コール アドミッション制御メカニズムを使用して維持できます。管理上、Client Services Framework を 1 つのリージョンのデバイス プールに入れると、ネットワーク帯域幅が重要なシナリオで、帯域幅利用率を制御する機能が得られます。Unified CM リージョン コール アドミッション制御によって、使用できるコーデックを指定できるようになるだけでなく、コールごとのリージョン間およびリージョン内の帯域幅を指定することもできるようになります。Unified CM ロケーション コール アドミッション制御は、ロケーション間の音声およびビデオの帯域幅制御、または RSVP の使用を提供します。Client Services Framework には、コールの音声部分とビデオ部分の両方をカバーするのに十分な Unified CM リージョンが必要です。たとえば、フレーム サイズが 720p でフレーム レートが毎秒 30 フレームのビデオ コールを発信するには、ビデオ専用の 2,000 kbps のシグナリング ビット レートが必要です。したがって、1 回のコール用のリージョン帯域幅には、64 kbps（G.711 または G.722 コーデックを想定した場合）の音声部分だけでなく、2,000 kbps（30 fps で 720p を想定した場合）のビデオ部分を含める必要があります。Unified CM でのリージョンおよびロケーション コール アドミッション制御のサポートの詳細については、「コール処理」（P.8-1）の章を参照してください。

Client Service Framework のシグナリングおよびメディア トラフィックは、音声とビデオの両方で、配置の柔軟性と制御を上げられるように、Differentiated Services Code Point（DSCP）によってマークされます。Client Services Framework は、すべてのシグナリングを CS3 の分類でマークします。音声専用のコールに関連付けられるメディアは、EF でマークされ、ビデオ コールは、音声とビデオ両方に AF41 という DSCP 値でマークされます。ただし、オペレーティング システムはこれらのマーキングを必ずしも利用するとは限らず、したがって PC からのトラフィックが信頼できないものになる場合もあります。詳細については、「ソフトウェアベースのエンドポイント」（P.18-41）の QoS 上の推奨事項を参照してください。

ダイヤル プラン

Client Services Framework を任意の Unified Communications エンドポイント戦略の一部として配置する際には、ダイヤル プランと番号の正規化に関する考慮事項を念頭に置いて作業してください。Unified Communications コラボレーション クライアントの一部としての Client Services Framework は、一般に、コンタクトの検索、解決、および追加にディレクトリを使用します。これらのコンタクトに関連付けられている番号は、クライアントが認識し、解決し、ダイヤルできる形式になっていなければなりません。

配置は、ディレクトリおよび Unified CM の設定によって変わってくる場合があります。ビジネス、モバイル、および家庭の電話番号用に E.164 の番号指定（たとえば +18005551212）がディレクトリに含まれており、Unified CM にも E.164 ダイヤル プラン（Unified CM 7.*x* 以降のリリース）が含まれている場合は、すべてのルックアップ、解決、およびダイヤルされたイベントが E.164 形式のダイヤル ストリングになるため、追加のダイヤル規則の必要性が最小化されます。

Unified CM の配置でプライベート ダイヤル プラン（51212 など）を実装している場合は、Unified CM 上で E.164 番号のプライベート ディレクトリ番号への変換の必要が生じます。発信コールは、アプリケーションのダイヤル規則によって変換されます。これによって、ダイヤルする番号の +18005551212 をプライベート番号の 51212 としてエンドポイントに表示できます。着信コールは、ディレクトリのルックアップ規則によって変換されます。これにより、着信した番号の 51212 が、逆番号ルックアップ発信者 ID に +18005551212 で示されます。

プライベートな番号プラン配置が生じる場合があり、その場合、会社のダイヤル プランと LDAP ディレクトリに保存されている電話番号情報によっては、Cisco Unified Communications Manager 上でアプリケーション ダイヤリング規則とディレクトリ ルックアップ規則を定義する必要が生じます。これらの規則は、ディレクトリ ルックアップ キーとして使用される着信コール ID を再形式化する方法、および LDAP ディレクトリから取得した電話番号を発信ダイヤリング用に変換する方法を定義します。

アプリケーション ダイヤリング規則

アプリケーション ダイヤリング規則は、ダイヤルされた番号を操作したり、ユーザがダイヤルする電話番号から番号を自動的に取り去ったり、あるいは追加したりするのに使用されます。Cisco Unified CM 7.*x* 以降のリリースでは、ダイヤルされる番号にプラス（+）文字を含む規則がサポートされています。7.*x* よりも前のリリースの Unified CM では、プラス文字はサポートされていませんでした。アプリケーション ダイヤル規則は、Unified CM 上で設定され、TFTP を介して Unified CM からクライアントにダウンロードされます。

ディレクトリ ルックアップ規則

ディレクトリ ルックアップ規則は、発信者 ID 番号をディレクトリで検索できる番号に変換します。そして、1 つの規則で、どの番号を変換するかを番号の最初の桁と長さに基づいて指定します。ディレクトリ ルックアップ規則は、Unified CM 上で設定され、TFTP を介して Unified CM からクライアントにダウンロードされます。

トランスレーション パターン

トランスレーション パターンは、コールがルーティングされる前にダイヤルされた桁を操作するために、Unified CM によって使用されます。これらは、Unified CM によって厳密に処理されます。Unified CM 7.*x* 以降のリリースを使用している場合は、Client Services Framework 配置での番号解決の柔軟性を上げるために、アプリケーション ダイヤリング規則ではなくトランスレーション パターンを使用することを推奨します。

トランスレーション パターンの使用方法およびダイヤル プラン管理に関するその他のガイドラインについては、「ダイヤル プラン」（P.9-1）の章を参照してください。

クライアント変換

コンタクト情報を通じてコールが発信される前に、クライアント アプリケーションがダイヤルされる電話番号から文字と数字以外のすべてのものを取り除きます。アプリケーションは、文字を数字に変換し、ダイヤリング規則を適用します。文字と数字のマッピングは、ロケール固有で、その場所の標準的な電話機のキーパッドにある文字に対応します。たとえば、US English ロケールでは、1-800-4UCSRND は 18004827763 に変換されます。コールがアプリケーションによって発信される前に、ユーザがクライアントの変換された番号を見たり変更したりすることはできません。

Client Services Framework の配置

Client Services Framework は、デスクトップ クライアントの統合と通信の基本構築ブロックであるため、これらのデバイスは多数のユーザに配置する必要があります。Client Services Framework の配置のための Bulk Administration Tool を使用することを推奨します。管理者は、デバイス プール、デバイス セキュリティ プロファイル、および電話のボタンの電話テンプレートを作成し、デバイス名をディレクトリ番号にマッピングするための CSV データ ファイルを作成できます。管理者は、有効になっていれば、ユーザのグループと CTI を含んだユーザ テンプレート、およびユーザを適切な制御対象デバイスにマッピングする CSV データ ファイルも作成できます。

Client Services Framework のキャパシティ プランニング

Cisco Unified Client Services Framework は、Unified CM に対する SIP 登録エンドポイントとして、または Unified CM に対する CTI を使用する Unified IP Phone のデスクフォン コントローラとして機能します。Client Services Framework を使用した配置を計画する際には、シスコのパートナーやスタッフが Cisco Unified Communications Sizing Tool（http://tools.cisco.com/cucst から入手可能）を使用して、SIP 登録エンドポイントまたは CTI 制御デバイスの適切なサイジングのお手伝いをします。Client Services Framework の配置では、さらに次の項目について考慮する必要があります。

- TFTP：ソフトフォン（コンピュータ上の音声）モードで設定した場合は、Unified CM 呼制御の設定情報のために、Client Services Framework のデバイス設定ファイルがクライアントにダウンロードされます。さらに、アプリケーション ダイヤル規則やディレクトリ ルックアップ規則があれば、それらも TFTP を介してダウンロードされます。
- CTI：デスクフォン（音声にデスクフォンを使用）で設定した場合は、IP 電話の制御を可能にするために、ログインと登録の際に Client Services Framework が Unified CM への CTI 接続を確立します。
- CCMCIP：Client Services Framework は、制御に使用できる IP 電話をリストするために、Unified CM IP Phone サービスを使用して、ユーザに関連付けられているデバイスに関する情報を収集します。
- IMAP：ボイスメール用に設定されている場合、Client Services Framework は、メールストアとの IMAP 接続を通じてボイスメールを更新および取得します。
- LDAP：クライアントのログインと認証、コンタクト プロファイル情報、および着信したコールの発信者 ID のすべてが、ローカル Client Services Framework キャッシュに保存されていない限り、LDAP 照会を通じて処理されます。

統合 Extension Mobility および Unified CM Assistant アプリケーションの IP Phone サービスを除き、IP Phone サービスは独立した Web サーバに存在する必要があります。Cisco Unified CM サーバで Extension Mobility および Unified CM Assistant 以外の電話サービスを実行することはサポートされていません。

Client Services Framework のハイ アベイラビリティ

Cisco Unified Client Services Framework は、TFTP Server、CTI Manager、CCMCIP Server、Voicemail Server、LDAP Server といった設定コンポーネントのそれぞれにプライマリ サーバとセカンダリ サーバを提供します。ソフトフォン（コンピュータ上の音声）モードで稼動しているときには、Client Services Framework は、Cisco Unified CM での SIP 登録エンドポイントであり、Unified CM の登録エンドポイントのすべての登録機能および冗長機能をサポートします。デスクフォン モードで稼動しているときには、Client Services Framework は、CTI を使用して Cisco Unified IP Phone を制御し、プライマリおよびセカンダリ CTI Manager の設定をサポートします。CTI 配置の詳細については、「コール処理」（P.8-1）の章を参照してください。

Client Services Framework の設計上の考慮事項

Cisco Unified Client Services Framework を配置する際には、設計上の次の考慮事項を知っておいてください。

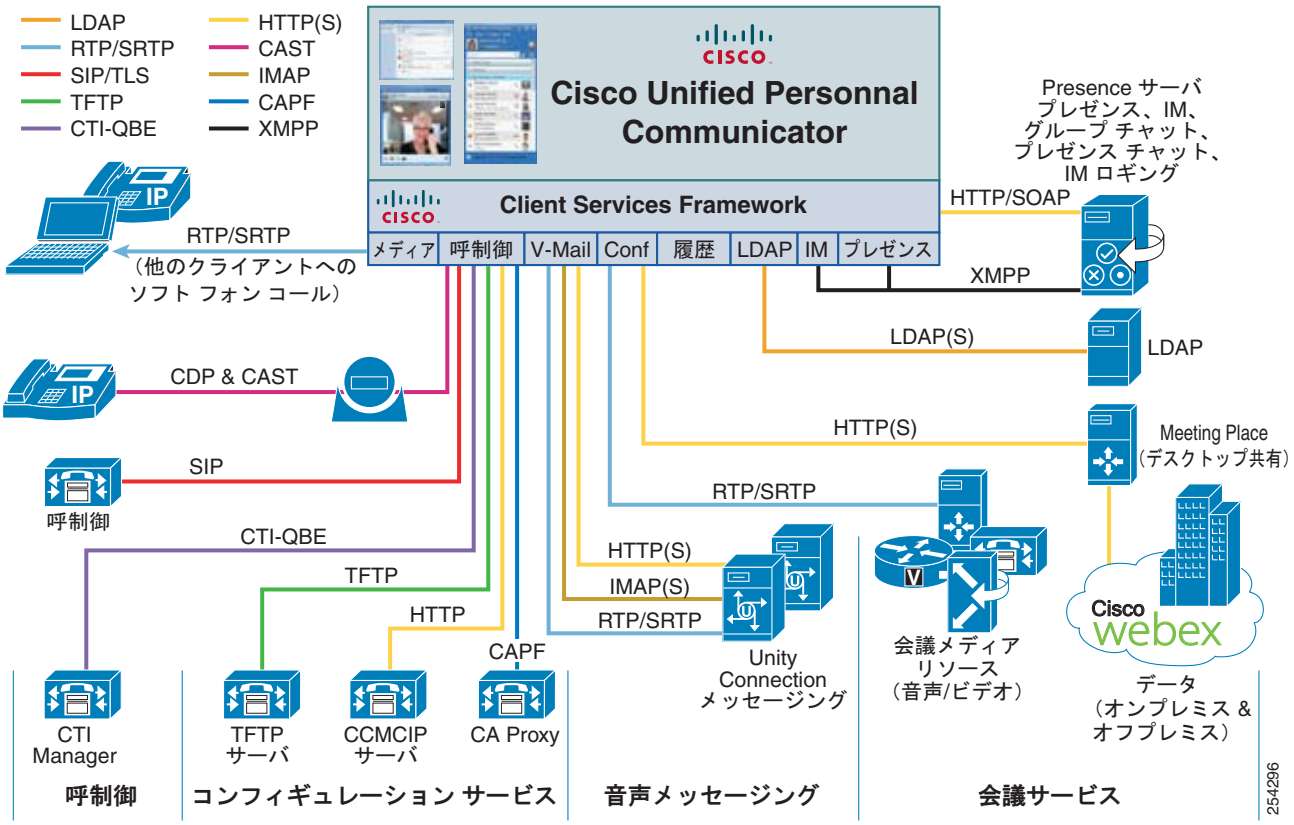
- 管理者は、組織における Unified Client Services Framework のインストール、配置、および設定方法を決定する必要がある。アプリケーションのインストールには Altiris などの有名なインストール パッケージを使用し、TFTP サーバ、CTI Manager、CCMCIP サーバ、ボイスメール パイロット、LDAP サーバ、LDAP ドメイン名、および LDAP 検索コンテキストといった必要なコンポーネントのユーザ レジストリ設定にグループ ポリシーを使用することを推奨します。
- Unified Communications とバックエンドのディレクトリ コンポーネントの適正な統合を可能にするため、Cisco Unified Client Services Framework ユーザのユーザ ID とパスワードの設定は、LDAP サーバに保存されているユーザのユーザ ID とパスワードに一致する必要がある。
- Cisco Unified CM のディレクトリ番号設定と LDAP の電話番号属性は、完全な E.164 番号で設定する必要がある。プライベート企業ダイヤル プランを使用できますが、それに伴ってアプリケーション ダイヤリング規則、ディレクトリ ルックアップ規則、トランスレーション パターンなどの使用が必要になる場合があります。
- Cisco Unified IP Phone の制御にデスクフォン モードを使用する場合は、CTI を使用する。したがって、Unified CM 配置のサイジングを行うときは、CTI の使用を必要とする他のアプリケーションも考慮に入れる必要があります。
- ファイアウォールとセキュリティの面での考慮事項については、Client Services Framework に必要なポート使用および統合される対応アプリケーションが、各アプリケーションの製品リリース ノートに記載されています。
- バックエンド LDAP サーバへのトラフィック量（照会およびルックアップ）への影響を低減するために、配置全体のためのトップレベルの検索ベースではなく、Client Services Framework のための簡潔な LDAP 検索ベースを設定してください。

Cisco Unified Personal Communicator のアーキテクチャ

Cisco Unified Personal Communicator は、完全に統合された Cisco Unified Communications ソリューションでの Cisco Unified Client Services Framework を使用することによる単一のデスクトップ クライアントでの一貫したユーザ エクスペリエンスの提供を可能にします。このソリューションは、標準ベースの音声とビデオ、ユニファイド メッセージング、Web 会議、デスクトップ制御、テレフォニー プレゼンスなどの幅広い一連の Cisco Unified Communications サービスへのアクセスを提供したうえで、Cisco Unified Presence の常に有効なプレゼンスとインスタント メッセージングの機能が組み込まれています。

Cisco Unified Personal Communicator 配置のソリューション アーキテクチャには、図 24-2 に示すように、ユーザの関連付け、音声、およびビデオ サービス、プレゼンスおよびインスタント メッセージング サービスのための Cisco Unified Presence、ユーザ アカウント情報のための LDAP、Cisco Unified Client Services Framework for PC の音声またはデスクフォン制御といった一連の機能のための Cisco Unified Communications Manager が含まれています。

図 24-2　Cisco Unified Personal Communicator



Cisco Unified Personal Communicator の配置では、ユーザ アカウントの一貫性のために、管理者がユーザのディレクトリ番号情報を E.164 値（例：+18005551212）で入力し、Unified CM での LDAP の同期化と認証を有効にすることを推奨します。Cisco Unified Personal Communicator は、音声とビデオの制御、およびプレゼンスとインスタント メッセージングのための Cisco Unified Presence について、Cisco Unified CM を使用して、すべての Cisco Unified Communications コンポーネントとしっか

り統合されています。完全な Unified Communications ソリューションを配置しないケースについては、Cisco Unified Presence からプレゼンスおよびインスタント メッセージング サービスを提供するために、Cisco Unified Personal Communicator は IM だけの設定でも稼動できます。IM だけのソリューションの配置ガイドラインについては、「Cisco Unified Presence」（P.23-1）の章を参照してください。

Cisco Unified Personal Communicator の配置

Cisco Unified Personal Communicator を配置する際には、次のガイドラインに従ってください。

コンフィギュレーション設定

Cisco Unified Personal Communicator は、その設定情報を Cisco Unified Presence から SOAP インターフェイスを介してダウンロードします。設定情報はすべて、Cisco Unified Presence（ボイスメール、会議、CTI ゲートウェイ、LDAP、および CCMCIP プロファイル）上のプロファイル内で作成され、保存され、ユーザに割り当てられます。ユーザがすでに作成され、ライセンスされ、割り当てられていることをあらかじめ確認してから、プロファイル コンフィギュレーション設定をユーザに割り当てることを推奨します。プロファイル設定の詳細については、次の URL から入手できる Cisco Unified Personal Communicator のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html

ソフトウェア インストール

ソフトウェア インストール配置は、多数の異なる方法で処理することができ、Microsoft Active Directory Group Policy、Systems Management Server（SMS）、Altiris、あるいはスクリプト/バッチファイルを持つ自己解凍式の実行可能ファイルなどのデスクトップ管理ツールを使用して配置されるように設計されています。お客様のトポロジはそれぞれ異なるため、どの方法を使用するかについての推奨はありません。ソフトウェア配置方法の詳細については、次の URL から入手できる Cisco Unified Personal Communicator のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6844/tsd_products_support_series_home.html

Cisco Unified Personal Communicator のキャパシティ プランニング

Cisco Unified Personal Communicator のためのソリューションの設計とサイジングを検討する際は、すべてのコンポーネントについて、スケーラビリティに関する次のインパクトを考慮する必要があります。

- クライアントのスケーラビリティ

  Cisco Unified Presence サーバ ハードウェアの配置が決まれば、クラスタがサポートできるユーザの数が決定されます。Cisco Unified Personal Communicator の配置は、クラスタ内のすべてのサーバに対し、すべてのユーザを均等に割り当てる必要があります。これは、User Assignment Mode Sync Agent サービス パラメータを [balanced] に設定すれば、自動的に処理されます。

  連絡先リストには、連絡先を最大 200 まで設定できます。

- IMAP のスケーラビリティ

  IMAP または IMAP-Idle の接続数は、メッセージング統合のプラットフォームのオーバーレイ（Cisco Unity または Cisco Unity Connection）によって決定されます。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unity または Cisco Unity Connection の製品マニュアルを参照してください。

- Web 会議

  Cisco Unified MeetingPlace Web ライセンシングは、同時に可能な Web 会議参加者の数を決定します。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unified MeetingPlace の製品マニュアルを参照してください。

- ビデオのサイジングとキャパシティ

  ビデオ会議とスイッチングは、Cisco Unified Videoconferencing MCU のサイジングと設定、Cisco MeetingPlace Hardware Media Server（HMS）のサイジングと設定、または Cisco Unified MeetingPlace Express VT によって同時音声、ビデオ、および Web 参加者のために決定されます。特定の設定のサイジングについては、http://www.cisco.com で入手可能な Cisco Unified MeetingPlace Express VT の製品マニュアルを参照してください。

Cisco Unified Personal Communicator は Unified CM と相互接続します。そのため、Cisco Unified Personal Communicator 音声またはビデオ コールを開始した場合、Unified CM の現在の機能に関する次のガイドラインが適用されます。

- CTI のスケーラビリティ

  Desk Phone モードでは、Cisco Unified Personal Communicator からのコールが、Unified CM 上の CTI インターフェイスを使用します。したがって、「コール処理」（P.8-1）の章に明記された CTI の制限を遵守してください。Unified CM クラスタのサイジングを行う際は、これらの CTI デバイスを含める必要があります。

- コール アドミッション制御

  Cisco Unified Personal Communicator は、Unified CM ロケーションまたは RSVP 経由で、音声またはビデオ コールに対してコール アドミッション制御を適用します。

- コーデックの選択

  Cisco Unified Personal Communicator の音声およびビデオ コールは、Unified CM リージョン設定よるコーデックの選択を利用します。

Cisco Unified Personal Communicator のすべての設定と連絡先は、Cisco Unified Presence データベースに保存されます。これらには、大量のデータが含まれる可能性があります。現在の会話履歴リストは、各タブ（[Chats]、[Voice Messages]、[Calls]）で 50 エントリに制限されており、連絡先リストのサイズは 200 個の連絡先に制限されています。したがって、プレゼンス データの交換と、会議、ビデオ、およびメッセージングのトラフィックに対して帯域幅の使用率を考慮する必要があります。

Cisco Unified Personal Communicator には、帯域幅に関する次の考慮事項も適用されます。

- Presence User Profile（PUP; プレゼンス ユーザ プロファイル）は、ログイン、プレゼンス ステータスの変更、および参加者の変更の数を考慮してユーザ配置トラフィック パターンを調べます。ログイン数が 1 時間あたり 0.5、プレゼンス ステータスの変更数が 1 時間あたり 0.5、参加者の変更数が 1 時間あたり 0.25 の一般的な PUP では、Cisco Unified Presence と Unified Personal Communicator 間の帯域幅使用率（1 秒あたりのキロビット数）を計算する場合の一般的なガイドラインとして次の式を使用できます（例については、表 24-3 を参照）。

  USERS * [30 + ROSTER*7 + IM*3 + CALLS * (33 + 3*ROSTER)] / 1000

  定義：

  - USERS = Unified Personal Communicator を使用しているユーザ数。
  - ROSTER = Unified Personal Communicator ユーザの平均参加者サイズ。
  - IM = Unified Personal Communicator ユーザの 1 時間あたりのインスタント メッセージ数。
  - CALLS = 1 時間あたりのソフトフォン コール数。

表 24-3　Unified Personal Communicator の帯域幅要件の例

エンタープライズ	ユーザ数	参加者サイズ	IM 数	1 時間あたりのコール数	帯域幅使用率
小	1,000	100	25	4	2,100 kbps（2.1 Mbps）
大	5,000	200	25	4	20,185 kbps（20.2 Mbps）

- Cisco Unified MeetingPlace の音声、ビデオ、Web コラボレーション セッションについては、「Cisco Unified MeetingPlace」（P.22-13）を参照してください。
- ビデオ コールについては、「IP ビデオ テレフォニー」（P.12-1）の章を参照してください。
- Cisco Unity または Unity Connection については、「シスコの音声メッセージング」（P.21-1）の章の「帯域幅の管理」（P.21-35）の項を参照してください。

Cisco Unified Personal Communicator のハイ アベイラビリティ

Cisco Unified Presence クラスタ内のすべてのユーザは、情報交換の前に、サーバに割り当てる必要があります。Cisco Unified Presence では、デフォルトで自動的にユーザがクラスタ内のすべてのサーバに均等に割り当てられます。管理者は、User Assignment Mode Sync Agent サービス パラメータをデフォルトの **balanced** から **None** に変更してユーザの割り当て先を制御できます。このパラメータが **None** に設定されている場合、ユーザの割り当ては [System] > [Topology] メニューから行われます。

Cisco Unified Personal Communicator は基本的な配置、自動的な冗長性を実現するハイ アベイラビリティ配置、および IM 専用配置を提供します。Cisco Unified Presence の 2 サーバ構成のサブクラスタでは、サブクラスタの片方のサーバに関連付けられたユーザが、自動的に他方のサーバにも認識されるので、設定されたサーバとの通信が中断した場合の自動フェールオーバーが可能です Cisco Unified Personal Communicator のハイ アベイラビリティは、Cisco Unified Presence サブクラスタ内でだけサポートされます。

図 24-3 に示されているように、サーバ リカバリ マネージャは Cisco Unified Presence 上のさまざまなサービスをモニタして、サービスが XMPP フェールオーバー イベントを開始するのに失敗したかどうかを調べます。XMPP フェールオーバー中は次の一連のイベントが発生します。

1. サービスが通信しなくなったことをサーバ リカバリ マネージャが検出すると、サーバ 1A からサーバ 1B へのフェールオーバー ユーザ移動操作が開始されます。ユーザ 123 がホーム サーバ 1A からサーバ 1B に移動されます。
2. Unified Personal Communicator は、サーバ 1A との接続がタイムアウト、接続損失、または XMPP プロトコル更新によって失われたことを調べ、サーバ 1B との新しい接続を開始します。

図 24-3　Unified Personal Communicator XMPP フェールオーバー

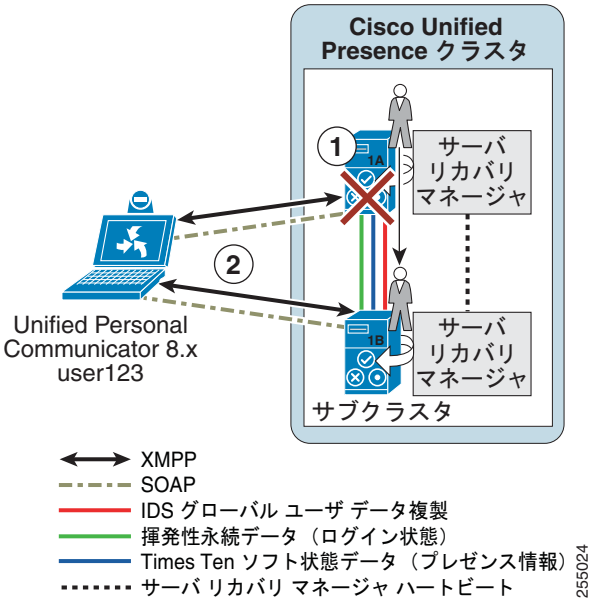
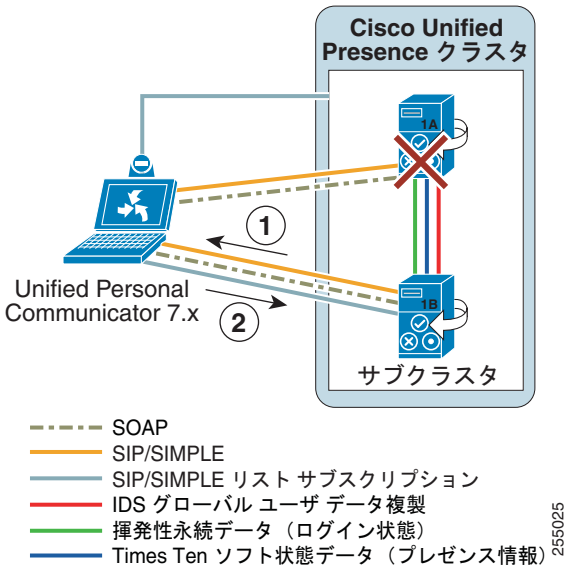


図 24-4 に示されているように、Cisco Unified Presence サーバ 1A の障害発生時には、SIP 対応クライアントで次の一連のイベントが発生します。

1. Cisco Unified Presence サーバ 1B が、Cisco Unified Personal Communicator 7.*x* に SIP NOTIFY を送信し、サーバ 1A での Presence と Unified Client Change Notification（UCCN）サブスクリプション状態を終了します。
2. Cisco Unified Personal Communicator 7.*x* が Cisco Unified Presence サーバ 1B に SIP SUBSCRIBE メッセージを送信し、その Presence と UCCN サブスクリプション状態を再度アクティブにします。

図 24-4　Unified Personal Communicator SIP フェールオーバー



Cisco Unified Personal Communicator の設計上の考慮事項

Cisco Unified Personal Communicator の必須インターフェイスには、Cisco Unified Presence、Cisco Unified Communications Manager（Unified CM）、および LDAP v3 準拠サーバがあります。Cisco Unified Personal Communicator のオプションのインターフェイスには、Cisco Unity、Cisco Unity Connection、Cisco Unified MeetingPlace、Cisco Unified Videoconferencing、および Cisco Unified MeetingPlace Express VT が含まれます。ソリューションの設計とサイジングを行う際には、キャパシティ プランニングのガイドラインに加えて、設計上の次の考慮事項を検討する必要があります。

- 管理者は、組織における Cisco Unified Personal Communicator のインストール、配置、および設定方法を決定する必要があります。Altiris などのよく知られたインストール パッケージを使用してアプリケーションをインストールすることを推奨します。Cisco Unified Personal Communicator は、LDAP、CTI、ボイスメール、会議、およびユーザに割り当てられている CCMCIP プロファイルのための設定情報を Cisco Unified Presence 上の SOAP インターフェイスを介して収集します。
- テキスト会議室を使用する場合は、次の制限事項があります。
  - テキスト会議の最大ユーザ数は、100 ユーザです。
  - テキスト会議の履歴に表示されるメッセージの最大数は、100 です。
- LDAP 検索コンテキスト

  LDAP フィルタを指定して、特定のオブジェクト クラスのみを検索する機能を使用すると、ディレクトリからコンピュータを除いたユーザだけを取得できます。これには、検索コンテキストの末尾に &(objectclass=user) を追加します。次の例を参考にしてください。

  cn=user,**dc**=example,**dc**=com;&(objectclass=user)

  複数の LDAP 検索コンテキストを指定するには、[Cisco Unified Presence Administration の LDAP Search Context] フィールドで、# をデリミタとして使用します。次の例では、サポートされる形式を示します。

  ou=test,**dc**=example,**dc**=com#**ou**=testing,**dc**=example,**dc**=com

Cisco Unified Personal Communicator は、両方の組織ユニットを「test」、「testing」の順に検索します。

LDAP 検索コンテキスト フィールドに指定できるのは最大 255 文字なので、サポートされる組織ユニットは、個別の検索コンテキストのサイズと文字数に応じて異なる可能性があります。

Cisco Unified Presence がフェデレーション配置の設定を完了すると、Cisco Unified Personal Communicator では、フェデレーションの連絡先の追加も可能になります。これによりユーザは、既存のドメイン内の連絡先と他のドメインのユーザを入力し、制御できます。この追加の連絡先機能によって、ユーザは、ブロック リストや通信可能なドメインなどのプライバシー設定も制御できます。

Cisco Unified Personal Communicator は、Differentiated Services Code Point（DSCP）により、レイヤ 3 IP パケットをマーキングします。Cisco Unified Personal Communicator は、コール シグナリング トラフィックを DSCP 24（PHB CS3）の値でマーキングします。またボイス メディア トラフィックを DSCP 46（PHB EF）の値でマーキングします。ただしパーソナル コンピュータ トラフィックは、通常、信頼されていないため、PC でアプリケーションによって施された DSCP マーキングは、ネットワークで除去されます。したがって、アクセス ルータやスイッチは、Cisco Unified Personal Communicator が利用するポート範囲で、これらの DSCP マーキングを許可するように設定する必要があります。トラフィック マーキングの詳細については、次の Web サイトで入手可能な『*Enterprise QoS Solution Reference Network Design (SRND)*』を参照してください。

http://www.cisco.com/go/designzone

Cisco WebEx Connect のアーキテクチャ

Cisco WebEx Connect は、セキュリティ、スケーラビリティ、パフォーマンス、アベイラビリティを強制的に確立するための拡張可能なオープン型コラボレーション プラットフォームを実現します。Cisco WebEx Connect は、次の 2 つの主要コンポーネントで構成されています。

- 「Cisco WebEx Connect Client」（P.24-16）
- 「Cisco WebEx Connect Platform」（P.24-17）

Cisco WebEx Connect Client

Cisco WebEx Connect クライアントは、Microsoft Windows XP、Vista、または Windows 7 オペレーティング システムを実行するエンド ユーザの PC 上に存在するリッチ クライアントであり、可用性ステータス、エンタープライズ クラスのインスタント メッセージング、スペース、音声、デスクトップ共有、Cisco WebEx 会議、および Cisco Unified Communications 統合を提供します。詳細については、次の URL から入手可能な「*Cisco WebEx Connect Product Sheet*」を参照してください。

http://www.cisco.com/en/US/prod/collateral/ps10352/0709_PS_Connect6.pdf

Cisco WebEx Connect サイト管理者は、エンド ユーザのユーザ ID とパスワードを別個に作成するのではなく、シングル サインオンを使用して、エンド ユーザによる Cisco WebEx Connect に対する認証および署名を可能にできます。WebEx Connect でのシングル サインオンの詳細については、次の Web サイトにある『*WebEx Connect: User Provisioning and SSO* Developer Technical Note』を参照してください。

http://developer.webex.com/c/document_library/get_file?folderId=11835&name=DLFE-244.pdf

Cisco WebEx Connect Platform

Cisco WebEx Connect Platform は、同期および非同期コラボレーションに対応したマルチテナント型 Software-as-a-Service（SaaS）プラットフォームです。WebEx Connect Platform は、Cisco WebEx Collaboration Cloud 内でホストされ、コラボレーション アプリケーションと統合を可能にします。これにより、会社およびエンド ユーザが自分の作業環境をカスタマイズすることが可能になります。WebEx Connect Platform の詳細については、次の URL から入手可能な「*WebEx Connect Platform Technical Overview*」を参照してください。

http://developer.webex.com/c/document_library/get_file?folderId=11836&name=DLFE-260.pdf

Cisco WebEx Software-as-a-Service 製品の詳細については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

Cisco WebEx Collaboration Cloud の詳細については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/prod/ps10352/collaboration_cloud.html

Cisco WebEx Connect の配置

Cisco WebEx Connect を配置する際には、ここで示すガイドラインに従ってください。

コンフィギュレーション設定

Cisco WebEx Connect ユーザは、次の URL から入手可能な『*Cisco WebEx Connect Administrator's Guide*』で説明するとおり、Cisco WebEx Connect Administration Tool を通じて設定および管理されます。

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco Unified Communications の統合

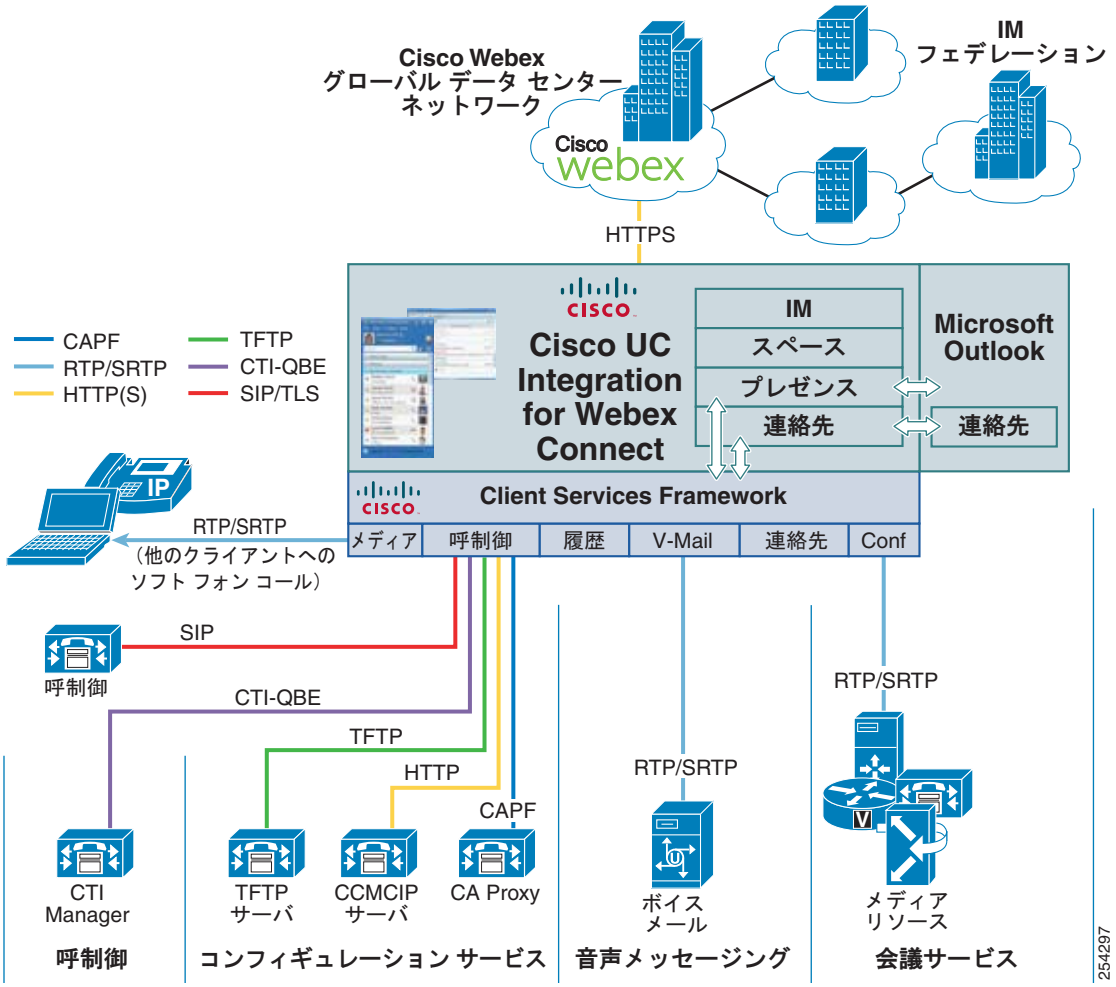
Cisco WebEx Connect は、Cisco Unified Communications Manager を使用した Cisco WebEx Connect 内からの直接のクリックコールを設定できます。Cisco Unified Communications は、配置トポロジとニーズに応じて次のいずれかの方法で Cisco WebEx Connect に統合できます。

- 「Cisco Unified Communications Integration™ for Cisco WebEx Connect」（P.24-17）
- 「Cisco WebEx Connect Unified Communications Widget」（P.24-19）（CTI WebDialer、ボイスメール、およびスピード ダイヤルを使用したクリックツーコール）

Cisco Unified Communications Integration™ for Cisco WebEx Connect

図 24-5 に示すように、Cisco Unified Communications Integration™ for Cisco WebEx Connect は、Client Services Framework を使用した Unified CM と Cisco WebEx Connect の強固な統合を可能にして、Cisco WebEx Connect クライアント内での完全な呼制御を有効にします。

図 24-5　Cisco Unified Communications Integration™ for Cisco WebEx Connect



Client Services Framework は、デスクトップ クライアントをオーディオ エンドポイントとするソフトフォン呼制御にも、デスクトップ クライアントが Cisco Unified IP Phone を制御するデスクフォン制御にも対応し、いずれの場合も WebEx Connect の [Phone] タブに表示されます。クリックコール機能用に連絡先を入力して使用する方法は、次のとおりです。

- コンタクトを選択するには、右クリックしてそのコンタクトの表示された電話番号を選択するか、またはハブの下部にある WebEx ボールを使用してそのコンタクトへの通信の方法（クリックコールなど）を選択します。
- インスタント メッセージ会話の間は、WebEx ボールを使用して通信方法を選択できます。
- WebEx Connect 内に表示されるハイパーリンクの番号をクリックします。この番号が有効な内線番号または有効な番号である場合、デスクトップフォンの統合を使用していればエンド ユーザの IP 電話とのコール、またはソフトフォンの統合を使用していればローカル PC とのコールを発信するためのコマンドが、Cisco Unified Communications Integration™ から Unified CM に送信されます。

- PC 上の Microsoft Outlook の個人用アドレス帳にある連絡先名を検索するか、ソフトフォンのディレクトリ ボックスを使用して電話番号を入力します。ユーザは、電話番号または連絡先名を入力し、番号を強調表示して、ダイヤル キーを押すだけです。
- デスクトップフォンの統合を使用している場合は IP 電話から、またはソフトフォン統合を使用している場合はローカルのダイヤル パッドから手動でコールします。呼制御は、WebEx Connect クライアントからも利用できます。

Cisco WebEx Connect Unified Communications Widget

Cisco WebEx Connect Unified Communications Widget（CTI WebDialer、ボイスメール、およびスピード ダイヤル）は、Cisco WebEx Connect Widget フレームワーク内で実行され、REST インターフェイス（JSON/HTTP）経由で Web アプリケーションと通信します。Web アプリケーションは、REST を使用した Lightweight Directory Access Protocol（LDAP; 軽量ディレクトリ アクセス プロトコル）照会用の LDAP Web サービス、REST 経由のログインおよびプレゼンス管理用のプレゼンス ログイン サービス、AVVID XML Layer（AXL）/Simple Object Access Protocol（SOAP）経由のスピード ダイヤル アクセス、およびバックエンド システムの設定を可能にする管理ポイントを提供します。

CTI WebDialer ウィジェットにより、ユーザはクリックコール統合および機能を利用できます。Cisco WebEx Connect 内の番号（4 桁以上）にはハイパーリンクが設定され、ユーザはその番号をクリックするだけで、電話機のキーパッドで電話番号を入力せずにコールを開始できます。Unified CM で CTI モニタリングを有効にして、WebEx Connect 管理ページで Unified CM 統合を有効にする必要があります。

Cisco WebEx Connect の設定方法の詳細については、次の Web サイトから入手可能な『*Cisco WebEx Connect Administrator's Guide*』の Cisco WebEx Connect の Cisco WebEx Meeting Center との統合に関する項を参照してください。

http://www.webex.com/webexconnect/orgadmin/help/index.htm?toc.htm?cs_singleptprov.htm

セキュリティ設定

図 24-6 は、WebEx セキュリティ モデルの機能層を構成する、相互に関連する独立した要素を示しています。

図 24-6　　WebEx セキュリティ モデル

最下位層は、Cisco WebEx データ センターの物理セキュリティを示しています。すべての従業員は、広範なバックグラウンド チェックを通過し、データ センターに入るためのデュアルファクタ認証を実行する必要があります。

次のレベルのポリシー管理では、WebEx Connect 組織管理者が、個々のユーザ、グループ、または Cisco WebEx Connect 組織全体に異なるポリシーを設定することによってアクセス制御レベルを設定し、管理できます。外部ユーザまたはドメインに固有のブラック リストまたはホワイト リスト ポリシーを作成して、インスタント メッセージング交換を制限したり、許可したりできます。Cisco WebEx Connect 組織モデルでは、ユーザ ベース全体に固有の役割やグループを作成することもでき、管理者は特定の権限を役割やグループに割り当てたり、組織全体に対してアクセス コントロールなどのポリシーを設定したりできます。

Cisco WebEx Connect へのアクセスは、認証層で制御されます。いずれのユーザも一意のログインとパスワードを所有します。パスワードが保存されたり、クリア テキストの E メールで送信されたりすることはありません。パスワードを変更できるのは、エンド ユーザ自身だけです。管理者は、次のログイン時にエンド ユーザがパスワードを変更するように、パスワードのリセットを選択できます。また、管理者は、Cisco WebEx Connect と企業の Active Directory との間の Single Sign On（SSO; シングル サイン オン）統合を使用して、エンド ユーザのアクセス管理を簡略化することもできます。シングル サイン オン統合は、Identity Management System（IDMS）を使用して実現されます。

暗号化層では、Cisco WebEx Connect ユーザ間のすべてのインスタント メッセージング通信が暗号化されます。Cisco WebEx Connect ユーザと Connect Collaboration クラウド内にあるサーバ間のすべてのインスタント メッセージング通信は、デフォルトで TLS 暗号化を使用して暗号化されます。その一方で、Cisco Webex Connect ユーザ間のインスタント メッセージング通信はデフォルトで AES 暗号化を使用して暗号化されます。Cisco Unified Communications Integration for Cisco WebEx Connect を PC（ソフトフォン）モードで使用する音声通話は、Secure Real-time Transport Protocol（SRTP）を使用して暗号化できます。インスタント メッセージング セキュリティ オプションは Cisco WebEx Connect サイト管理者によってポリシーで制御され、Cisco Unified Communications Integration for Cisco WebEx Connect セキュリティ オプションは Cisco Unified Communications Manager 管理者によって制御されるか、[Unified Communications] タブの Cisco WebEx Connect クライアント設定を使用してエンド ユーザによって制御されます。

Cisco WebEx Connect Platform では、SAS70 Type II 監査などのサードパーティによる監査を使用して、カスタマーに半年ごとに個別のセキュリティ レポートを提供します。カスタマーは、シスコのセキュリティ組織に要求すればいつでもこのレポートを確認できます。その他の Cisco WebEx Connect セキュリティについては、次の URL から入手可能な Cisco WebEx Connect IM セキュリティ ホワイト ペーパーを参照してください。

http://wwwin.cisco.com/csg/docs/CiscoWebExConnectSecurityWP.pdf

ファイアウォール ドメインのホワイト リスト

アクセス コントロール リストは、webex.com ドメインおよび webexconnect.com ドメインと、この両ドメインのすべてのサブドメインからのすべての通信を許可するように明確に設定する必要があります。WebEx Connect Platform からエンド ユーザにユーザ名とパスワードを通知する電子メールが送信されます。これらの電子メール メッセージは mda.webex.com ドメインから発信されます。

インスタント メッセージのロギング

Cisco WebEx Connect インスタント メッセージング通信は、ユーザがログインしているパーソナル コンピュータのローカル ハード ドライブに記録されます。インスタント メッセージのロギングは、Org Admin ツールでポリシーを使用して有効にすることができる、Cisco WebEx Connect の機能です。インスタント メッセージのロギングを Cisco WebEx Connect に対して有効にすると、インスタント メッセージは記録され、次のパスに保持されます。

file:///c:/Documents and Settings/user/_Connect/Archive/_username

エンド ユーザは、ロギングの詳細、ロギングの有効化または無効化、およびログの保存期間を設定できます。これらの設定は、Cisco WebEx Connect クライアント設定の [General IM] で行います。

Cisco WebEx Connect の以前のリリースで使用していた Cisco WebEx Connect Advanced Auditor には、Cisco WebEx Connect の C6 リリースとの互換性はありません。詳細な監査機能や e-Discovery（電子情報の開示）機能を必要とする場合は、サードパーティ製のソリューションを利用することも検討してください。現在シスコでは、インスタント メッセージング通信の詳細な監査や中央集中型ロギングをサポートしていません。ただし、Cisco WebEx Connect では、サードパーティの SaaS アーカイブ サービスまたはセキュアな SMTP サービスを使用して組織内のユーザ間で交換されるインスタント メッセージのロギングとアーカイブを実行できます。

IM アーカイブの詳細については、次の Web サイトにある『*Cisco WebEx Connect Administrator's Guide*』を参照してください。

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco WebEx Connect のキャパシティ プランニング

エンド ユーザが WebEx Connect にログインして、プレゼンス、インスタント メッセージング、および Voice over IP（VoIP）コーリングなどの基本機能を利用するために必要なものは、56 kbps ダイヤルアップ インターネット接続だけです。ただし、小規模のオフィスや支店でファイル転送、スクリーン キャプチャ、PC 同士のビデオ コール、チーム スペースなどの高度な機能を利用するには、512 kbps 以上のブロードバンド接続が必要です。

Cisco Unified Communications 統合は、クリックコール アプリケーションおよび Cisco Unified Client Services Framework でのデスクフォン制御モードに Unified CM CTI Manager を使用します。したがって、「コール処理」（P.8-1）の章に明記された CTI の制限を遵守してください。Cisco UC Integration™ for WebEx Connect がソフトフォン（コンピュータ上の音声）モードで稼動しているときには、Cisco Unified Client Services Framework は、Cisco Unified CM での SIP 登録エンドポイントです。Cisco Unified Communications を含むソリューションのサイジングを行う際には、Unified CM クラスタ上のリソースを使用する CTI デバイスと SIP エンドポイント デバイスを含める必要があります。

Cisco WebEx Connect のハイ アベイラビリティ

WebEx Connect は、Software-as-a-Service アプリケーションです。エンド ユーザが WebEx Connect にログインするには、エンド ユーザの PC をインターネットに接続する必要があります。標準のインターネット接続があれば、利用できます。エンド ユーザがリモートの場合は、WebEx Connect にログインするために、そのユーザが会社の VPN を介して接続する必要はありません。Cisco WebEx Connect は、可用性の高い冗長なトポロジに配置できます。Cisco WebEx Connect Software-as-a-Service アーキテクチャの配置は、この項で説明する各種のネットワークおよびデスクトップ要件で構成されます。

ハイ アベイラビリティ

マルチテナント型 Software-as-a-Service アーキテクチャを使用していて、グループ内のいずれかの個別サーバが何らかの理由で停止した場合、要求を Cisco WebEx Connect Platform 内の利用可能な他のサーバにルーティングできます。

Cisco WebEx Network Operations Team は、Cisco WebEx Network Operations Center（NOC）から Cisco WebEx Collaboration Cloud を毎日 24 時間アクティブにモニタします。Cisco WebEx テクノロジーの概要については、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10352/products_category_technologies_overview.html

冗長性、フェールオーバー、およびディザスタ リカバリ

Cisco WebEx のグローバル サイト バックアップ アーキテクチャは、電源異常、自然災害による停電、放電過多、ネットワーク容量過多、その他のタイプのサービス中断を処理します。グローバル サイト バックアップでは、手動と自動の両方のフェールオーバーをサポートします。手動フェールオーバー モードは通常、メンテナンス時間枠で使用されます。自動フェールオーバー モードは、サービス中断によるリアルタイム フェールオーバーの場合に使用されます。

グローバル サイト バックアップは、エンド ユーザに対して自動的かつ透過的であり、すべてのユーザが利用でき、フェールオーバー可能なユーザ数の制限もありません。

グローバル サイト バックアップは、次の主要コンポーネントで構成されます。

- グローバル サイト サービス：ネットワーク レベルでトラフィックのモニタリングとスイッチングを行います。
- データベース複製：プライマリ サイトでのデータ トランザクションをバックアップ サイトに確実に転送します。
- ファイル複製：ファイル変更が、プライマリ サイトとバックアップ サイト間で同期されるようにします。

Cisco WebEx Connect に関する設計上の考慮事項

Cisco WebEx Connect は、Software as a Service モデルとして配置されるため、設計上のおよび配置上の考慮事項が最小限になります。Cisco WebEx Connect ソリューションは、デスクトップに存在するシック クライアントとして提供され、各ユーザに対する Web IM クライアント（ブラウザが必要）も含みます。設計と配置には、Cisco WebEx Connect Platform との相互作用、あるいは Cisco Collaboration Cloud として知られるものが必要です。Cisco WebEx Connect は、Cisco Unified Communications Manager およびサードパーティ製アプリケーションと統合されます。Cisco WebEx Connect を配置する際は、以降の項に示す設計上の考慮事項を使用してください。

1 つの管理対象の Connect ドメインあたり 1 つの Unified CM 統合

同じ管理対象 Cisco WebEx Connect ドメイン上のすべてのエンド ユーザが、同じ Unified CM 統合を使用する必要があります。エンド ユーザのサブグループの作成、および異なる Unified CM 統合を異なるサブグループに割り当てる機能は、現在のところサポートされていません。

Unified CM CTI Manager

Cisco WebEx Connect と Cisco Unified Communications を統合すると、Client Services Framework のクリックコールが CTI から使用できるようになります。その他のコール フローや呼制御機能は使用できません。

サポートされている CTI の最大限度については、「コール処理」（P.8-1）の章を参照してください。Cisco Unified Communications Widgets for Cisco WebEx Connect で CTI WebDialer を使用する際には、また、Cisco Unified Communications Integration™ for Cisco WebEx Connect でのデスクフォン制御モードには、CTI の数値が重要になります。

サードパーティ製の XMPP クライアントから Cisco WebEx Connect Platform への接続

シスコでは、他の XMPP クライアントによる Cisco WebEx Connect Platform への接続を公式にサポートしていませんが、XMPP プロトコルの性質上、エンド ユーザはさまざまな XMPP クライアントで WebEx Connect クレデンシャルを使用してプレゼンス クラウドに接続できます。XMPP ソフトウェア クライアントのリストは、次の Web サイトで入手できます。

http://xmpp.org/software/clients.shtml

組織のポリシーは、サードパーティ製の XMPP クライアントに適用できません。また、エンドツーエンド暗号化、デスクトップ共有、ビデオ コール、PC 間コール、および電話会議などの機能は、サードパーティ製のクライアントではサポートされていません。WebEx Connect 以外の XMPP IM クライアントでの Connect ドメインに対する認証を可能にするには、Domain Name System Service（DNS SRV; ドメイン ネーム システム サービス）レコードを更新する必要があります。[Configuration and IM Federation] の Cisco WebEx Connect サイト管理スペースに、特定の DNS SRV エントリを見つけることができます。

[Configuration and XMPP IM Clients] の Cisco WebEx Connect サイト管理スペースで、Connect 以外の XMPP クライアントの使用を明示的に許可する必要があります。

サードパーティ製 XMPP クライアントを使用したインスタント メッセージおよびプレゼンス フェデレーション

Cisco WebEx Connect ネットワークは、GoogleTalk および Jabber.org などの XMPP ベースのインスタント メッセージング ネットワークとフェデレーションできます。XMPP に基づいた公衆インスタント メッセージング ネットワークのリストは、次の Web サイトで入手できます。

http://xmpp.org/

WebEx Connect は、IBM Lotus Sametime XMPP ゲートウェイ経由で IBM Lotus Sametime と、また、Microsoft Office Communications Server XMPP ゲートウェイ経由で Microsoft Office Communications Server とフェデレーションできます。これらのサードパーティ製 XMPP ゲートウェイを使用する場合、IBM Lotus Sametime や Microsoft Office Communications Server の配置のバック エンドで設定を有効にする必要があります。シスコではこれらの設定を公式にサポートしていません。また、クライアント間の相互運用性も保証していません。

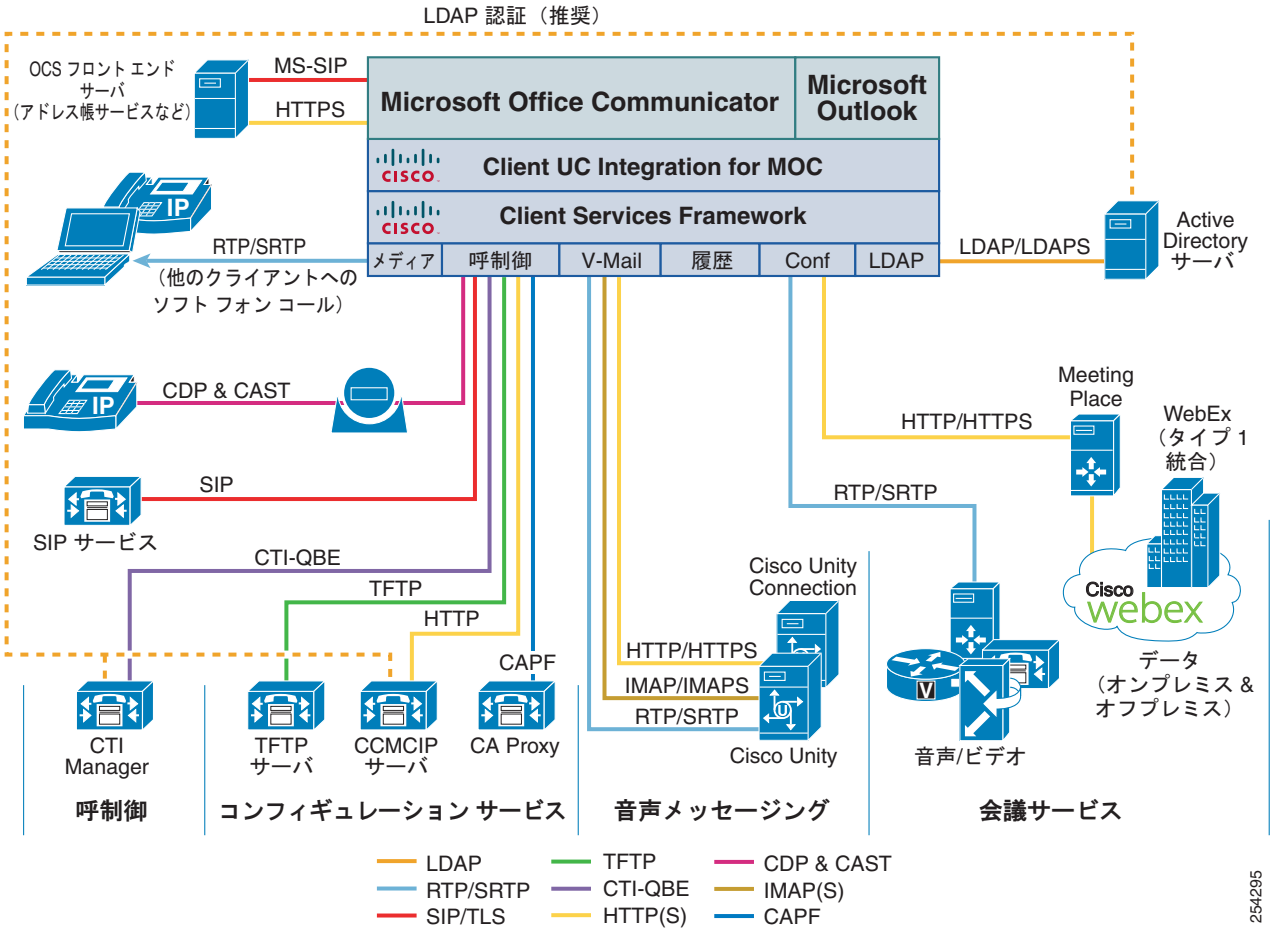
現在、WebEx Connect には Yahoo! Messenger および Windows Live Messenger との相互運用性はありませんが、フェデレーション ゲートウェイ経由で AIM とフェデレーションできます。

Cisco UC Integration™ for Microsoft Lync アーキテクチャ

Cisco UC Integration™ for Microsoft Lync は、一貫したユーザ エクスペリエンスを保ちつつ、Cisco Unified Client Services Framework を使用して Cisco Unified Communications の Microsoft Lync との緊密な統合を可能にします。このソリューションは、標準ベースの音声とビデオ、ユニファイド メッセージング、Web 会議、デスクトップ制御、テレフォニー プレゼンスなどの幅広い一連の Cisco Unified Communications サービスへのアクセスを提供することにより、Microsoft Lync のプレゼンスとインスタント メッセージングの機能を拡張します。

Cisco UC Integration™ for Microsoft Lync の配置のソリューション アーキテクチャ（図 24-7 を参照）には、音声およびビデオ サービス、プレゼンスおよびインスタント メッセージング サービスのための Microsoft Office Communications Server 2007、ユーザ アカウント情報のための Microsoft Active Directory、PC 音声またはデスクフォン制御のための Cisco Unified Client Services Framework、および Microsoft Lync が含まれます。

図 24-7　Cisco UC Integration™ for Microsoft Lync



Cisco UC Integration™ for Microsoft Lync の配置により、クライアントは、クライアントにダウンロードされた Office Communications Server Address Book からのユーザ情報を使用できます。いったんユーザがプレゼンスとインスタント メッセージングについて有効になると、アドレス帳が Office Communications Server から生成され、クライアントに配布されます。ユーザ アカウントの一貫性のために、管理者がユーザのディレクトリ番号情報を E.164 値（例：+18005551212）で入力し、Unified CM での LDAP の同期化と認証を有効にすることを推奨します。Cisco UC Integration™ for Microsoft Lync が Cisco Unified CM と Microsoft Active Directory の両方に接続され、アカウント クレデンシャルの同期規則を提供します。

Cisco UC Integration™ for Microsoft Lync の配置

Cisco UC Integration™ for Microsoft Lync を配置する際には、ここで示すガイドラインに従ってください。

コンフィギュレーション設定

Cisco UC Integration™ for Microsoft Lync は、そのコンフィギュレーション設定を、管理者が設定する必要がある一連のレジストリ エントリから読み取ります。これらのレジストリ コンフィギュレーション設定は、Microsoft Active Directory からグループ ポリシーを使用してプッシュして、コンフィギュレーション設定をクライアント コンピュータに自動的に配布することを推奨します。グループ ポリシーが推奨されるインストール メカニズムですが、サードパーティ製のソフトウェア配置ツール、バッチ ファイル、Vbscrip、手動での設定など、その他の方法も利用可能です。

Microsoft Active Directory グループ ポリシーは管理テンプレートを使用して拡張でき、Cisco UC Integration™ for Microsoft Lync は管理者がグループ ポリシーをサポートするために追加できる管理テンプレートを提供します。管理者は、管理テンプレートをロードしたら、レジストリ コンフィギュレーション設定（TFTP サーバ、CTI サーバ、CCMCIP サーバ、ボイスメール、LDAP サーバ）のための Cisco UC Integration™ 設定ポリシーを作成できます。これらの設定が格納されているレジストリの場所は、次のとおりです。

HKCU¥Software¥Policies¥Cisco Systems, inc.¥Client Services Framework¥AdminData

これらのグループ ポリシーがどこでどのように個々の組織単位に適用されるかを制御するために、グループ ポリシー管理コンソールを使用できます。クライアント ポリシーの観点から、Cisco UC Integration™ for Microsoft Lync を配置する際には、Microsoft Telephony Mode Policy を [IM and Presence Only] および [DisableAVConferencing] に設定することを推奨します。このクライアント ポリシー変更により、Microsoft Lync のユーザ エクスペリエンスで単一セットのコール オプションだけを表示できるようになります。

Cisco UC Integration™ for Microsoft Lync 配置では、インストールされた cisco-presence-states-config.xml ファイル内でカスタム プレゼンス状態の定義と展開を行うことも可能です。ただし、次のレジストリの場所に基づいて Microsoft Lync がこのカスタム プレゼンス状態ファイルを使用できるように、管理者がこのファイルを Microsoft Office Communications Server などの HTTP ロケーションに置き直すことを推奨します。

HKLM¥Software¥Policies¥Microsoft¥Communicator¥CustomStateURL

ソフトウェア インストール

ソフトウェア インストールは、多数の異なる方法で処理することができ、Microsoft Active Directory Group Policy、Systems Management Server（SMS）、Altiris、あるいはスクリプト/バッチ ファイルを持つ自己解凍式の実行可能ファイルなどのデスクトップ管理ツールを使用して配置されるように設計されています。お客様のトポロジはそれぞれ異なるため、どの方法を使用するかについての推奨はありません。ソフトウェア配置方法の詳細については、次の Web サイトで入手可能な Cisco UC Integration™ for Microsoft Lync のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps10317/index.html

Cisco UC Integration™ for Microsoft Lync のキャパシティ プランニング

Cisco UC Integration™ for Microsoft Lync は、Cisco Unified Client Services Framework でのクリックツーダイヤル アプリケーションとデスクフォン制御モードに Unified CM CTI Manager を使用します。したがって、「コール処理」（P.8-1）の章に明記された CTI の制限を遵守してください。Cisco UC Integration™ for Microsoft Lync がソフトフォン（コンピュータ上の音声）モードで稼動している場合、Cisco Unified Client Services Framework は、Cisco Unified CM での SIP 登録エンドポイントです。Cisco Unified Communications を含むソリューションのサイジングを行う際には、Unified CM クラスタ上のリソースを使用する CTI デバイスと SIP エンドポイント デバイスを含める必要があります。

Cisco UC Integration™ for Microsoft Lync のハイ アベイラビリティ

Cisco Unified Client Services Framework は、TFTP Server、CTI Manager、CCMCIP Server、Voicemail Server、LDAP Server といった設定コンポーネントのそれぞれにプライマリ サーバとセカンダリ サーバを提供します。ソフトフォン（コンピュータ上の音声）モードで稼動しているときには、Client Services Framework は、Cisco Unified CM での SIP 登録エンドポイントであり、Unified CM の登録エンドポイントのすべての登録機能および冗長機能をサポートします。デスクフォン モードで稼動しているときには、Client Services Framework は、CTI を使用して Cisco Unified IP Phone を制御し、プライマリおよびセカンダリ CTI Manager の設定をサポートします。CTI 配置の詳細については、「コール処理」（P.8-1）の章を参照してください。Client Services Framework は、ハイ アベイラビリティをサポートするために、オンライン状態の Microsoft Lync に依存しません。

Microsoft Lync は、プライマリ サーバとセカンダリ サーバに、Office Communications Server 配置のためのエンタープライズ プールの設定を提供します。その他の詳細については、次の URL から入手できる Microsoft Office Communications Server 2007 の展開マニュアルを参照してください。

http://technet.microsoft.com/en-us/library/dd425168%28office.13%29.aspx

Cisco UC Integration™ for Microsoft Lync の設計上の考慮事項

Cisco UC Integration™ for Microsoft Lync を配置する際には、次の設計上の考慮事項に注意してください。

- 管理者は、組織での Cisco UC Integration™ for Microsoft Lync のインストール方法、配置方法、および設定方法を決定する必要があります。アプリケーションのインストールには Altiris などの有名なインストール パッケージを使用し、TFTP サーバ、CTI Manager、CCMCIP サーバ、ボイスメール パイロット、LDAP サーバ、LDAP ドメイン名、および LDAP 検索コンテキストといった必要なコンポーネントのユーザ レジストリ設定にグループ ポリシーを使用することを推奨します。

- Cisco UC Integration™ for Microsoft Lync は、Cisco Unified CM と Microsoft Active Directory の両方に接続します。したがって、Unified Communications とバックエンド ディレクトリ コンポーネントの統合を可能にするために、Unified CM での LDAP 同期と LDAP 認証を有効にすることを推奨します。
- Cisco UC Integration™ for Microsoft Lync は、音声およびビデオ コールを開始するために、Microsoft Office Communications Server によって生成され、クライアントに配布されたアドレス帳を使用します。Microsoft Office Communications Server のインスタント メッセージングおよびプレゼンスについてユーザを有効にする前に、ユーザを Microsoft Active Directory 内で E.164 の電話番号で設定しておくことを推奨します。

Cisco IP Phone Messenger アプリケーションのアーキテクチャ

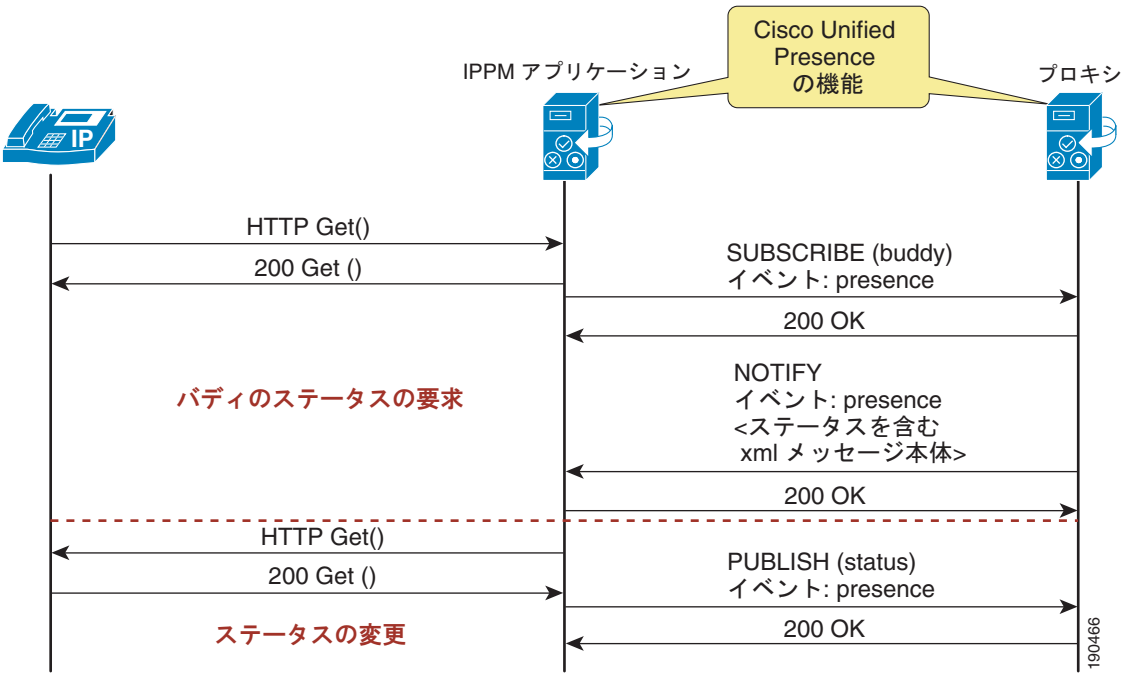
Cisco IP Phone Messenger は、ユーザが、バディ リストの作成、バディの集約プレゼンス情報の監視、およびバディの Cisco Unified IP Phone または準拠する SIP や SIMPLE クライアントまたはゲートウェイとのインスタント メッセージの交換などを行うための Cisco Unified の IP 電話サービスです。

Cisco Unified Presence のコンポーネントである Cisco IP Phone Messenger（IPPM）アプリケーションは、HTTP と SIP メッセージングの間のプロトコル変換プログラムとして動作します。IPPM アプリケーションは、Cisco Unified IP Phones との通信には XML over HTTP（http://www.cisco.com/go/apps）を使用し、SIP プロキシ/ レジストラ サーバとの通信には SIP を使用します。IPPM は、異なるパーティション内にあり、同じディレクトリ番号を持つ 2 つのデバイスを区別します。また、ユーザがエクステンション モビリティ経由でログインした場合も、同様に動作します。ただし、新しいユーザがログインするには、Cisco Unified Presence パブリッシャが必要です。

IPPM アプリケーションは、次のプレゼンス機能を提供します（図 24-8 を参照）。

- バディの集約されたプレゼンス ステータスを表示します。
- 手動によるプレゼンス ステータス（Available、Busy、Do Not Disturb）を上書きします。
- 電話機へのログイン時に、すべての電話機バディのプレゼンス ステータスに対し SUBSCRIBE を呼び出します。電話機からのログアウト時に、Expires=0（サブスクリプションの終了）に設定して SUBSCRIBE を呼び出します。
- プレゼンス エンジンからの NOTIFY メッセージの受信時に、IPPM アプリケーションで、バディのプレゼンス ステータスを更新します。
- 電話機（Phone Messenger Service）と Web インターフェイス（http://<*cup_server_address*>/ccmuser）のどちらからでも連絡先リストが管理できます。

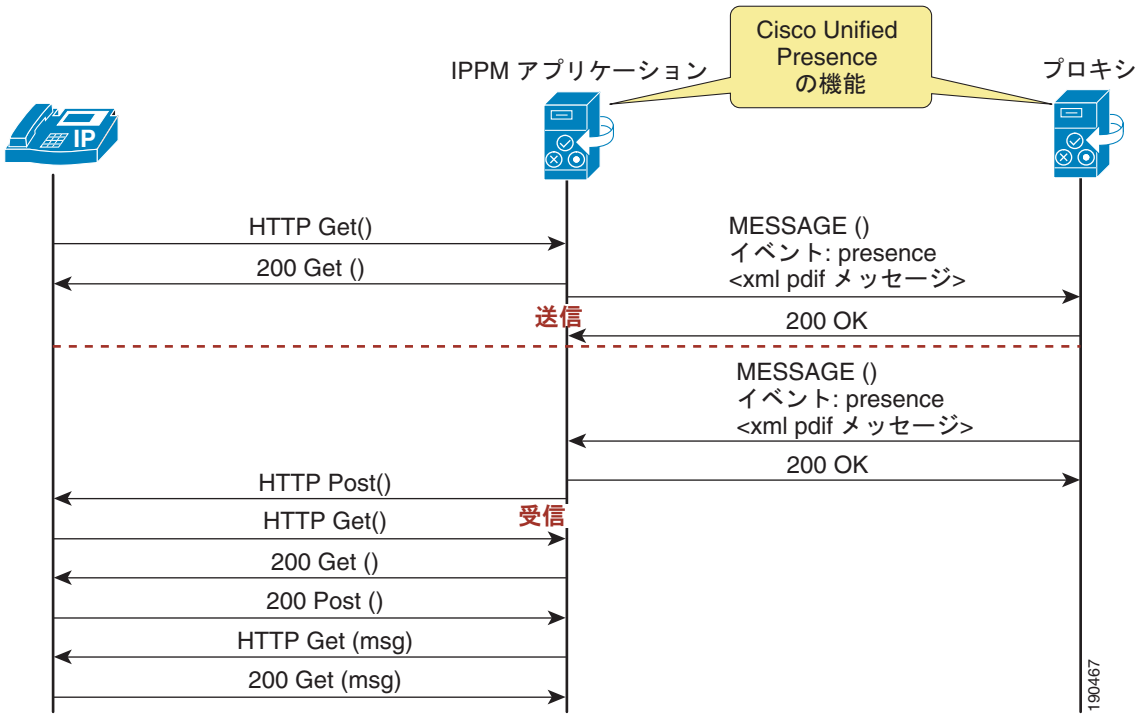
図 24-8　IPPM プロトコル変換とプレゼンス



IPPM アプリケーションは、次のインスタント メッセージング（IM）機能を提供します（図 24-9 を参照）。

- 電話機の HTTP インスタント メッセージを変換して、SIP MESSAGE メッセージを発信します。
- 着信の SIP MESSAGE メッセージを HTTP インスタント メッセージに変換して電話機に出力します。
- バディ情報の画面または IM の画面から、バディにダイヤルバックできます。
- 電話機（Phone Messenger Service）から、メッセージ履歴が管理できます。
- ユーザは、システム全体または個人的な定型文の IM メッセージを設定したり、メッセージを作成したりできます。

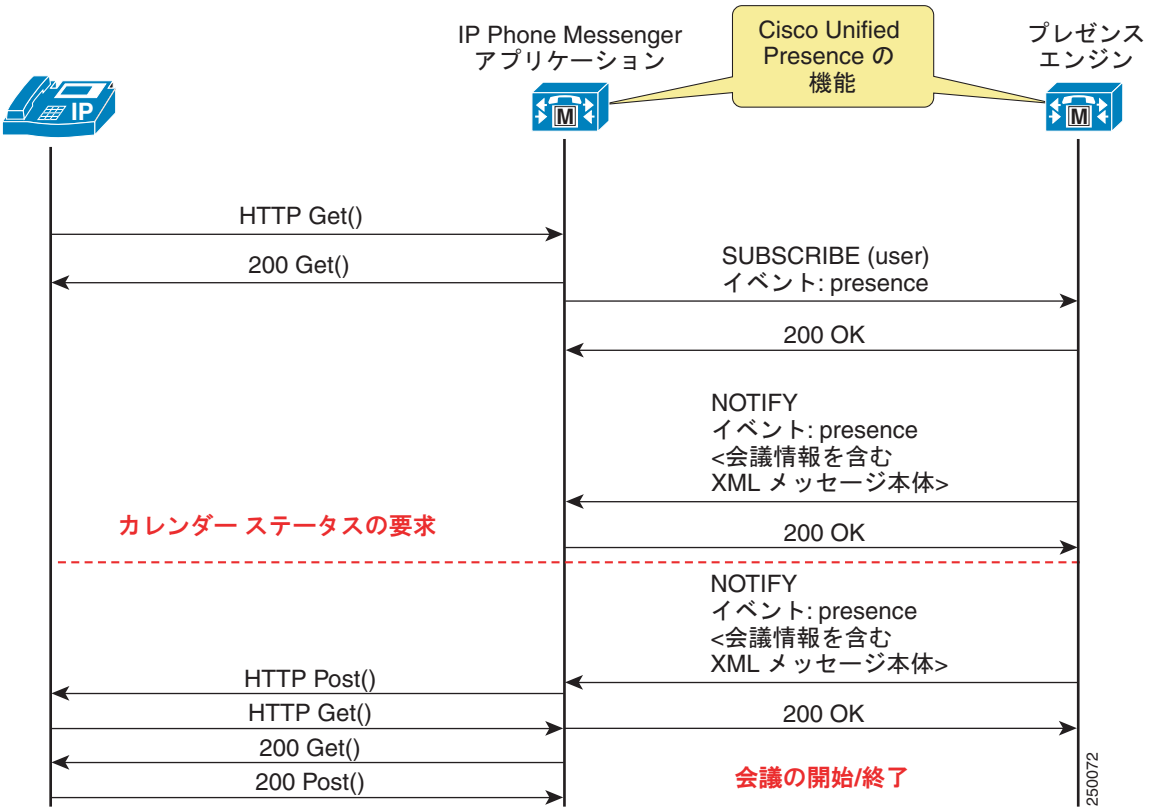
図 24-9　IPPM プロトコル変換とインスタント メッセージ



IPPM アプリケーションは、次の会議通知機能を提供します（図 24-10 を参照）。

- ユーザはデスクトップ カレンダー クライアントにログインすることなく、Cisco Unified Presence から登録済みの IPPM 電話機宛てに対し、会議のリマインダを送信できます。
- （参加、ダイヤル、またはコールバックにより）IPPM サービスから会議に参加できる機能が用意されています。
- 会議のリマインダ機能をブロックするかどうかは、エンド ユーザ用設定ページから制御できます。
- ユーザは、会議の参加者リストを会議の詳細画面に表示できます。これにより、IPPM モジュールからプレゼンス エンジンに、参加者のプレゼンス ステータスを照会する SUBSCRIBE メッセージが参加者ごとに送信されます。これで、現在の対応可能性に基づいて、参加者リストに記載されているユーザに、会議のリマインダとインスタント メッセージを送信できます。

図 24-10　IPPM プロトコル変換と会議の通知



Cisco IP Phone Messenger をサポートしている電話機モデルのリストについては、次の URL で入手可能な『*Hardware and Software Compatibility Information for Cisco Unified Presence*』を参照してください。

http://www.cisco.com/en/US/products/ps6837/products_device_support_tables_list.html

Cisco IP Phone Messenger のハイ アベイラビリティ

Cisco Unified Communications システムの現在の IP 電話サービスには、IP アドレスまたは HTTP Service URL の DNS A レコード エントリが設定されていますが、IP 電話サービスが冗長性が設定されていない場合、これがシングル ポイント障害になる可能性があります。

IP 電話サービスの冗長性が設定されていない場合、IP Phone Messenger 配置は、Cisco Unified Presence パブリッシャおよびサブスクライバの両方にわたって設定して、ロードバランスする必要があります。

次の例に示すように、Unified CM で、IP Phone Messenger に対して、Cisco Unified Presence パブリッシャを使用する電話サービスと、Cisco Unified Presence サブスクライバを使用するサービスの 2 つを設定します。

- PhoneMessenger1：

  http://publisher.cups.com:8081/ippm/default?name=#DEVICENAME#

- PhoneMessenger2:

  http://subscriber.cups.com:8081/ippm/default?name=#DEVICENAME#

Cisco IP Phone Messenger を使用して、次のいずれかの方法で、Cisco Unified IP Phones を配置できます。

- シングル電話サービス

  シングル電話サービスでは、Cisco Unified IP Phone の半分が Cisco Unified Presence パブリッシャを指し（上の例の PhoneMessenger1）、残りの半分が Cisco Unified Presence サブスクライバを指す（上の例の PhoneMessenger2）ように設定します。

  利点：管理者が設定によって IP Phone Messenger ユーザをロードバランスできます。

  欠点：その電話機が動作する Cisco Unified Presence サーバに障害が発生した場合、ユーザが IP Phone Messenger サービスを利用できなくなります。

- デュアル電話サービス

  デュアル電話サービスでは、すべての Cisco Unified IP Phone が 2 つの IP Phone Messenger サービスを持つように設定します（上の例では、PhoneMessenger1 と PhoneMessenger2 の両方）。

  利点：その電話機が動作する Cisco Unified Presence サーバに障害が発生した場合、ユーザは、2 番めのサーバ上で動作する IP Phone Messenger サービスの使用を試みることができます。

  欠点：この方法では、Services メニューからどの IP Phone Messenger サービスを選択するかが、電話のユーザに委ねられています。この方法は、どちらかの Cisco Unified Presence サーバを選択するユーザが他方を選択するユーザより多くなり、その結果、片方の Cisco Unified Presence サーバにユーザが偏る可能性があります。

次の例に示すように、IP Phone Services の冗長性を使用すれば（「IP Phone Service のハイ アベイラビリティ」（P.19-6）を参照）、IP Phone Messenger を、サーバ ロード バランサ（SLB）IP アドレスを使用する単一の電話サービスとして Unified CM 上に設定できます。

- PhoneMessenger:

  http://*slb_ip_address*:8081/ippm/default?name=#DEVICENAME#

Cisco IP Phone Messenger のキャパシティ プランニング

ユーザのメッセージ履歴と連絡先リストは、いずれも Cisco Unified Presence データベースに保存され、大量のデータが含まれる可能性があります。ユーザが IP Phone Messenger アプリケーションにログインするたびに、メッセージ履歴や連絡先リストがダウンロードされます。したがって、帯域幅に不安がある場合は、Cisco Unified Presence の管理ページで [IP Phone Messenger] の下の [Max Instant Message History Size] と [Max Contact List Size] を設定して、メッセージ履歴のサイズと連絡先リスト サイズを制限できます。

ユーザは、Session Timer パラメータを設定して、ユーザが現在のセッションにログインしている時間を制御したり、Refresh Interval パラメータを設定して、プレゼンス ステータスが更新される比率を制御したりできます。現在、管理者はこれらのパラメータを制御することができないので、デフォルト設定（Session Timer = 480 分、Refresh Interval = 30 分）が使用される可能性が最も高いと考えられます。

その他のリソースおよびドキュメンテーション

『*Cisco WebEx Connect Administrator's Guide*』は、次の Web サイトで入手できます。

http://www.webex.com/webexconnect/orgadmin/help/index.htm

Cisco WebEx Connect のエンド ユーザ向けガイドは、次の Web サイトで入手できます。

http://www.webex.com/webexconnect/help/wwhelp/wwhimpl/js/html/wwhelp.htm

CHAPTER 25

モバイル ユニファイド コミュニケーション

モバイル ユニファイド コミュニケーションを使用すれば、モバイル ワーカーはどこからでも会社の IP コミュニケーション環境の機能を利用できます。モバイル ユニファイド コミュニケーション ソリューションを使用すると、モバイル ユーザはビジネス コールをさまざまなデバイスで扱うことができ、オフィスビル内の移動中やオフィス間の移動中、地理的に会社外のロケーション間の移動中に企業アプリケーションにアクセスできます。モバイル ユニファイド コミュニケーション ソリューションでは、モバイル ワーカーは持続的に到達可能性を得ることができ、さまざまな場所での移動中や作業中の生産性を向上させることができます。

Unified Communications のモビリティ ソリューションは、主に次の 2 つのカテゴリに分けられます。

- 社内型モビリティ

  このタイプのモビリティは、企業の敷地内での移動に限られます。

- 社外型モビリティ

  このタイプのモビリティは、企業インフラストラクチャの外部にまで至るモビリティを指し、一般には何らかの形のインターネット、モバイル ボイス ネットワーク、およびモバイル データ ネットワーク通過が含まれます。

社内型モビリティは、企業のネットワーク境界内に使用が制限されます。この境界は単一の物理的な建物のみを範囲としても、近くの、あるいは離れた複数の物理的な建物を範囲としても、またはホーム オフィスまで広がったネットワーク インフラストラクチャの場合、企業により制御され管理されるホーム オフィスを範囲としてもかまいません。

一方、社外型モビリティには、企業インフラストラクチャによるインターネットまたはモバイル プロバイダー インフラストラクチャへのブリッジングが含まれ、ユーザは公共およびプライベート ネットワークを使用して企業サービスに接続できます。これらの 2 つのタイプのモビリティ間の線引きはあいまいな場合もあり、特にモバイル デバイスが、インターネットまたはモバイル データおよびモバイル ボイス ネットワークを介したユニファイド コミュニケーション サービスで企業に接続するようなシナリオの場合に顕著です。

社内型モビリティは、機能セットおよびソリューションに基づき、次の 3 つの主要な領域に分けられます。

- キャンパス / 単一サイト モビリティ

  このタイプの企業モビリティでは、ユーザの移動は、一般に単一の IP アドレス空間および公衆網入出力境界により区切られた単一の物理ロケーション内になります。このタイプのモビリティには、1 つの物理ネットワーク ポートから他のポートへの電話の移動や、ワイヤレス インフラストラクチャ アクセス ポイント間でのワイヤレス LAN デバイスのローミング、ユーザが一時的に異なる領域への特定の電話機に企業電話番号などのデバイス プロファイルを適用する Cisco Extension Mobility（EM; エクステンション モビリティ）などの操作や機能が含まれます。

- マルチサイト モビリティ

  このタイプのモビリティでは、ユーザは企業内の 1 つの物理ロケーションから他のロケーションに移動します。この移動には、一般的に IP アドレス空間の交差や公衆網入出力境界も含まれます。このタイプのモビリティには、キャンパス モビリティと同じタイプの操作や機能（物理的なハードウェアの移動、WLAN ローミング、Cisco エクステンション モビリティ）が含まれますが、それらは企業内のそれぞれのサイトに複製されます。さらに、デバイス モビリティ機能を利用して、ユーザがサイト間でデバイスを移動させると、電話のコールがローカル サイトの出力ゲートウェイを介してルーティングされ、メディア コーデックが適切にネゴシエートされ、コール アドミッション制御メカニズムでデバイスの場所が認識されるようにできます。

- リモート サイト モビリティ

  このタイプのモビリティでは、ユーザは社外のロケーションに移動しても、仮想的に企業ネットワークをリモート ロケーションまで拡張して、何らかの安全な形式で会社に接続できます。このタイプのモビリティは一般に、Cisco Virtual Office や、VPN ベースの電話機や Office Extend Access Point 機能などのその他のリモート接続方法などの、リモート テレワーカーに対するソリューションが含まれます。

社外型モビリティは、大まかに次の 4 つの Cisco ソリューション セットに分けられます。

- Cisco Unified Mobility

  Cisco Unified Communications Manager（Unified CM; ユニファイド コミュニケーション マネージャ）の一部である Cisco Unified Mobility 機能スイートにより、モバイル ユーザの会社の番号をユーザのモバイルまたはリモート デバイスに関連付け、企業ネットワーク上のユーザの固定の会社のデスクトップフォンと、モバイル ボイス プロバイダー ネットワーク上のユーザのモバイル デバイスとを接続できます。このタイプの機能は、固定モバイル コンバージェンスと呼ばれることがあります。

- デュアルモードの電話機とクライアント

  デュアルモードの電話機とデバイスには、802.11 ワイヤレス LAN ネットワークと携帯電話音声およびデータ ネットワークの両方に接続できる二重無線アンテナが装備されています。これらのデバイスに配置されたデュアルモード クライアントにより、Unified CM に企業ワイヤレス LAN 経由で関連付けることができ、その後企業の IP テレフォニー インフラストラクチャを発信および着信に利用できます。モバイル ユーザがこれらのデバイスを持って会社の外に移動した場合、モバイル ボイス プロバイダー ネットワークを使用して電話のコールが発着信されます。

- Cisco Unified Mobile Communicator

  Cisco Unified Mobile Communicator ソリューションを使用すると、企業用のさまざまな Unified Communications アプリケーションにユーザのモバイル デバイスからリモート アクセスできます。安全なモバイル データ接続を介して企業に接続し、Cisco Unified Mobile Communicator クライアントが企業のモビリティ機能やルーティング、ボイスメール、プレゼンス サービスにアクセスします。

- ダイレクト コネクト モバイル クライアント

  ダイレクト コネクト モバイル クライアントを使用した場合も、企業用の音声およびコラボレーション アプリケーションや、コール ルーティング、社内ディレクトリ アクセス、ならびにプレゼンスおよびインスタント メッセージング サービスなどのサービスにユーザのモバイル デバイスからリモート アクセスできます。これらのクライアントはデュアルモード機能も提供し、企業の WLAN ネットワークに接続したときの Voice over WLAN 機能を有効にします。

特に断りがない限り、この章で説明するさまざまなアプリケーションと機能は、すべての Cisco Unified Communications 配置モデルに適用されます。

この章ではまず、モビリティ機能と企業インフラストラクチャ内で利用可能なソリューションについて説明します。これには、キャンパス / 単一サイトの配置、マルチサイトの配置、さらにはリモート サイトの配置での、機能検証や設計上の考慮事項が含まれます。この一連の包括ソリューションは、企業ク

ラスのコミュニケーションや物理ロケーションに関係しない生産性の改善などを含め、社内のモバイル ワーカーに多くの利点をもたらします。この社内型モビリティに関する説明を踏まえて、モバイル プロバイダーおよびインターネット プロバイダーのインフラストラクチャおよび機能を活用した、社外型モビリティ ソリューションを検証します。これらのソリューションにより、安定した企業モビリティ インフラストラクチャの上に構築できる高度なモバイル機能とコミュニケーション フローを活用するための企業ネットワーク インフラストラクチャとプロバイダー ネットワーク インフラストラクチャのモバイル機能のブリッジングが可能になります。

この章では、企業用の Unified Communications モビリティ ソリューションのモビリティ アーキテクチャ、機能性、および設計と配置の示す意味について包括的に検証します。この章の分析と説明は、大まかに次のような構成になっています。

- 社内型モビリティ
  - 「キャンパス企業モビリティ」（P.25-5）
  - 「マルチサイト企業モビリティ」（P.25-12）
  - 「リモート企業モビリティ」（P.25-31）
- 社外型モビリティ
  - 「Cisco Unified Mobility」（P.25-37）
  - 「デュアルモードの電話機とクライアント」（P.25-64）
  - 「Cisco Unified Mobile Communicator」（P.25-85）
  - 「ダイレクト コネクト モバイル クライアント」（P.25-99）

この章の新規情報

表 25-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 25-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
細部の訂正および変更	この章の各項で説明	2011 年 7 月 29 日
Android デバイス対応の Cisco Jabber 8.6 デュアルモード クライアント	「デュアルモードの電話機とクライアント」（P.25-64）	2011 年 6 月 2 日
Cisco Mobile 8.5 for Nokia クライアントのサポートを含む、ダイレクト コネクト モバイル クライアント ソリューション	「ダイレクト コネクト モバイル クライアント」（P.25-99）	2011 年 6 月 2 日
モバイル トール バイパスの最適化機能	「モバイル トール バイパスの最適化」（P.25-106）	2011 年 6 月 2 日
セッション再開機能（以前の Dial-via-office 転送リダイヤル）	「セッション再開」（P.25-106）	2011 年 6 月 2 日
Cisco Mobile iPhone デュアルモード クライアントのデスクトップフォンの統合	「デュアルモード クライアント：Cisco Mobile および Cisco Jabber」（P.25-71）	2010 年 11 月 15 日
企業キャンパス、マルチサイト、およびリモート モビリティ ソリューションおよび機能	「社内型モビリティ」（P.25-5）	2010 年 11 月 15 日
元のデバイス モビリティの章はこのバージョンの SRND から削除され、内容は「モバイル ユニファイド コミュニケーション」のこの章に統合されました。	「デバイス モビリティ」（P.25-15）	2010 年 11 月 15 日

表 25-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報（続き）

新規トピックまたは改訂されたトピック	説明箇所	改訂日
エンタープライズ機能アクセス 2 ステージ ダイヤリング機能オートメーションが Nokia Call Connect デュアルモード クライアントで利用可能になりました。	「デュアルモード クライアント：Nokia Call Connect」（P.25-77）	2010 年 7 月 23 日
Cisco Mobile iPhone デュアルモード クライアントのハンドアウトのハンドオフ番号方式	「デュアルモード クライアント：Nokia Call Connect」（P.25-77）	2010 年 7 月 23 日
Cisco Mobile iPhone デュアルモード クライアントの AP-to-AP ローミングに関する WLAN 設計ガイドライン	「Cisco Mobile iPhone および Cisco Jabber Android デュアルモード クライアントの WLAN 設計上の考慮事項」（P.25-76）	2010 年 7 月 23 日
Nokia Call Connect デュアルモード クライアントのハンドオフと AP-to-AP ローミングに関する WLAN 設計ガイドライン	「Nokia Call Connect デュアルモード クライアントの WLAN 設計上の考慮事項」（P.25-80）	2010 年 7 月 23 日
Cisco Mobile iPhone デュアルモード クライアントおよび Nokia Call Connect デュアルモード クライアントのサポートを含む、デュアルモード電話機のソリューション	「デュアルモードの電話機とクライアント」（P.25-64）	2010 年 4 月 2 日
企業内から発信され、発信先がリモート接続先番号やモビリティ ID 番号のコールのモビリティ コール アンカリングを行う Intelligent Session Control 機能	「Cisco Unified Mobility のダイヤル プランに関する考慮事項」（P.25-56）	2010 年 4 月 2 日
*74（デフォルトの機能アクセス コード）を使用した新しい通話切替セッション ハンドオフ機能、およびデスクトップフォンのピックアップ操作の意味	「デスクトップフォンのピックアップ」（P.25-40）	2010 年 4 月 2 日
Cisco Unified Communications Manager Business Edition（Unified CMBE）の Unified Mobility キャパシティ プランニング情報	「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）	2010 年 4 月 2 日

社内型モビリティ

この項では、社内で使用可能なモビリティ機能およびソリューションについて検証します。この検証には、次のタイプの企業モビリティのアーキテクチャ、機能性、および設計と配置の意味に関する説明が含まれます。

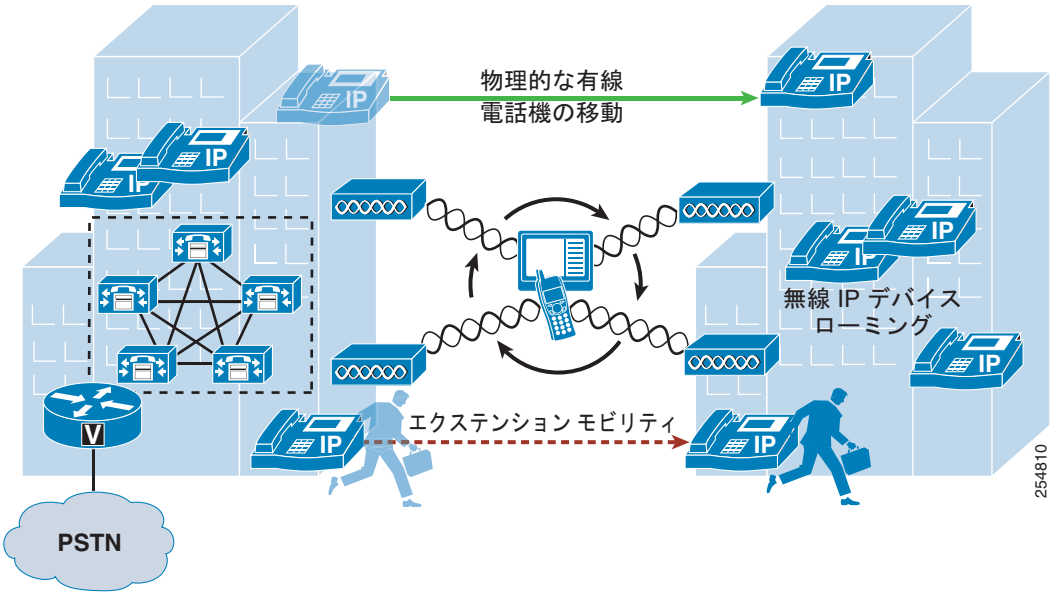
キャンパス企業モビリティ

キャンパスまたは単一サイトの企業モビリティは、一般に単一の IP アドレス空間および公衆網入出力境界により区切られた単一の物理ロケーション内のモビリティを指します。ここでのモビリティには、この物理ロケーション内でのユーザの移動だけではなく、エンドポイント デバイスの移動も含まれます。

キャンパス企業モビリティのアーキテクチャ

図 25-1 に示すように、キャンパス企業モビリティのアーキテクチャは、（図のように）近接する単一の建物または複数の建物を含む単一の物理ロケーションに基づいており、ユーザはキャンパス内を自由に移動でき、IP および公衆網接続を維持できます。一般にキャンパス配置には、アドレス空間および公衆網入出力境界によって区切られた公衆網およびインターネット プロバイダー ネットワークへの、単一 IP 共有一般接続または接続セットが含まれます。この企業キャンパス内のすべてのユーザは、一般ネットワーク インフラストラクチャに接続され、一般ネットワーク インフラストラクチャから到達可能です。

図 25-1　　キャンパス企業モビリティのアーキテクチャ



キャンパス モビリティのタイプ

企業キャンパス内のモビリティには一般的に、デバイス、ユーザ、またはその両方のキャンパス インフラストラクチャ全体の移動が含まれます。Cisco Unified Communications 展開内のキャンパス企業モビリティは主に、有線電話機の物理的な移動、ワイヤレス デバイスの移動、電話機や通話ソフトウェアを持たないユーザのみの移動の 3 つに分けられます。移動のタイプについては後で説明します。

物理的な有線デバイスの移動

図 25-1 に示すように、物理的な有線電話機の移動は、キャンパス インフラストラクチャ内で簡単に行えます。このタイプの電話機の移動は、建物の単一階内、建物の複数階にわたって、またはキャンパス内の建物間で発生することが考えられます。従来の、物理的な電話機のポートが特定のオフィス、パーティション、または建物内のその他の空間に固定されている PBX 配置とは異なり、IP テレフォニーの配置では、電話はネットワーク インフラストラクチャの任意の IP ポートにつないで IP PBX に接続できます。

Cisco 環境では、これは単に Cisco Unified IP Phone をネットワークから取り外し、キャンパス内の他の場所に運んで他の有線ネットワーク ポートに接続するだけということです。新しいネットワーク ロケーションに接続すると、この電話が Unified CM に再登録され、前のロケーションと同じように発信や着信ができます。

物理デバイスのこれと同じ移動は、有線 PC で実行するソフトウェアベースの電話にも適用されます。たとえば、Cisco IP Communicator または Cisco Unified Personal Communicator を実行しているラップトップ コンピュータを、キャンパス内のあるロケーションから別のロケーションへ移動でき、ラップトップを新しいロケーションのネットワーク ポートに接続すると、ソフトウェアベースの電話を Unified CM を再登録して、電話のコール処理を再開できます。

キャンパス内の物理的なデバイス モビリティに対応するには、電話デバイスやソフトウェアベースの電話を実行しているコンピュータを物理的に移動する際は、新しいロケーションで使用されるネットワーク接続の IP 接続、接続速度、サービス品質、セキュリティ、およびインライン パワーや Dynamic Host Control Protocol（DHCP; 動的ホスト制御プロトコル）などのネットワーク サービスが前の場所のものと同じであるよう注意してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下し、場合によっては、機能が完全に失われます。

ワイヤレス デバイスのローミング

キャンパス エッジでワイヤレス ネットワークに接続できるようワイヤレス LAN ネットワークが展開されている場合、ワイヤレス デバイスは、図 25-1 で示すように、企業キャンパス全体を移動またはローミングできます。

ワイヤレス デバイスの例としては、Cisco Unified Wireless IP Phone 7925G、無線で接続された Cisco Unified IP Phone 9971、Cisco Cius、Cisco Mobile 8.5 for Nokia などのダイレクト コネクト モバイル クライアント（「ダイレクト コネクト モバイル クライアント」（P.25-99）を参照）、および Cisco Mobile 8、Cisco Jabber 8.6、Nokia Call Connect などのデュアルモード電話機クライアント（「デュアルモードの電話機とクライアント」（P.25-64）を参照）などが挙げられます。

WLAN ネットワークは、1 箇所以上のワイヤレス Access Point（AP; アクセス ポイント）から構成されます。ワイヤレス AP は、ワイヤレス デバイスに対してワイヤレス ネットワーク接続を提供します。ワイヤレス AP は、ワイヤレス ネットワークと有線ネットワークとの間の境界ポイントとなります。ネットワークのカバー領域および容量を拡張するために、物理的なネットワーク敷設領域に複数の AP が分散して配置されます。

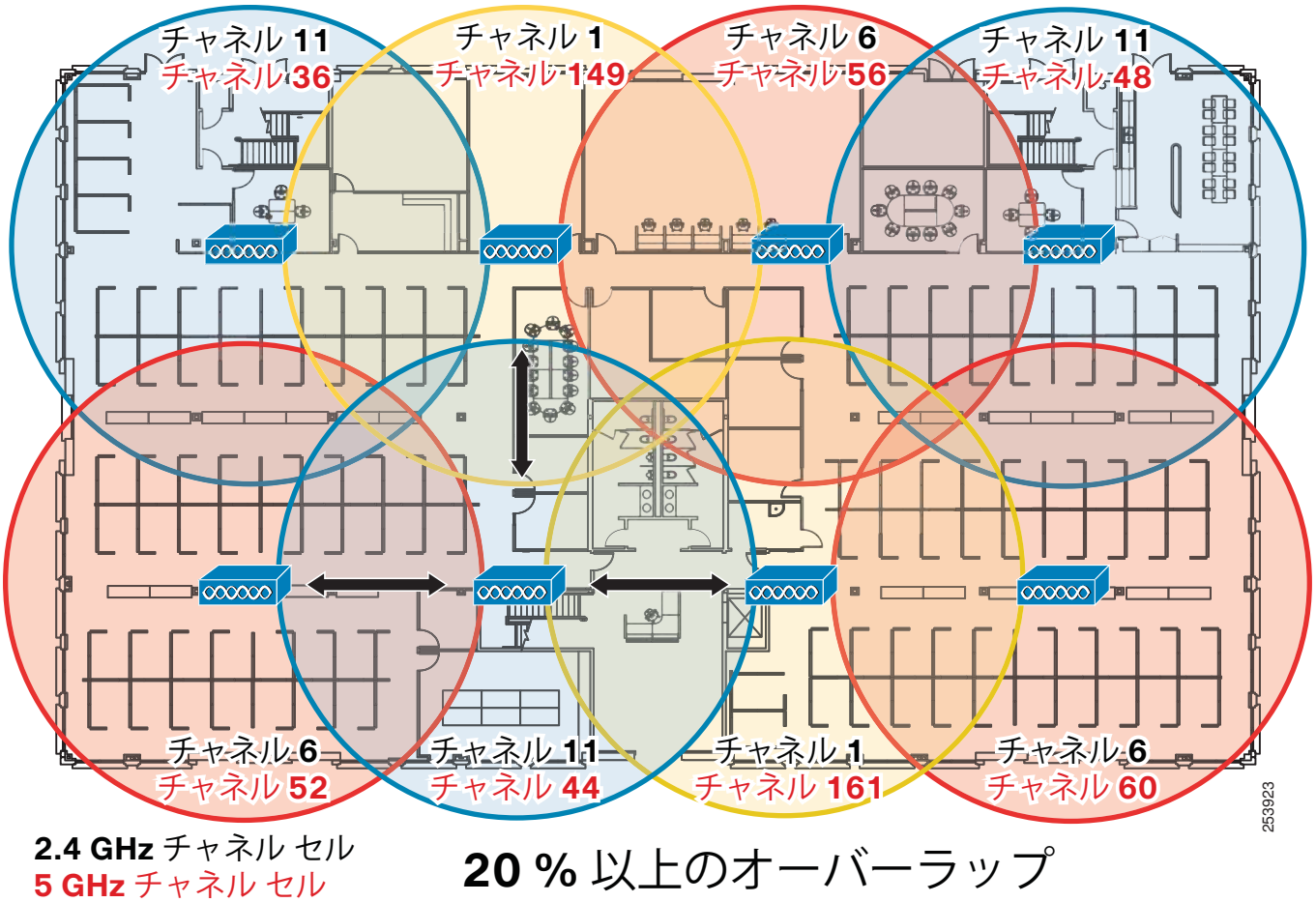
無線電話は、基礎となる WLAN インフラストラクチャに依存して重要なシグナリングとリアルタイム音声メディア トラフィックの両方を伝送するため、データ トラフィックとリアルタイム音声トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワーク

の配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように展開された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、ワイヤレス電話機を配置する場合は、Voice over WLAN（VoWLAN）の配置が正常に行われるように、配置前、配置中、配置後に WLAN Radio Frequency（RF; 無線周波数）実地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。

AP は、ネットワーク内に自律的に配置して、各 AP が他のすべての AP とは独立して設定、管理、および運用されるようにすることも、WLAN コントローラによってすべての AP が設定、管理、および制御されるように管理して配置することもできます。後者の方法において、WLAN コントローラは、AP の管理、および AP 設定と AP 間ローミングの処理を担当します。いずれの場合も、VoWLAN が正常に配置されるには、次の一般的なガイドラインに従って AP を配置する必要があります。

- 図 25-2 に示すように、隣接していない WLAN AP チャネル セルは、20 % 以上オーバーラップする必要があります。このようにオーバーラップさせることによって、ワイヤレス デバイスがキャンパス ロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。2 つの AP 間で正常にローミングしたデバイスは、音声品質や音声パスに目立った変更なしにアクティブな音声コールを維持できます。

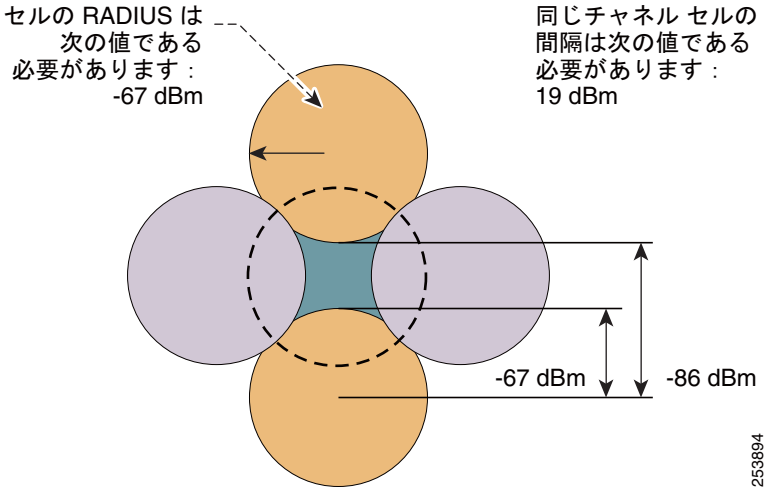
図 25-2　　WLAN チャネル セル オーバーラップ



- 図 25-3 に示すように、WLAN AP チャネル セルは、-67 デシベル / ミリワット（dBm）のセル パワーレベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。

  約 -67 dBm（またはそれ未満）のセル半径にすることで、リアルタイムの音声トラフィックで問題となるパケット損失を最小限に抑えることができます。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。セル半径についての -67 dBm のガイドラインは、2.4 GHz（802.11b/g）と 5 GHz（802.11a）の両方の配置に該当します。

図 25-3　　WLAN セル半径および同一チャネル セル分離



（注） 19 dBm の同一チャネル セル分離は、単純化されたものであり、理想的な状態を示しています。ほとんどの配置においては、このような 19 dBm の分離を実現することができません。最も重要な RF 設計基準は、-67 dBm のセル半径と、セル間の 20 % 以上の推奨オーバーラップです。これらの制約を遵守して設計することによって、チャネルの分離が最適化されます。

無線ローミングは無線電話だけではなく、PC で実行するソフトウェアベースの電話にも適用されます。たとえば、ユーザは Cisco IP Communicator または Cisco Unified Personal Communicator を実行しているラップトップ コンピュータを使用して、キャンパス中を無線でローミングできます。

ほとんどのワイヤレス AP、無線電話、および無線 PC クライアントでは、企業の WLAN に安全にアクセスできるように、さまざまなセキュリティ オプションが用意されています。WLAN インフラストラクチャとワイヤレス電話機の両方でサポートされており、企業のセキュリティ ポリシーおよびセキュリティ要件に一致するセキュリティの方法を必ず選択してください。

Cisco Unified Wireless Network のインフラストラクチャの詳細については、「ワイヤレス LAN インフラストラクチャ」（P.3-57）を参照してください。Voice over WLAN 設計の詳細については、次の Web サイトで入手可能な『*Voice over Wireless LAN Design Guide*』を参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns820/landing_voice_wireless.html

エクステンション モビリティ（EM）

図 25-1 に示すように、有線およびワイヤレス電話機の物理的な移動に加え、ユーザ自身も電話機または PC ハードウェアを持たずにキャンパス インフラストラクチャ内を移動できます。これらの場合、ユーザの会社の電話番号および他の設定を含むプロファイルを適用することにより、ユーザは 1 つのデバイスから別のデバイスに、会社の内線番号または会社の番号を移動できます。

EM 機能により、ユーザはセキュリティ クレデンシャル（ユーザ ID および PIN 番号）のセットを使用して、キャンパス内にある IP 電話にログインできます。ログインすると、会社の電話番号やコール特権から設定したスピード ダイヤルまでを含めたユーザ個人のデバイス プロファイルが、ユーザがデバイスをログアウトするまで、またはログインのタイムアウトまで、一時的にこの電話に適用されます。EM 機能は、Unified CM の一部として使用できます。

この機能は、会社の外でほとんどの時間を費やし、物理的に、オフィスには時々しかいないモバイル企業ユーザに特に役に立ちます。ホット シーティングまたはフリー シーティングと呼ばれることもあるこれらのタイプのモバイル ユーザに、一時的にオフィスのスペースを提供することで、システム管理者は頻度が低く一時的にしか IP 電話ハードウェアを使用する必要がない多数のモバイル ユーザに対応できます。

キャンパス内で EM を利用するには、Unified CM 管理者がユーザ デバイス プロファイルおよびユーザ クレデンシャルを設定し、EM 電話サービスへ IP 電話を登録する必要があります。

EM の詳細については、「エクステンション モビリティ」（P.19-8）を参照してください。

キャンパス企業モビリティのハイ アベイラビリティ

キャンパス企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するよう、冗長な方式で設定し配置する必要があります。

たとえば、有線の IP 電話およびソフトウェアベースの IP 電話を実行しているコンピュータを効率的にサポートするため、冗長で普及しているネットワーク接続またはポートが使用可能である必要があります。さらに、これらの冗長なネットワーク接続は、適切なセキュリティ、サービス品質、およびその他のネットワークベースの機能などの、有線デバイスのロケーションを移動しても最適な操作とボイス品質を確保できる適切な特性を備えたまま配置される必要があります。最終的には、正常なキャンパス モビリティの配置は、ネットワーク接続、公衆網接続、およびその他のアプリケーションやサービスが、ハイ アベイラビリティのある方式で配置されている場合にのみ可能です。

同様に、ワイヤレス デバイスを接続およびローミングするための WLAN ネットワークの配置や調整では、無線サービスに対するハイ アベイラビリティを考慮することも重要です。配置するデバイス数に対する弾力性と十分なカバレッジを確保するために、WAN ネットワークは、同一チャネル セルがオーバーラップすることなく、適切で冗長なセルによるカバレッジが保証されるように配置する必要があります。同一チャネル セルがオーバーラップしない十分なセル カバレッジ、および AP 間のローミングを容易に実行可能にするための異なるチャネル セルの十分なオーバーラップを提供することによって、ワイヤレス デバイスおよびクライアントに対するネットワーク接続でハイ アベイラビリティを確保できます。

最後に、EM をキャンパス内のユーザ モビリティに利用する場合、Unified CM クラスタ内の単一ノードの障害が Extension Mobility 機能の動作を妨げないよう、この機能を冗長な方式で配置する必要があります。可用性が高くなるような Cisco Extension Mobility の詳細については、「エクステンション モビリティのハイ アベイラビリティ」（P.19-15）を参照してください。

キャンパス企業モビリティのキャパシティ プランニング

キャンパス企業モビリティを正常に配置するには、これらのモビリティ機能とソリューションを使用するすべてのモバイル ユーザに対応できる十分なキャパシティを用意する必要があります。

有線デバイスおよびコンピュータの物理的な移動に対するキャパシティの考慮は、キャンパス ネットワーク インフラストラクチャ内で使用できるネットワーク ポート数に完全に依存しています。キャンパス内でデバイスを移動するユーザのため、それぞれのロケーションに、モバイル ユーザのデバイスの接続に使用できるある程度の数の使用可能なネットワークポートがある必要があります。ネットワークポートが不足してこの有線デバイスの移動に対応できないと、1 つのロケーションから別のロケーションへ物理的にデバイスを移動できないことになる可能性があります。

企業 WLAN 内にワイヤレス デバイスを配置し、ワイヤレス デバイス ローミングを利用する場合、WLAN インフラストラクチャのデバイスの接続性とコール キャパシティを考慮することも重要です。デバイス数またはアクティブ コール数の面でのキャンパス WLAN インフラストラクチャのオーバーサブスクリプションは、無線接続のドロップ、音声品質の低下、またはコール セットアップの遅延や失敗の原因となります。必要なコール キャパシティを処理するのに十分な数の AP を配置することによって、VoWLAN の配置においてオーバーサブスクリプションが発生する確率を大幅に減少できます。AP のコール キャパシティは、単一チャネル セル領域内でサポートできる同時 VoWLAN コール数に基づきます。VoWLAN のコール キャパシティの一般的なルールは次のとおりです。

- 802.11b または 802.11g（2.4 GHz）チャネル セルあたり最大 7 個の同時 VoWLAN コール。802.11b のみの配置、アクティブな 802.11b クライアントの数が非常に多い配置、または Bluetooth をイネーブルにした配置においては、802.11b/g（2.4 GHz）チャネル セルあたりの最大同時コール数は 4 個まで減少する場合があります。
- データ レート 24 Mbps 以上の Bluetooth を無効にした 802.11g（2.4 GHz）チャネル セルあたり最大 27 個の同時 VoWLAN コール。
- データ レート 24 Mbps 以上の 802.11a（5 GHz）チャネル セルあたり最大 27 個の同時 VoWLAN コール。

これらのコール キャパシティ値は、RF 環境、VoWLAN 無線ハンドセット機能、および基礎となる WLAN システム機能に大きく依存します。一部の配置では、実際のキャパシティはこれよりも小さくなることもあります。

（注）　同じ AP に関連付けられている 2 台のワイヤレス電話機間の単一のコールは、2 つの同時 VoWLAN コールであると見なされます。

EM のスケーラビリティは、Unified CM 内のログイン率およびログアウト率にほぼ依存します。ログインおよびログアウトの操作負荷がクラスタの 2 ノードに分散した場合、1 分あたり最大 375 回の順次ログインおよびログアウト操作が、1 つの Unified CM クラスタでサポートされます。Unified CM クラスタ サーバ ハードウェアによっては、配置のキャパシティがこれより少なくなる可能性もあります。したがって、十分なキャパシティがモバイル ユーザに提供できるよう、Unified CM クラスタ内で有効なエクステンション モビリティ ユーザ数と、キャンパス内を移動するユーザ数、任意の時間にこの機能を使用しているユーザ数を知ることが重要です。EM のキャパシティ プランニングの詳細については、「エクステンション モビリティのキャパシティ プランニング」（P.19-17）を参照してください。

いずれの場合も、キャンパス内の Unified CM クラスタには、有線デバイスかワイヤレス デバイスにかかわらず、移動されたデバイスに対するデバイス登録を処理する十分なデバイス登録キャパシティが必要です。もちろん、キャンパス全体で移動されているすべてのデバイスがすでにキャンパス ネットワーク内に配置済みの場合、Unified CM 内の十分なキャパシティは、デバイスの移動の前にすでに配置されているはずです。ただし、新しいデバイスをモビリティを目的として配置に追加する場合は、デバイス登録キャパシティを考慮する必要があり、必要に応じてさらにキャパシティを追加する必要があります。

最後に、Unified CM によって提供される多くの機能により、これらのモビリティ ソリューションの設定および配置はシステム全体のサイジングと関わっています。適切なシステム サイジングを確実に行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用して、エンドポイント デバイスや EM ユーザの数、Busy Hour Call Attempt（BHCA; 最繁時呼数）、配置されている CTI アプリケーションの数などあらゆる要素に基づいて、システムのキャパシティを決定します。このツールで提供されるサイジング ガイダンス全体に従えば、サポートされているキャパシティ制限内でこれらの機能および全体的なシステムを展開できます。Unified CST は、シスコの従業員およびパートナーだけが（適切なログイン認証を使用して）、http://tools.cisco.com/cucst より利用することが可能です。

キャンパス企業モビリティの設計上の考慮事項

キャンパス企業モビリティ機能を配置する際は、次の設計上の考慮事項に従ってください。

- キャンパス内の物理的なデバイス モビリティに対応するには、新しいロケーションで使用されるネットワーク接続の IP 接続（VLAN や VLAN 間ルーティングなど）、接続速度、サービス品質、セキュリティ、およびネットワーク サービス（インライン パワー、Dynamic Host Control Protocol（DHCP; 動的ホスト制御プロトコル）など）が前のネットワーク接続と同じタイプであることを確認してください。これらの接続パラメータ、サービス、および機能が同じでないと、機能が低下するか、場合によっては機能が完全に失われます。
- ワイヤレス IP デバイスやソフトウェアベース クライアントを展開する場合は、Voice over WLAN（VoWLAN）の展開が正常に行われるように、展開前、展開中、展開後に WLAN Radio Frequency（RF; 無線周波数）実地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。
- AP は、20 % 以上のセル オーバーラップを確保して配置する必要があります。このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。
- 単一の Unified CM ノードが失われた場合に機能の実行に悪影響が及ばないように、EM サービスは冗長性の高い方式で配置してください。EM サービスが重要な場合、Unified CM ノード障害を回避し可用性が高い機能を提供するためのサーバ ロード バランシング ソリューションを考えます。EM のハイ アベイラビリティの詳細については、「エクステンション モビリティのハイ アベイラビリティ」（P.19-15）を参照してください。
- キャンパス ネットワークのワイヤレス音声コールのキャパシティは十分に用意してください。そのためには、無線ユーザの BHCA レートに基づき、目的のコール キャパシティの処理に適した数のワイヤレス AP を展開します。各 802.11g（2.4 GHz）または 802.11a（5 GHz）チャネル セルは、24 Mbps 以上のデータ レートで 27 個の同時コールをサポートできます。802.11g 配置では、このキャパシティを実現するには Bluetooth を無効にする必要があります。各 802.11b または 802.11g（2.4 GHz）チャネル セルは、最大 7 個の同時コールをサポートできます。ただし、802.11b のみの配置では、802.11b クライアントの数が非常に多い配置、または Bluetooth を使用した配置の場合、チャネル セルの最大キャパシティは 4 個の同時コールまで下がる場合があります。
- 1 分あたり最大 375 回の順次ログインまたはログアウトが単一の Unified CM クラスタでサポート可能です。最大 2 つの Unified CM サブスクライバ ノードが、アクティブに EM ログインを処理できます。EM のキャパシティの詳細については、「エクステンション モビリティのキャパシティ プランニング」（P.19-17）を参照してください。

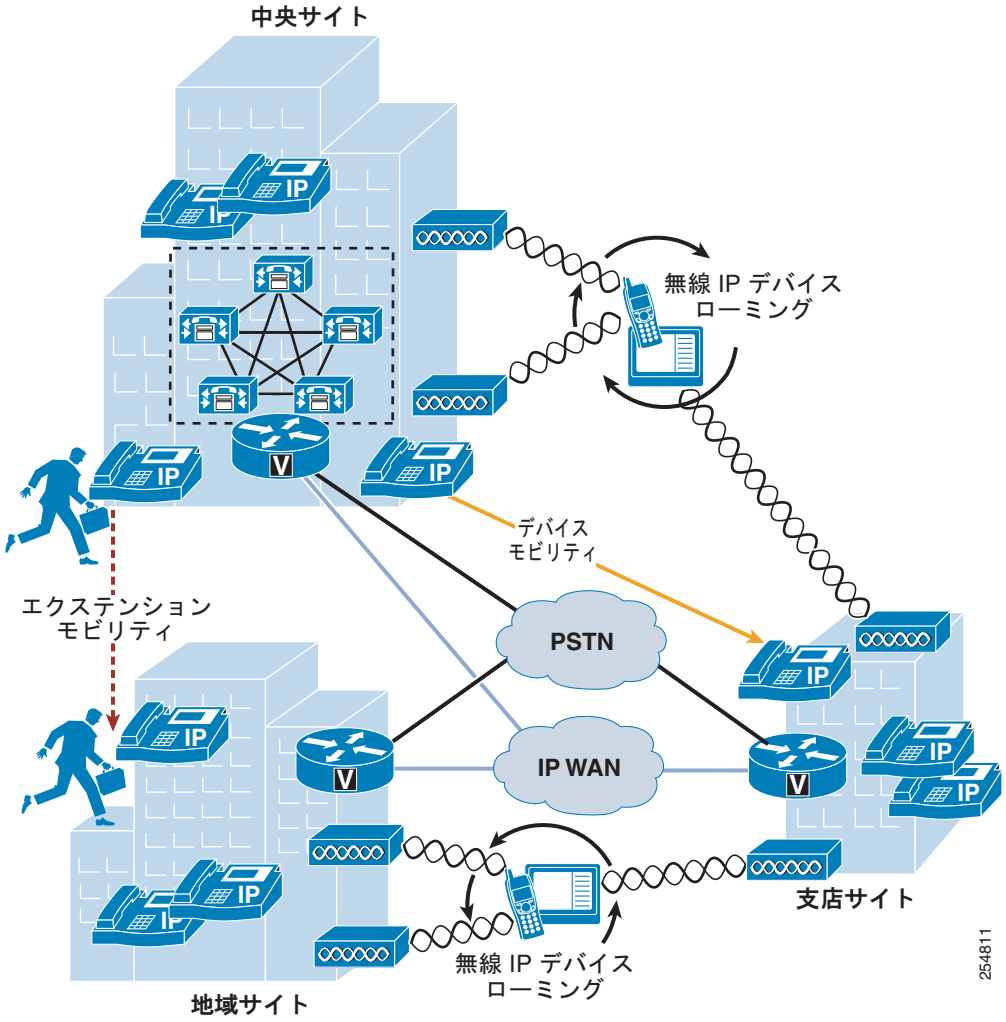
マルチサイト企業モビリティ

マルチサイト企業モビリティとは、複数の物理ロケーションがあり、それぞれが一意の IP アドレス空間および公衆網入出力境界を持つ社内でのモビリティを指します。この場合のモビリティには、ユーザやエンドポイント デバイスの各物理ロケーション内の移動だけではなく、サイトおよびロケーション間のユーザやエンドポイント デバイスの移動も含まれます。

マルチサイト企業モビリティのアーキテクチャ

図 25-4 に示すように、マルチサイト企業モビリティのアーキテクチャは、地理的に離れた 2 つ以上のロケーションまたはサイトに基づいています。ユーザとデバイスの数が多い中央またはキャンパス サイトから、ユーザとデバイスの数が少なめの中規模の地域サイト、それよりも小規模な支社サイトまで、サイトの規模は異なってもかまいません。一般にマルチサイト企業配置は、サイトを相互接続する IP WAN リンクや、各ロケーションでのローカル公衆網入出力で構成されています。さらに多くの場合、サイト間のネットワーク障害中でも機能を維持するため、重要なサービスはそれぞれの物理サイトに複製されています。モビリティの観点からは、ユーザとそのデバイスはサイト内またはサイト間で移動できます。

図 25-4　マルチサイト企業モビリティのアーキテクチャ



（注）　図 25-4 では、集中コール処理を使用するマルチサイト配置（中央サイト内にある単一 Unified CM クラスタから明らか）を示していますが、マルチサイト企業モビリティの配置と同じ設計および配置の考慮が、分散型コール処理環境に適用されます。分散型コール処理環境で配置された場合のモビリティ機能の動作の違いについて、以降で説明します。

マルチサイト企業モビリティのタイプ

マルチサイト企業モビリティ配置には、デバイス、ユーザ、またはその両方の単一サイト内での移動だけではなく、サイト間のユーザおよびデバイスの移動も含まれます。

キャンパス / 単一サイト企業配置でサポートされているタイプと同じモビリティ機能とソリューションが、マルチサイト配置の単一サイト内でのユーザやデバイスのサイト内移動に適用されます。これらには、有線電話機の物理的な移動、無線電話ローミング、およびエクステンション モビリティが含まれます。これらのタイプのモビリティソリューションおよび機能の詳細については、「キャンパス企業モビリティ」（P.25-5）を参照してください。

マルチサイト配置でのサイト内モビリティでも、これらのモビリティ機能が同じようにサポートされます。ただし、2 つ以上のサイト間に適用される場合の機能との主な違いとして、これらの機能はデバイス モビリティ機能により拡張されます。デバイス モビリティ機能では、企業ネットワークに接続するときにデバイスが使用する IP アドレスを基にしたダイナミックなロケーション認識メカニズムが提供されます。

物理的な有線デバイスの移動

物理的な有線電話機の移動は、マルチサイト配置の各サイト内でも、サイト間でも簡単に対応できます。キャンパス / 単一サイト配置と同様、マルチサイト配置の単一サイトに制限された有線デバイスの移動は、Cisco Unified IP Phone をネットワークから外し、サイト内の別のロケーションに移動して、別の有線ネットワーク ポートに接続するだけです。新しいネットワーク ロケーションに接続すると、この電話が Unified CM に再登録され、前のロケーションと同じように発信や着信ができます。

マルチサイト配置でのサイト間またはロケーション間の有線デバイスの移動も、基本的には同じ形です。ただし、このタイプのモビリティと組み合わせた場合、デバイス モビリティ機能により、デバイスが移動先の新しいロケーションで再登録されると、適切にコール アドミッション制御が動作し、ゲートウェイおよびコーデックが選択されます。この機能の詳細については、「デバイス モビリティ」（P.25-15）を参照してください。

ワイヤレス デバイスのローミング

各サイトで使用できる、ワイヤレス ネットワークに接続するためのワイヤレス LAN ネットワーク インフラストラクチャが使用可能な場合、単一サイトのキャンパス展開と同様、ワイヤレス デバイスは、図 25-4 に示すように、マルチサイト企業展開全体を移動またはローミングできます。しかし、サイト間の有線電話機の移動と同様ワイヤレス デバイスでも、コールの発着信の際に正しいゲートウェイおよびコーデックが確実に使用されるよう、またコール アドミッション制御が帯域幅を適切に管理するよう、デバイス モビリティ機能が展開されなければなりません。この機能の詳細については、「デバイス モビリティ」（P.25-15）を参照してください。

分散型コール処理環境では、有線電話機と同様、コール ルーティングに伴う問題が発生する可能性を避けるため、単一の Unified CM クラスタのみに登録するようワイヤレス デバイスを設定する必要があります。

エクステンション モビリティ（EM）

単一サイト内での EM のサポートに加え、図 25-4 に示すように、この機能はサイト間でもサポートされ、ユーザが企業内のサイト間を移動して、各ロケーションで電話機にログインできます。

また、ユーザが異なる Unified CM クラスタのサイト間や電話間を移動する場合、EM も分散型コール処理の配置でサポートされます。分散型コール処理環境でエクステンション モビリティをサポートするには、Cisco Extension Mobility Cross Cluster（EMCC; クラスタ間のエクステンション モビリティ）機能を設定する必要があります。この機能の詳細については、「クラスタ間のエクステンション モビリティ（EMCC）」（P.19-10）を参照してください。

デバイス モビリティ

Cisco Unified Communications Manager（Unified CM）では、ロケーション、リージョン、コーリング サーチ スペース、メディア リソースなど、さまざまな設定を使用して、サイト、つまり物理ロケーションが識別されます。特定のサイトにある Cisco Unified IP Phone は、これらの設定により静的に設定されます。Unified CM では、適切なコールの確立、コール ルーティング、メディア リソースの選択などのためにこれらの設定を使用します。一方、Cisco IP Communicator、Cisco Cius、または Cisco Unified Wireless IP Phone などのデュアルモード電話機やその他のモバイル クライアント デバイスがそれらのホーム サイトからリモート サイトに移動されたときに、それらのデュアルモード電話機では電話機に静的に設定されているホーム設定を保持しています。この結果 Unified CM では、リモート サイトの電話機にあるこれらのホーム設定を使用します。この状況は、コール ルーティング、コーデックの選択、メディア リソースの選択、およびその他のコール処理機能における問題の原因となる場合があるため望ましくありません。

Cisco Unified CM では、デバイス モビリティという機能を使用します。この機能により、Unified CM では、IP 電話がホーム ロケーションにあるのか、ローミング ロケーションにあるのかを判別できます。Unified CM では、デバイスの IP サブネットを使用して、その IP 電話の正確な場所を判別します。クラスタ内でのデバイス モビリティを使用できるようにすることで、モバイル ユーザは 1 つのサイトから別のサイトにローミングでき、このときサイト固有の設定を取得します。次に、Unified CM では、これらの動的に割り当てられた設定を使用して、コール ルーティング、コーデックの選択、メディア リソースの選択などを行います。

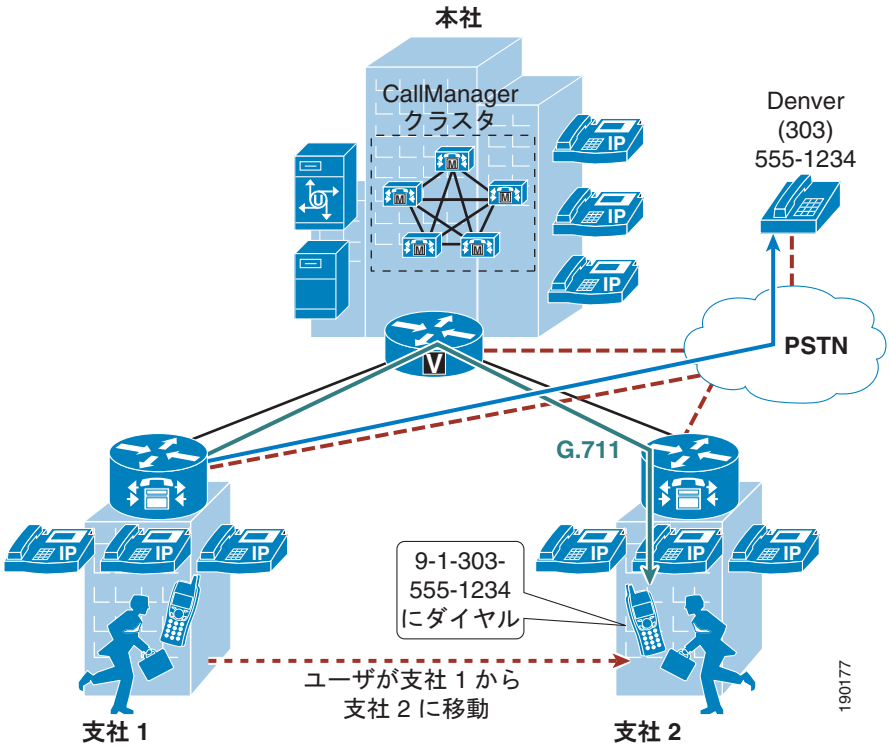
この項では、最初にデバイス モビリティ機能の主要な目的について説明し、続いてデバイス モビリティ機能そのものについて詳細に説明します。ここでは、デバイス モビリティ機能のさまざまなコンポーネントおよび構成要素について取り上げます。また、この項では、デバイス モビリティ機能が企業ダイヤル プランに与える影響を、さまざまなダイヤル プラン モデルの意味も含めて詳細に説明します。

デバイス モビリティの必要性

この項では、Unified CM クラスタに多くのモバイル ユーザが含まれている場合のデバイス モビリティの必要性について説明します。

図 25-5 は、本社サイト（HQ）にあり、デバイス モビリティ機能を備えない Unified CM クラスタを含んでいる架空のネットワークを示しています。このクラスタには、支店 1 と支店 2 の 2 つのリモート サイトがあります。サイト内コールでは、いずれも G.711 音声コーデックが使用されます。一方サイト間コール（IP WAN を経由するコール）では、いずれも G.729 音声コーデックが使用されます。各サイトには、外部コールのための公衆網ゲートウェイがあります。

図 25-5　　リモート サイトを 2 つ持つネットワークの例



支社 1 のユーザが支社 2 に移動し、Denver にいる公衆網ユーザに通話すると、次のような動作が発生します。

- Unified CM では、そのユーザが支社 1 から支社 2 に移動したことを認識していません。公衆網への外部コールが WAN を経由して支社 1 のゲートウェイに送られ、そこから公衆網に出ます。これにより、モバイル ユーザの公衆網コールすべてに、引き続きそのユーザのホーム ゲートウェイが使用されます。
- このモバイル ユーザと支社 1 ゲートウェイは、同じ Unified CM リージョンおよびロケーションに存在しています。ロケーション ベースのコール アドミッション制御は、異なるロケーションに存在しているデバイスおよび G.711 音声コーデックを使用するリージョン内コールにだけ適用可能です。したがって、IP WAN を経由する支社 1 ゲートウェイへのコールでは G.711 コーデックが使用され、コール アドミッション制御のための Unified CM によるトラッキングは行われません。この動作の結果、リモート リンクすべてが低速リンクである場合に、IP WAN 帯域幅のオーバー サブスクリプションが発生する場合があります。

- モバイル ユーザが、複数の支社 2 ユーザを Denver にいる公衆網ユーザとの既存のコールに追加することで、会議を作成します。モバイル ユーザは支社 1 ゲートウェイの会議リソースを使用します。したがって、すべての会議ストリームが IP WAN 経由で流れます。

（注）　デバイス モビリティは、クラスタ内機能で、複数の Unified CM クラスタには拡張されません。分散型コール処理環境では、配置内の各 Unified CM クラスタでデバイス モビリティを有効にし、設定する必要があります。

デバイス モビリティのアーキテクチャ

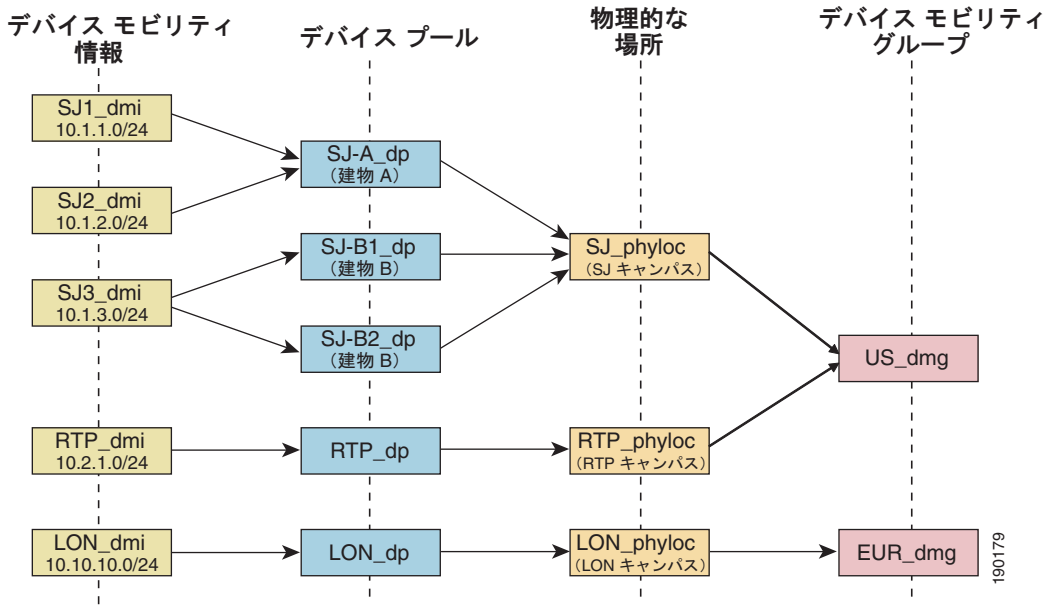
Unified CM デバイス モビリティ機能は、上記の問題を解決するために有用です。この項では、この機能の動作方法を簡単に説明します。ただし、この機能の詳細説明については、http://www.cisco.com で入手可能な製品マニュアルを参照してください。

デバイス モビリティには次のような要素が含まれます。

- デバイス モビリティ情報 : IP サブネットを設定し、デバイス プールを IP サブネットに関連付けます。
- デバイス モビリティ グループ：ダイヤリング パターンが類似しているサイトの論理グループを定義します（たとえば、図 25-6 の US_dmg および EUR_dmg）。
- 物理ロケーション：デバイス プールの物理ロケーションを定義します。言い換えると、この要素では、IP 電話およびデバイス プールに関連付けられているその他のデバイスの地理的なロケーションを定義します（たとえば、図 25-6 に示されている San Jose の IP 電話は、すべて物理ロケーション SJ_phyloc を使用して定義されています）。

図 25-6 は、この 3 つの用語すべての関係を示します。

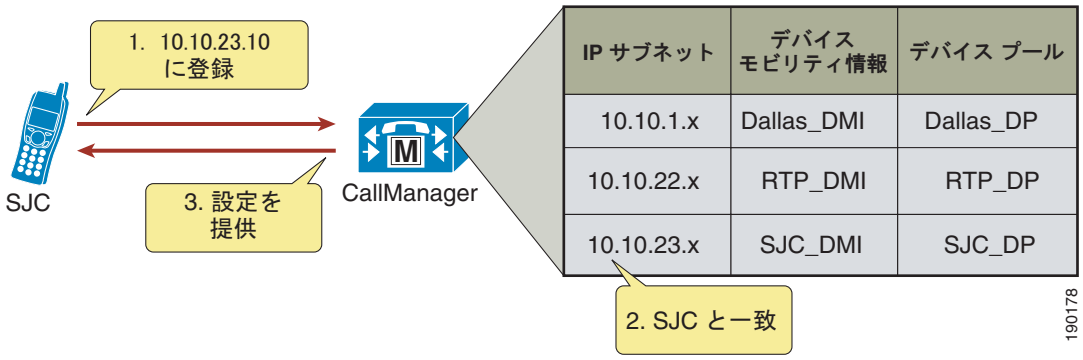
図 25-6　　デバイス モビリティ コンポーネントの関係



Unified CM では、デバイスの IP サブネットに基づいてデバイス プールを IP 電話に割り当てます。次の手順は、図 25-7 に図示がありますが、この動作を説明したものです。

1. IP 電話では、その電話の IP アドレスを Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）登録メッセージに含めて送信することにより、Unified CM への登録を試行します。
2. Unified CM では、デバイスの IP サブネットを抽出し、デバイス モビリティ情報に設定されているサブネットと照合します。
3. サブネットが一致すると、Unified CM では、デバイス プール設定に基づいて、デバイスに新規設定を提供します。

図 25-7　　電話登録プロセス



Unified CM では、デバイス プール設定にあるパラメータ一式を使用して、デバイス モビリティに対応します。これらのパラメータは、次の 2 つの主要なタイプについてのパラメータです。

- 「ローミングに依存する設定」（P.25-18）
- 「デバイス モビリティ関連の設定」（P.25-19）

ローミングに依存する設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部または外部をローミングしているときに、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- 日付/時刻グループ
- リージョン
- メディア リソース グループ リスト
- ロケーション
- ネットワーク ロケール
- SRST リファレンス
- 物理ロケーション
- デバイス モビリティ グループ

ローミングに依存する設定は、主に、適切なコール アドミッション制御および音声コーデックの選択を実施するために有用です。これは、ロケーションおよびリージョンの設定は、デバイスのローミング デバイス プールに基づいて使用されるためです。

さまざまなコール アドミッション制御手法については、「コール アドミッション制御」（P.11-1）の章を参照してください。

ローミングに依存する設定により、メディア リソース グループ リスト（MRGL）も更新されて、保留音、会議、トランスコーディングなどで適切なリモート メディア リソースが使用されるようになり、これによりネットワークが効率的に使用されます。

ローミングに依存する設定により、Survivable Remote Site Telephony（SRST）ゲートウェイも更新されます。モバイル ユーザは、ローミング中に別の SRST ゲートウェイに登録します。この登録が、ローミング電話機が SRST モードであるときのダイヤリング動作に影響することがあります。

たとえば、ユーザが Unified CM への接続を失う新しいロケーションに電話機を移動した場合、ローミングに依存するデバイス モビリティ設定に基づいて、移動された電話機に対して新しい SRST リファレンスが設定されます。また、移動された電話機はローカルなローミング ロケーション SRST ルータの制御下に入ります。この場合、デバイスの DID が変更されず、ホーム ロケーションに固定されたままになるために、ユーザの電話機は公衆網や他のサイトから到達不能になるだけでなく、SRST 内で実装されている短縮ダイヤルを使用しなければ、ローカルな障害発生サイト内のデバイスから到達することも困難になる可能性があります。

たとえば、ユーザが電話機を San Jose のホーム ロケーション（ディレクトリ番号が 51234 で、関連付けられた DID が 408 555 1234）から New York のリモート ロケーションに移動したとします。また、ユーザが New York ロケーションにローミングして間もなく、New York のサイトと San Jose の間のリンクに障害が発生したとします。このシナリオでは、New York サイトにある電話機はすべて、そのサイト内の SRST ルータにフェールオーバーされます。また、ローミング電話機または移動された電話機は、その SRST リファレンスがデバイス モビリティのローミング依存設定に基づいて更新されたために、New York の SRST ルータに登録されます。このシナリオでは、New York のローカルなデバイスが Unified CM に登録するのと同じように、5 桁の内線番号とともに SRST ルータに登録されます。その結果、ローミング電話機のディレクトリ番号は 51234 のまま変わりません。他のすべてのサイトから、および公衆網からローミング電話機に到達するために、番号 408 555 1234 が、この特定の DID が固定されている San Jose の公衆網ゲートウェイにルーティングされます。New York サイトは San Jose サイトから切断されているため、このようなコールはいずれもユーザのデスクトップフォンには到達不可能です。したがって、コールはユーザのボイスメール ボックスにルーティングされます。同様に、ローカルの障害発生サイト内のコールは、5 桁の短縮ダイヤルを使用して、または SRST ルータ内の **dialplan-pattern** および **extension-length** コマンドで定義されているように設定済みの番号をプレフィックスとして付加して、ダイヤルする必要があります。いずれの場合も、ローカル発信者が、短縮ダイヤルによりローカル ローミング デバイスに到達するために必要なダイヤリング動作を理解している必要があります。ローカル ローミング電話機に到達するために、5 桁をダイヤルするだけでよいこともあれば、ユーザが特別な番号プレフィックスをダイヤルする必要があることもあります。同じロジックが、New York の移動された電話機またはローミング電話機からの発信ダイヤリングにも適用されます。短縮ダイヤルを使用してローカル内線番号に到達するためには、そのダイヤリング動作を変更する必要があるためです。ただし、ローカルなローミング デバイスから公衆網への発信ダイヤリングは、常に同じである必要があります。

デバイス モビリティ関連の設定

これらの設定にあるパラメータは、デバイスがデバイス モビリティ グループの内部をローミングしているときにだけ、デバイス レベルの設定より優先されます。この設定には、次のパラメータが含まれます。

- デバイス モビリティ コーリング サーチ スペース
- AAR コーリング サーチ スペース
- AAR グループ
- 発信側変換 CSS
- 着信側変換 CSS

コーリング サーチ スペースは、ダイヤルできるパターンまたは到達できるデバイスを指示するため、デバイス モビリティ関連の設定は、ダイヤル プランに影響します。

デバイス モビリティ グループ

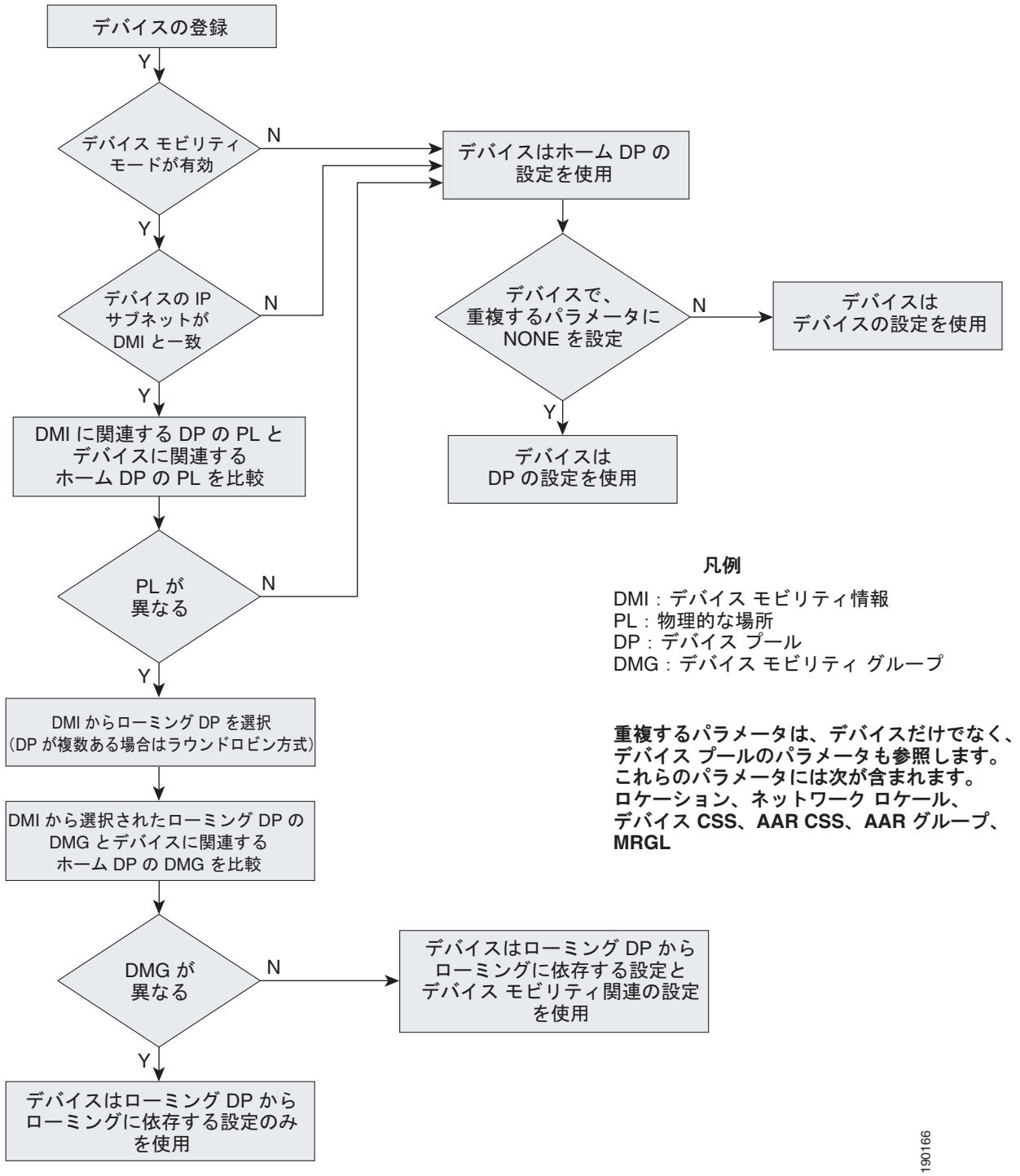
前述したように、デバイス モビリティ グループは、ダイヤリング パターンが類似したサイト（たとえば、同じ公衆網アクセス コードを持つサイトなど）の論理グループを定義します。このガイドラインを使用すると、すべてのサイトがサイト固有のコーリング サーチ スペースに類似したダイヤリング パターンを持ちます。ダイヤリング動作が異なるサイトは、異なるデバイス モビリティ グループに属します。図 25-6 に示すように、San Jose サイトと RTP サイトのデバイス モビリティ情報、デバイス プール、および物理ロケーションは異なります。ただし、必要なダイヤリング パターンと公衆網アクセス コードは 2 つのロケーション間で同じであるため、これらはすべて同じデバイス モビリティ グループ US_dmg に割り当てられています。一方、London サイトは別のデバイス モビリティ グループ EUR_dmg に割り当てられています。これは、必要なダイヤリング パターンと公衆網アクセス コードが US サイトのものとは異なるためです。デバイス モビリティ グループ内をローミングするユーザは、新規コーリング サーチ スペースを受け取ったあとも、ダイヤリング動作をリモート ロケーションで維持できます。デバイス モビリティ グループの外部をローミングするユーザは、自身のホーム コーリング サーチ スペースを使用するため、やはり、ダイヤリング動作をリモート ロケーションで維持できます。

ただし、デバイス モビリティ グループが、異なるダイヤリング パターンを持つ複数のサイトとともに定義されている場合（たとえば、あるサイトではユーザが外線使用時に 9 をダイヤルする必要があるが、別のサイトではユーザが外線使用時に 8 をダイヤルする必要がある場合）、そのデバイス モビリティ グループ内のユーザ ローミングにより、すべてのロケーションで同じダイヤリング動作を維持できないことがあります。ユーザは、各ロケーションで新規コーリング サーチ スペースを受け取った後で、異なるロケーションにおいて異なる番号をダイヤルする必要がある場合があります。この動作はユーザの混乱を招く可能性があるため、異なるダイヤリング パターンを持つサイトを同じデバイス モビリティ グループに割り当てることは推奨しません。

デバイス モビリティの動作

デバイス モビリティ機能の動作を図 25-8 のフローチャートに示します。

図 25-8　デバイス モビリティ機能の動作



デバイス モビリティ機能には、次のガイドラインが適用されます。

- 図 25-8 にリストされている重複するパラメータがデバイスおよびデバイス プールで同じ設定を持つ場合は、デバイスではこれらのパラメータに NONE を設定できます。次にこれらのパラメータをデバイス プールに設定する必要があります。この方法を実施すると、デバイスにすべてのパラメータを個別に設定する必要がないため、設定の量を大幅に削減できます。
- サイトごとに物理ロケーション 1 つを定義してください。1 つのサイトが複数のデバイス プールを持つことができます。
- 公衆網または外部/オフネット アクセスのダイヤリング パターンが類似したサイトを、同じデバイス モビリティ グループを使用して定義してください。
- 企業のポリシーに応じて、未定義のサブネットすべてに対応する、IP サブネット 0.0.0.0 の「catch-all」デバイス モビリティ情報を定義できます。このデバイス モビリティ情報は、ネットワーク リソースのアクセスまたは使用を制限できるデバイス プールを割り当てるために使用できます（たとえば、ローミング中にこのデバイス プールに関連付けられているデバイスからのコールすべてをブロックするコーリング サーチ スペース NONE を使用してデバイス プールを設定できます）。ただし、これを行う場合、管理者は、911 およびその他の緊急コールであってもブロックされるという事実を承知する必要があります。コーリング サーチ スペースは、911 またはその他の緊急コールだけにアクセスを許すパーティションを含めて設定できます。

ダイヤル プランの設計に関する考慮事項

デバイス モビリティ機能を使用する場合、電話機のダイヤリング動作は電話機のローミング（またはホーム）ロケーションに依存します。前述したように、デバイス プール内のデバイス モビリティ関連設定が、コール フローの動作に影響します。これは、コーリング サーチ スペースが、Unified CM 内の宛先パターンの到達可能性を示すためです。この項では、デバイス モビリティのための複数のダイヤル プラン アプローチについて説明します。

さまざまなダイヤル プラン アプローチの詳細については、「ダイヤル プラン」（P.9-1）の章を参照してください。

サービス クラスを構築するためのデバイス モビリティの考慮事項

ローミング中のモバイル ユーザは、一般に、ホーム ロケーションにいるときと同じコール特権を持つ必要があります。「ダイヤル プラン」（P.9-1）の章では、サービス クラスを構築するための 2 つのアプローチについて説明します（「従来のアプローチ」（P.25-22）および「回線/デバイス アプローチ」（P.25-22））。

従来のアプローチ

従来のアプローチでは、パス選択とサービス クラスはいずれも、デバイスレベルのコーリング サーチ スペースにより決定されます。回線/デバイス アプローチでは、パス選択はデバイスレベルのコーリング サーチ スペースにより決定され、サービス クラスは回線レベルのコーリング サーチ スペースにより決定されます。いずれの配置でも、サービス クラスの構築には回線/デバイス アプローチを推奨します。特に、デバイス モビリティを使用する配置においては、回線/デバイス アプローチを使用することが重要です。このアプローチを使用すると、モバイル デバイスから発信されたコールはいずれもホーム サイト ゲートウェイでなくローミング サイトまたはローカル ゲートウェイを使用するためです。従来のアプローチも使用できますが、この章では、推奨される回線/デバイス アプローチだけを取り上げます。従来のアプローチの全般的な説明は、「ダイヤル プラン」（P.9-1）の章を参照してください。

回線/デバイス アプローチ

Unified CM では、所定の IP 電話の回線およびデバイスのコーリング サーチ スペースを連結します。回線/デバイス アプローチにおいては、次の概念が重要です。

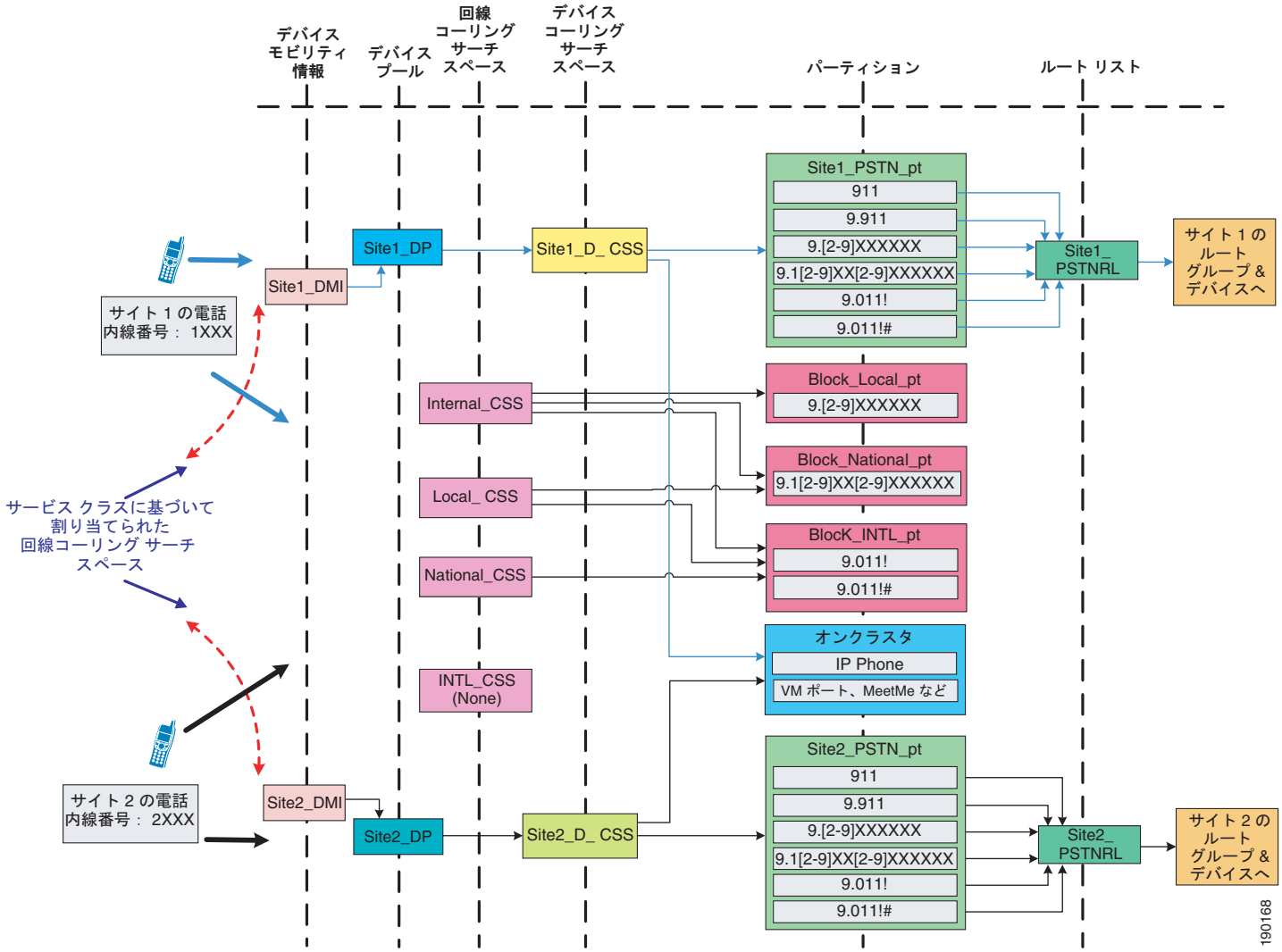
- デバイス コーリング サーチ スペースは、コール ルーティング情報を提供します。

- 回線コーリング サーチ スペースは、サービス クラス情報を提供します。

デバイス モビリティ機能を使用すると、デバイス コーリング サーチ スペースは、電話機のロケーションに基づいて、動的に電話機に関連付けられます。デバイス モビリティを使用する場合に、回線/デバイスにおける重要な概念は、引き続き同じです。回線コーリング サーチ スペースがサービス クラス情報を提供する一方、選択されたローミングまたはホーム デバイス コーリング サーチ スペースは、コール ルーティング情報を提供します。

図 25-9 は、クラスタ内でデバイス モビリティを使用する場合に、回線/デバイス アプローチを使用してサービス クラスを構築する例を示します。

図 25-9　サービス クラスを構築するための回線/デバイス アプローチ



回線/デバイス アプローチを使用して、サービス クラスを構築することを推奨します。このモデルでは、次の公式が示すように、必要なデバイス プールの数が大幅に削減されるため、デバイス モビリティを使用するうえで重要な利点があります。

合計デバイス プール数 =（サイト数）

このアプローチには、次の設計上の考慮事項が適用されます。

- 電話デバイスのコーリング サーチ スペースは NONE に設定できます。デバイス プールのコーリング サーチ スペース設定が電話デバイスに割り当てられます。この方法では、電話機にデバイス コーリング サーチ スペースを個別に設定する必要がないため、設定の量を大幅に削減できます。
- 同じサービス クラスまたはコール特権をすべてのモバイル ユーザに設定することに関して制限はありません。サービス クラスは、回線コーリング サーチ スペースを使用して定義されるため、モバイル ユーザはローミング中に同じサービス クラスを維持します。
- モバイル ユーザはプロファイルのデバイス モビリティとエクステンション モビリティの両方を有効にできます。

ダイヤル プラン モデルの選択

「ダイヤル プラン」（P.9-1）の章で説明したように、ダイヤル プラン モデルには主に 3 つのアプローチがあります。

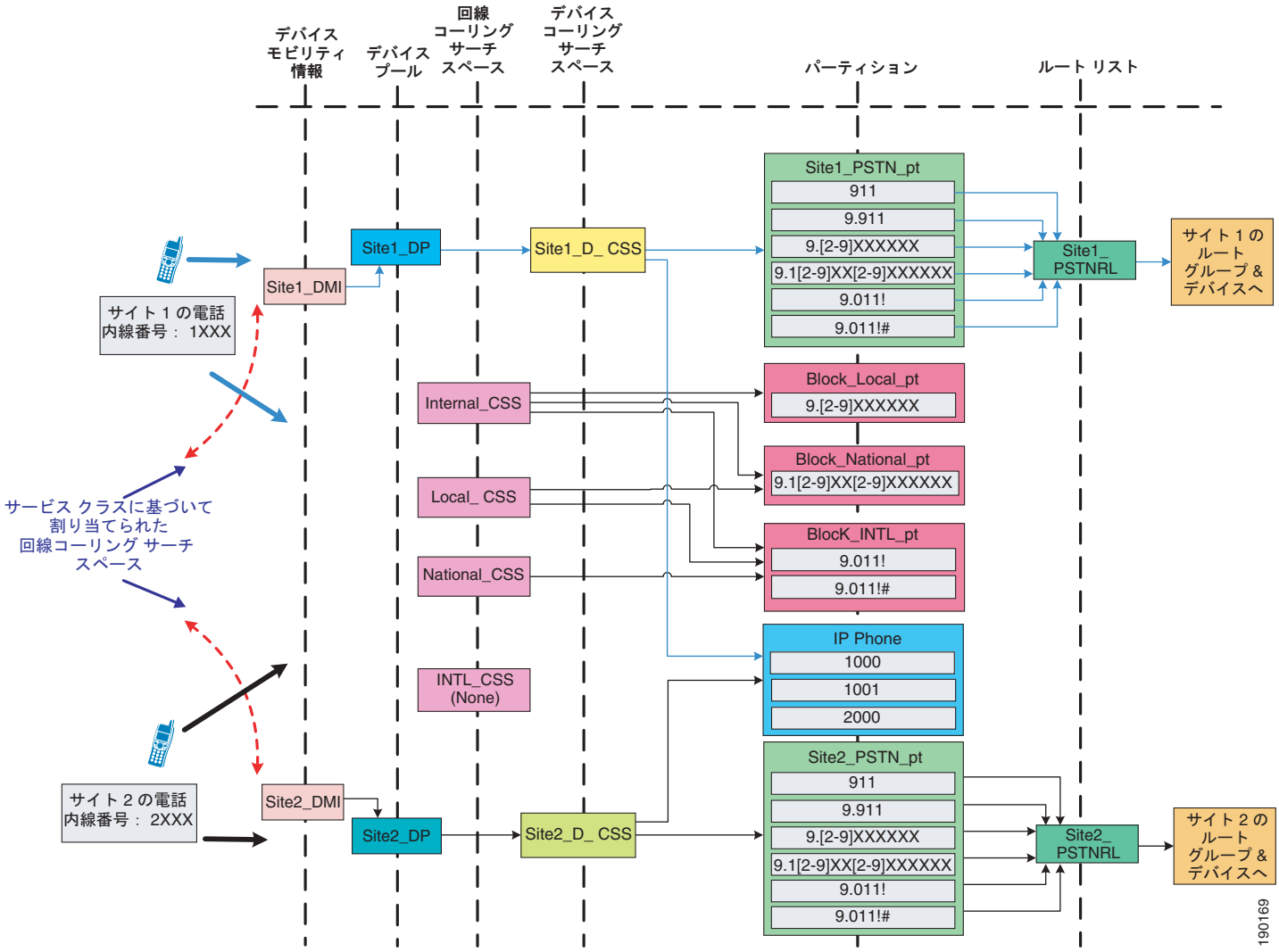
- 固定オンネット ダイヤリング
- 分割アドレッシングの可変長のオンネット ダイヤリング
- フラット アドレッシングの可変長のオンネット ダイヤリング

次の項では、サービス クラスを構築するためのアプローチと組み合わされたさまざまなダイヤル プラン モデルを示します。

回線 / デバイス アプローチを使用する固定オンネット ダイヤリング

図 25-10 は、デバイス モビリティのための固定オンネット ダイヤル プランを示します。

図 25-10　デバイス モビリティのための固定オンネット ダイヤル プラン



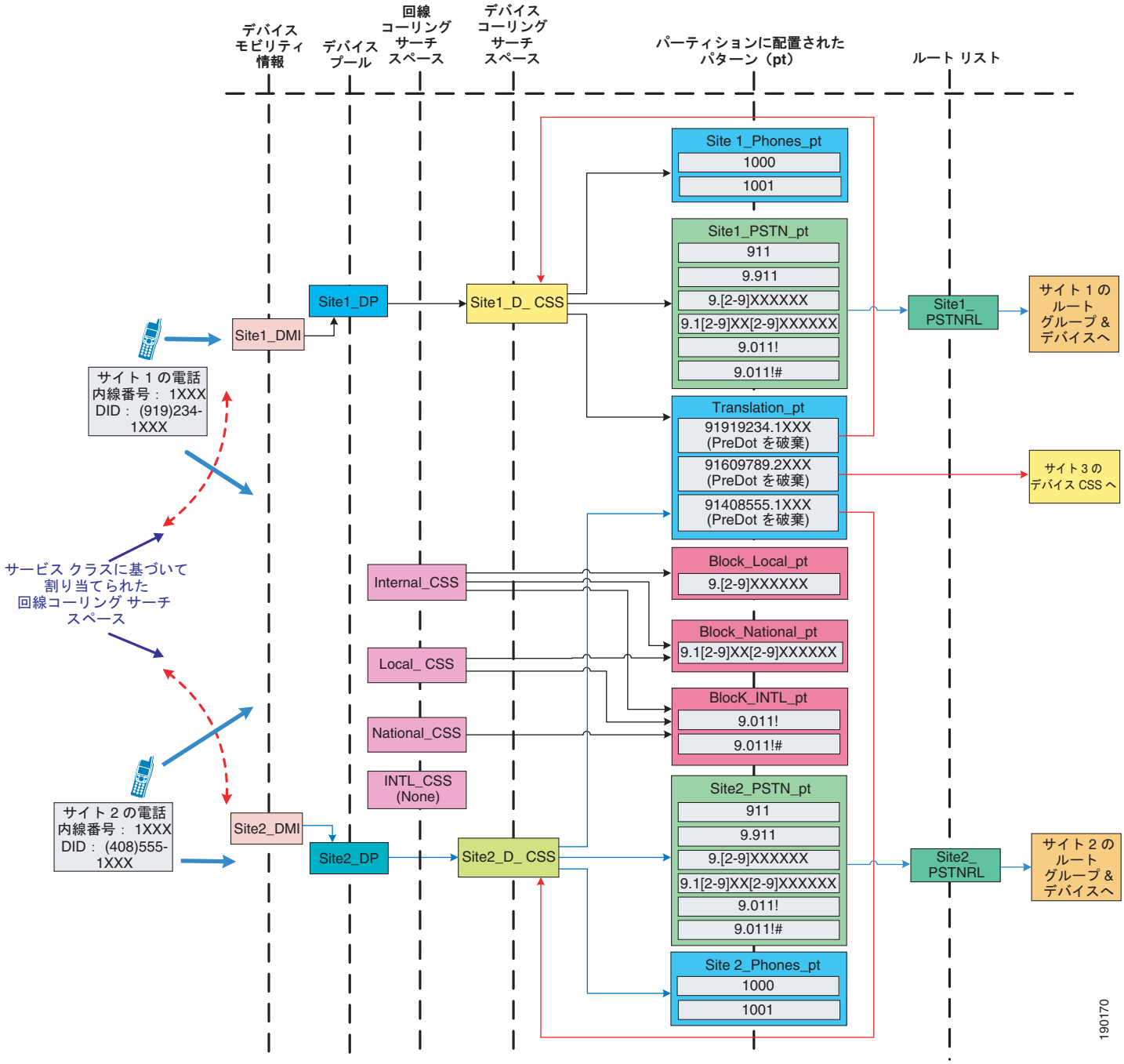
これは、最も基本的なダイヤル プラン モデルであり、次の特性があります。

- モバイル ユーザは、すべてのロケーションから短縮ダイヤル（図 25-10 の例に示されている 4 桁）を使用できます。
- 内線用の短縮設定されたスピード ダイヤルが、ローミング ロケーションにいるユーザの電話機で引き続き動作します。
- モバイル ユーザがリモート ロケーションにいるときは、「ローミング」コーリング サーチ スペースが使用されます。サイトすべての公衆網コールに同じアクセス コードを設定することを推奨します。公衆網アクセス コードが同じでないと、ユーザは、さまざまなアクセス コードを知る必要があります。

回線 / デバイス アプローチを使用する、分割アドレッシングの可変長のオンネット ダイヤリング

図 25-11 は、デバイス モビリティのための分割アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 25-11　デバイス モビリティのための分割アドレッシングによる可変長オンネット ダイヤリング プラン



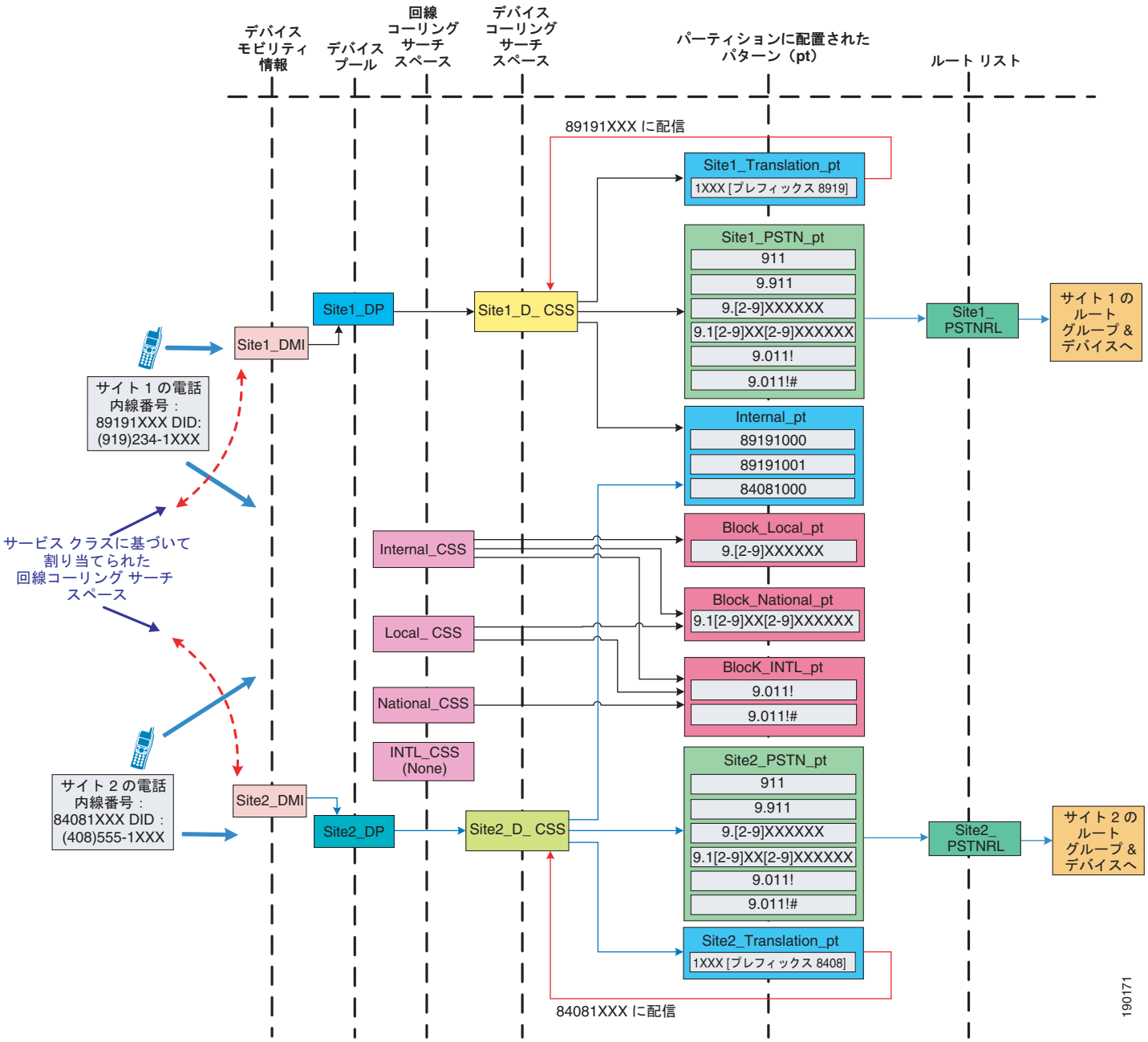
次の設計上の考慮事項が、図 25-11 のダイヤル プラン モデルに適用されます。

- モバイル ユーザがローミング ロケーションから短縮ダイヤルを使用すると、コールが誤った宛先にルーティングされることがあります。図 25-11 の例で、サイト 1 のモバイル ユーザ 1 の内線が 1000 であり、サイト 2 に移動するとします。ユーザ 1 がサイト 1 にいるユーザと通話しようと 1001 をダイヤルすると、コールは代わりにサイト 2 の内線 1001 にルーティングされます。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。図 25-8 に示すように、デバイスがローミングを行うときに、「ホーム」デバイス プールのデバイス モビリティ グループが、デバイス モビリティ情報の「ローミング」デバイス プールで定義されているデバイス モビリティ グループと異なる場合、「ローミング」デバイス プールからのローミング依存設定だけが適用されます。つまり、ローミング電話機がコールを発信するときに、ローミング依存の設定ではないデバイス モビリティ コーリング サーチ スペースは使用されず、（電話機のデバイス レベル設定またはデバイス プール設定で定義されている）「ホーム」コーリング サーチ スペースが使用されます。図 25-11 に示す例では、ユーザ 1 が内線番号 1001 をダイヤルすると、サイト 2 で「ホーム」サイトのコーリング サーチ スペースを使用してコールがルーティングされ、その結果、サイト 1 ではコールが内線番号が 1001 にルーティングされます。ただし、このコール シナリオでは、WAN 帯域幅が消費されます。さらに、この例でユーザ 1 が外部公衆網コールにダイヤルしたとすると、ローミング電話機はホーム ゲートウェイも使用します。また、「ホーム」サイトのコーリング サーチ スペースが使用されるため、WAN 帯域幅も消費します。
- 公衆網およびトランスレーション パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。
- 短縮設定のスピード ダイヤルを使用しないでください。すべてのロケーションでユーザがスピード ダイヤルを使用できるようにする普遍的な方法でスピード ダイヤルを設定することを推奨します。たとえば、ユーザは、E.164 番号を使用するか、サイト コードおよびアクセス コードを使用してスピード ダイヤルを設定できます。
- 複数のサイトの内線番号が重複していると、ローミング ユーザがリモート SRST ゲートウェイに登録されたときに問題を引き起こすことがあります。図 25-11 の例で、サイト 1 のモバイル ユーザ A の内線が 1000 であり、サイト 2 に移動するとします。さらに、サイト 2 の WAN リンクがダウンし、電話機がサイト 2 の SRST ゲートウェイに登録されることになったとします。SRST ゲートウェイにおける内線 1000 への着信コールは、実際のサイト 2 の内線 1000 のほかに、内線番号が 1000 であるモバイル ユーザにもルーティングされます。この結果、コールが適切にルーティングされないことがあります。この問題は、ネットワーク全体で一意の内線番号を使用することにより回避できます。

回線 / デバイス アプローチを使用する、フラット アドレッシングの可変長のオンネット ダイヤリング

図 25-12 は、デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プランを示します。

図 25-12　デバイス モビリティのためのフラット アドレッシングによる可変長オンネット ダイヤリング プラン



次の設計上の考慮事項が、図 25-12 のダイヤル プラン モデルに適用されます。

- モバイル ユーザは、別のサイトにローミングした後では、コールが誤った宛先にルーティングされるおそれがあるため、短縮ダイヤルを使用できません。この動作が望ましくない場合は、各サイトをデバイス モビリティ グループとして定義することを検討してください。ただし、ユーザは、外部公衆網コールすべてで、モバイル電話では引き続きホーム ゲートウェイが使用され、したがって WAN 大域幅が消費されることを承知しておく必要があります。
- 公衆網および内部電話機パーティションへのアクセスだけを持つローミング ユーザのために追加のデバイス コーリング サーチ スペースを設定できます。この設定には、サイトごとに 1 つ以上の追加のデバイス プールとコーリング サーチ スペースが必要です。したがって、*N* 個のサイトには、*N* 個のデバイス プールおよび *N* 個のコーリング サーチ スペースが必要です。ただし、この設定では、各サイトをデバイス モビリティ グループとして定義する必要がありません。
- リモート SRST ゲートウェイに登録されているモバイル ユーザは、一意な内線番号を持ちます。ただし、モバイル ユーザは、リモート SRST ゲートウェイに登録されているときは、公衆網ユーザがモバイル ユーザと通話できないことを承知しておく必要があります。

マルチサイト企業モビリティのハイ アベイラビリティ

マルチサイト企業モビリティ機能およびソリューションは、モビリティ機能のハイ アベイラビリティを保証するため、冗長性を備えた方法で設定、配置する必要があります。有線電話機の移動、無線ローミング、およびマルチサイト モビリティ配置での EM のハイ アベイラビリティの考慮事項は、キャンパス モビリティ配置での考慮事項と同様です。キャンパス環境と同じく、冗長ネットワーク ポート、無線セル カバレッジ、およびエクステンション モビリティのログインおよびログアウトを処理する Unified CM ノードが、高可用なサービスを確保するために必要です。

また、デバイス モビリティ機能のハイ アベイラビリティを考慮することも重要です。デバイス モビリティ機能はネイティブで Unified CM 内に統合されているため、デバイス モビリティの機能がクラスタ ノードの障害による影響を受けることはありません。パブリッシャ ノードまたはコール処理（サブスクライバ）ノードに障害が発生した場合、デバイス プール、デバイス モビリティ情報、デバイス モビリティ グループ、およびデバイス モビリティに関連する他のすべての設定は保持されます。また、コール処理ノードに障害が発生した場合、影響を受ける電話機は、Unified CM Group の構成要素に基づいて、通常どおりセカンダリ コール処理ノードまたは SRST リファレンス ルータにフェールオーバーします。

マルチサイト企業モビリティのキャパシティ プランニング

デバイス モビリティのスケーラビリティの考慮事項と同様、この機能および各種の構成要素（デバイス プールやデバイス モビリティ グループなど）に関連する特定のキャパシティ制限または強制的なキャパシティ制限はありません。しかし、適切なサイジングを行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用してシステムのキャパシティを決定します。また、サイジング ツールにより具体的なデバイス モビリティ サイズが指定されることはありませんが、このツールで提供されるサイジング ガイダンス全体に従えば、サポートされているキャパシティ制限内でこの機能および全体的なシステムを配置できます。Unified CST は、シスコの従業員およびパートナーだけが（適切なログイン認証を使用して）、http://tools.cisco.com/cucst より利用することが可能です。

マルチサイト企業モビリティの設計上の考慮事項

企業モビリティの設計上の考慮事項はすべて、マルチサイト企業モビリティ配置にも適用されます（「キャンパス企業モビリティの設計上の考慮事項」（P.25-11）を参照）。さらに、次の設計に関する推奨事項が、特にマルチサイト モビリティ環境に適用されます。

- サイト間の接続や、他のサイトの接続の障害が重要な動作を妨害しないよう、すべての重要なサービス（デバイス登録、公衆網接続、DNS、DHCP など）をマルチサイト配置内の各サイトで確実に配置してください。加えて、デバイスや必要なコール キャパシティをサポートするため、十分な数の物理ネットワーク ポートおよびワイヤレス LAN AP が各サイトで使用できるようにしてください。
- 異なるダイヤリング パターンを持つ複数のサイト（たとえば、異なる公衆網アクセス コードを持つ複数のサイト）が同じデバイス モビリティ グループ内に設定されている場合、ローミング ユーザが各自のロケーションに基づいて異なる方法で番号をダイヤルする必要があるため、混乱を招く可能性があります。このため、類似のダイヤリング パターンを持つサイト（たとえば、同じ公衆網アクセス コードを持つサイト）を同じデバイス モビリティ グループに割り当てることを推奨します。これにより、ローミング ユーザは、デバイス モビリティ グループ内のすべてのサイトで同じ方法で番号をダイヤルできます。
- 「ローミング」デバイス プールからのデバイス モビリティ設定が適用されるのは、同じデバイス モビリティ グループ内でローミングするときだけです。移動された電話機からの元のコールが「ホーム」またはデバイスで設定されているコーリング サーチ スペースを使用し、結果的にコール ルーティング動作が引き起こされるため、異なるデバイス モビリティ グループ間でのローミングを避けてください。これにより、ローカルな「ローミング」ゲートウェイではなく別のサイトのゲートウェイを経由してコールがルーティングされる可能性があります。その結果、不必要に WAN 帯域幅が消費されることがあります。
- 物理ロケーションは各サイトに 1 つだけ定義してください。そうすることで、ユーザがサイト間でローミングを行う場合にだけ、デバイス モビリティが適用されます。同じサイト内でローミングを行う場合は、デバイス モビリティに影響する要素（たとえば、WAN 帯域幅消費、コーデック選択、コール アドミッション制御など）を考慮する必要はありません。単一のサイト内では通常、低速のリンクは配置されないためです。
- フェールオーバーのシナリオでは、「ローミング」電話機は、「ローミング」デバイス プールのローミング依存設定に従って、SRST リファレンス/ゲートウェイを利用します。したがって、これらの状況においては、「ローミング」電話機の DID は別のロケーションの公衆網ゲートウェイに固定されているために、公衆網からこの電話機に到達することはできません。さらに、「ローミング」電話機からコールを発信する場合は、公衆網アクセス コードなどの要素に対してダイヤリング動作を変更する必要があることがあります。また、電話機で設定されているスピード ダイヤルが使用できなくなることもあります。
- 一般的に、ダイヤル プランには常に回線/デバイス アプローチを使用することが推奨されます。特にこれが重要なのは、デバイス モビリティを配置する際に、各モバイル ユーザに異なるサービス クラスまたはコーリング特権が許可されるためです。回線/デバイス アプローチでは、サービス クラスは、デバイスの回線コーリング サーチ スペースを使用して定義されます。これはローミング時も変わらず、モバイル ユーザはローミング時も同じサービス クラスを保持できます。
- システムで、短縮ダイヤルを使用できることや、短縮ダイヤルに依存するスピード ダイヤルを使用できることが要求されている場合は、固定オンネット ダイヤル プラン モデルを使用することを推奨します。このモデルを使用すると、（直接またはスピード ダイヤルによる）短縮ダイヤルは、モバイル ユーザの電話機がローミング ロケーションにあっても、正常に機能するためです。すべての内線番号またはディレクトリ番号は全サイトにわたって一意であるため、短縮ダイヤルを使用し続けることができます。また、重複する内線番号がないため、短縮ダイヤルを普遍的に使用できます。

- システムで可変長のオンネット ダイヤル プラン モデル（分割アドレッシングまたはフラット アドレッシング）が使用されている場合、発信時に 1 つの一意な内線番号に到達できるように、普遍的な方法でスピード ダイヤルを設定することを推奨します。完全な E.164 番号を使用するか、サイトまたはアクセス コードを使用してスピード ダイヤルを設定することにより、ローミング ユーザはすべてのロケーションで同じスピード ダイヤルを使用できます。
- VPN 接続を介して企業ネットワークにアクセスすることがあるユーザに対してデバイス モビリティを有効にした場合は、VPN ロケーションへの「ローミング」により確実に動的デバイス モビリティ設定変更が行われるように、VPN が接続された電話機の Device Mobility Info（DMI; デバイス モビリティ情報）に、VPN コンセントレータにより配信または所有された IP サブネットが含まれている必要があります。DMI は、VPN コンセントレータと同じ場所にあるデバイスに使用されているデバイス プールに関連付ける必要があります。

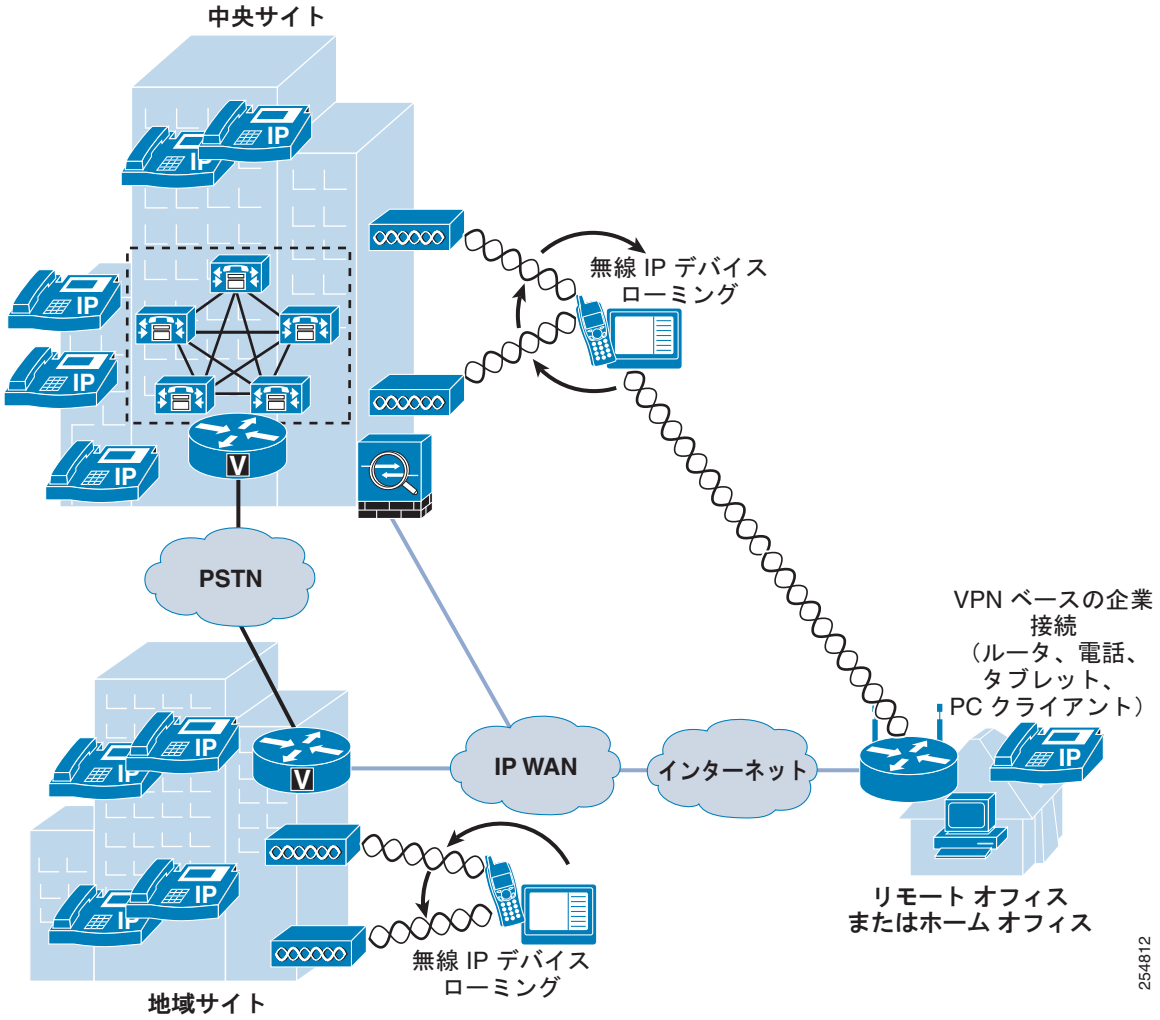
リモート企業モビリティ

リモート企業モビリティは、企業から離れたロケーションにいて、公共のインターネットを介した安全な接続により企業ネットワーク インフラストラクチャに接続しているモバイル ユーザを指します。ここでモビリティは、これらのリモート ロケーションでのエンドポイント デバイスの配置や、企業と各自のロケーション間での頻度に関わらないユーザの移動や、場合によってはユーザが使用するモバイル デバイスを処理します。

リモート企業モビリティのアーキテクチャ

図 25-13 に示すように、リモート企業モビリティのアーキテクチャは、リモート物理ロケーション（一般に、従業員のホーム オフィスや、それ以外の、インターネット経由で会社に安全に接続できるあらゆるリモート ロケーション）に基づいています。これらのリモート サイトは、一般にユーザのコンピュータ、電話機、およびその他の機器またはエンドポイントへ接続できる IP ネットワークで構成されます。場合によっては、この IP ネットワークを企業の制御下に置き、リモート ロケーションと企業ネットワーク間に安全なトンネルを備えた VPN ルータを構成できます。また、リモート サイト IP ネットワークをユーザが用意したルータを介してインターネットに接続し、ユーザのコンピュータまたはエンドポイント デバイスでソフトウェアベースの VPN クライアント機能を使用して会社のネットワークへの安全な接続を作成する必要がある場合もあります。無線接続をリモート ロケーションで使用して、ユーザのコンピュータまたはエンドポイントを無線接続できるようにすることもできます。無線接続をリモート ロケーションで使用する場合、ワイヤレス電話機を企業ネットワークからホーム オフィスへ移動することもでき、企業デバイスまたはモバイル電話機をリモート ロケーション内で利用して受信することもできます。

図 25-13　リモート企業モビリティのアーキテクチャ



リモート企業モビリティのタイプ

リモート企業モビリティ配置は、通常のユーザまたはデバイスの移動をサポートすることではなく、主にリモート ユーザをサポートすることに重点を置いています。確かにユーザは、エンドポイント デバイスを持っても持たなくても定期的に企業ロケーション間またはロケーションとリモート サイト間を移動できます。ただし、これらの配置の主な目的は、企業ユーザのリモート接続をサポートすることです。一般的にリモート サイト モビリティには、主にルータベースの安全な接続とクライアントベースの安全な接続の 2 つのタイプがあります。両方のタイプとも、リモート サイトへの安全な接続をサポートしており、デュアルモード モバイル電話機、ワイヤレス IP 電話機およびタブレット、さらには有線 IP 電話機などの、リモート サイトと企業間で移動できるさまざまなエンドポイント デバイスに対応できます。

クライアントベースの安全なリモート接続

無線および有線 IP 電話機と、ソフトウェアベースの PC テレフォニー クライアントは、図 25-13 に示すように、リモート サイト ロケーションに接続できます。これらのデバイスおよびエンドポイントは、企業の VPN ヘッドエンド ターミネーション コンセントレータに安全に VPN 接続する必要があります。

企業ネットワークに接続するためのこれらのタイプのデバイスの例には、Cisco Mobile 8 iPhone クライアントなどの、ネイティブ VPN クライアント機能を使用した無線接続のデュアルモード電話機およびクライアント（「デュアルモードの電話機とクライアント」（P.25-64）を参照）、Cisco Mobile 8.5 Nokia クライアント（「ダイレクト コネクト モバイル クライアント」（P.25-99）を参照）、Cisco Unified IP Phone 7965 などの組み込み VPN クライアントを使用した有線 Cisco Unified IP 電話、および Cisco IP Communicator などの、ソフトウェアベースのテレフォニー クライアントを実行しているパーソナル コンピュータなどがあります。

ルータベースの安全なリモート接続

一方、リモート サイト接続は、ルータベースの安全な VPN トンネルを介して行うことができます。これらのタイプのシナリオでは、配置したワイヤレス ネットワーク接続も可能なリモート サイト ルータで、企業ネットワークへの安全な VPN トンネルを設定する必要があります。これにより実質的に、企業ネットワークの境界をリモート サイト ロケーションまで広げます。このタイプの接続のメリットは、より幅広い種類のデバイスとエンドポイントをリモート サイトに配置できることです。これらのデバイスで接続の安全性を確保する必要がなく、特別なソフトウェアや設定の必要がないためです。代わりに、これらのデバイスはリモート サイト ネットワークに接続するだけで、リモート サイト ルータから企業 VPN ヘッドエンドまでの安全な VPN IP パスを利用できます。

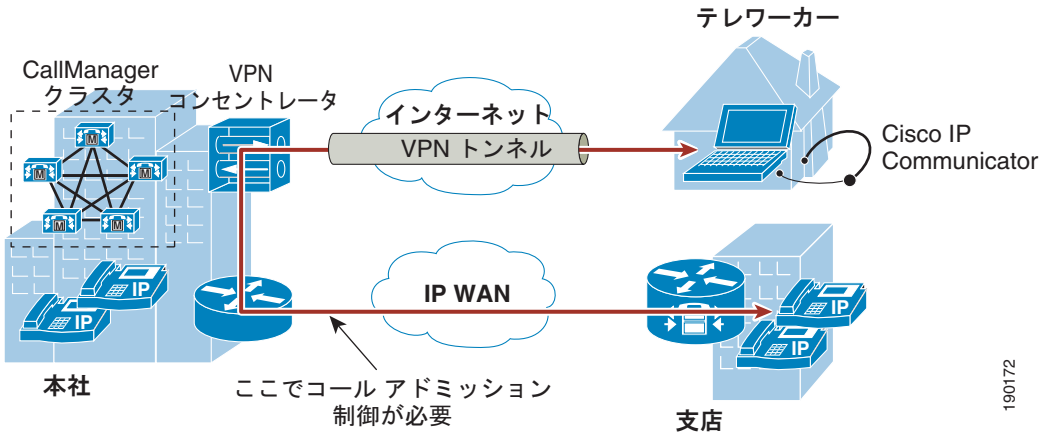
このタイプのルートベースのリモート サイト接続の例には、Cisco Virtual Office ソリューションがあります。

デバイス モビリティと VPN ベースのリモート企業接続

クライアントベース接続とルータベースの安全なリモート接続のどちらを配置するかにかかわらず、コール アドミッション制御およびコーデックがエンドポイント デバイスに正しくネゴシエートされ、適切な企業サイトの公衆網ゲートウェイおよびメディア リソースが使用されるようにするため、デバイス モビリティ機能を使用できます。VPN 接続経由で受信したエンドポイント デバイスの IP アドレスに基づいて、Unified CM はデバイスのロケーションを動的に決定します。

図 25-14 は、Cisco IP Communicator ソフトウェア電話がリモート サイトのコンピュータで実行されている、クライアントベースの安全なリモート接続の例です。このソフトウェアベースの IP 電話は、クライアントベースの VPN を介して企業に接続され、Unified CM に登録されています。

図 25-14　リモート サイトの Cisco IP Communicator 向けのクライアントベースの VPN 接続



次は、企業に VPN 接続経由で接続しているリモート サイトにおいて、ユーザ デバイスでのデバイス モビリティ機能の有効化に関する設計ガイドラインです。

- VPN コンセントレータによって配布または所有されている IP サブネットを指定してデバイス モビリティ情報（DMI）を設定します。
- VPN コンセントレータと同じ場所にあるデバイスに使用されるデバイス プールと同じデバイス プールに DMI を関連付けます。ただし、コール特権、ネットワーク ロケールなどのパラメータを考慮する必要があります。
- リモート サイトのユーザに、クライアントベースまたはルータベースの VPN 接続を行う場合は、地理的に最も近い企業 VPN コンセントレータを指定するよう指導します。

これらのガイドラインにより、確実に、企業 WAN 上でおよびリモート サイトへの接続を介して、コール アドミッション制御が正しく適用されます。

VPN の配置の詳細については、次のサイトの「Design Zone for WAN/MAN」の「*Security in WAN*」で入手可能な各種の VPN 設計ガイドを参照してください。

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns817/landing_wan_security.html

リモート企業モビリティのハイ アベイラビリティ

リモート サイト モビリティ環境では、企業 VPN サービスが、冗長性を備えた方法で企業内に構成され配置されている必要があります。これにより確実に、クライアントベースおよびルータベース両方の安全な接続の可用性が高くなります。企業内の VPN コンセントレータに障害がある場合、新しい安全な接続を、他の VPN コンセントレータでセットアップできます。このタイプの配置では、デバイス登録および音声サービスの可用性は、組み込み Unified CM ノードの冗長性のおかげで高くなります。

リモート企業モビリティのキャパシティ プランニング

リモート企業モビリティ環境のスケーラビリティの考慮事項で最も重要なのは、VPN コンセントレータのキャパシティです。管理者は、クライアントベースまたはルータベースの安全なトンネル接続のいずれの場合でも、すべてのリモート サイトの接続に対応する十分な VPN セッション キャパシティを配置する必要があります。適切なキャパシティを用意しないと、一部のリモート サイトが会社に接続できなくなり、基本的なテレフォニー サービスでもアクセスできなくなります。さらに、キャンパスまたはマルチサイト企業モビリティの配置と同様、すべてのリモート ユーザのデバイスを処理できるよう、企業内に十分なデバイス登録キャパシティを用意することが重要です。

リモート企業モビリティの設計上の考慮事項

モバイル ユーザがリモート サイト接続できるようにする場合、次の設計上の推奨事項を考慮してください。

- デバイス モビリティを使用する場合、VPN コンセントレータが配布または所有する IP サブネットを含む Device Mobility Info（DMI; デバイス モビリティ情報）を忘れずに設定し、この DMI を VPN コンセントレータと同じロケーションに配置するデバイスに設定される同じデバイス プールに割り当ててください。
- リモート サイト ユーザに、VPN を接続する場合は最も近い VPN コンセントレータを選択するよう指導します。
- すべてのリモート サイト ユーザへの接続を用意するため、適切な VPN セッション キャパシティが確実に使用できるようにしてください。

社外型モビリティ

モビリティ ユーザは、デスクトップフォンだけでなく、1 つまたは複数のリモート電話機で会社の電話番号にかかってきた電話に出ることができます。また、モビリティ ユーザは、まるで社内から電話をかけているかのようにリモート電話機から電話をかけることもできます。さらに、モビリティ ユーザは、保留、転送、会議などのエンタープライズ機能だけでなく、携帯電話上でのボイスメール、会議、プレゼンスなどのエンタープライズ アプリケーションも利用できます。これによって、ユーザは外出先でも生産性を持続させることができます。

さらに、モバイル ボイス ネットワークと企業の WLAN の両方への接続を提供するデュアルモード電話機を使用すると、ユーザは、社外からエンタープライズ アプリケーションを利用できるだけでなく、社内にいる場合でも、分単位で料金が発生するモバイル ボイス ネットワークを使用せずにエンタープライズ テレフォニー インフラストラクチャを利用してコールを発信および受信できます。

Cisco Unified Communications ソリューションに付属のモビリティ機能は、Cisco Unified Communications Manager（Unified CM）を通して提供され、Cisco Unified Mobile Communicator アプリケーション、デュアルモード電話機、およびデュアルモード クライアントと組み合せて使用できます。

Cisco Unified Mobility では、次のモビリティ アプリケーション機能が提供されます。

- モバイル コネクト

  シングル ナンバー リーチとも呼ばれるモバイル コネクトを使用すれば、1 つの会社の電話番号で Cisco Unified Communications ユーザの IP 卓上電話と携帯電話の両方を同時に呼び出すことができます。モバイル コネクト ユーザは、着信コールをデスクトップフォンでも携帯電話でも受けることができ、通話中のコールを妨げることなく別の電話に転送できます。

- 通話切替機能

  通話切替機能により、モビリティ コールの通話中に、携帯電話の保留、保留解除、転送、会議、およびリダイレクト コール パーク機能を呼び出すことができます。これらの機能は、携帯電話のキーによって呼び出され、保留音やカンファレンス ブリッジといった企業のメディア リソースを活用します。

- シングル企業ボイスメール ボックス

  シングル企業ボイスメール ボックスは、ユーザの会社の電話番号に着信し、さらに携帯電話に転送されたコールに応答がなかった場合に、携帯電話のボイスメール システムではなく、会社のボイスメール システムにコールを蓄積します。これにより、ボイスメール ボックスが 1 箇所に統合され、ユーザは複数のボイスメール システムでメッセージを確認する必要がなくなります。

- 2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセス

  2 ステージ ダイヤリング機能付きモバイル ボイス アクセスとエンタープライズ機能アクセスによって、まるで会社の IP 卓上電話からかけているかのように、携帯電話から発信できます。長距離電話や国際電話、または通常は企業外部から到達不能なシステム上の内部の DID 以外の内線番号へのコールにおいてこれらの機能を使用すると、通話料金を節約できます。また、企業でこれらの 2 ステージ ダイヤリング機能を使用すると、中央で一括管理されたコール詳細レコードによって、ユーザのコール発信を容易に追跡管理できるようになります。さらに、これらの機能によって、発信者 ID を送信する際にユーザの携帯電話番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。

デュアルモードの電話機とクライアントを使用すると、モバイル ボイス ネットワーク、モバイル データ ネットワーク、および音声接続とデータ接続用の企業ワイヤレス ネットワークのすべてに接続できます。これにより、ユーザは、単一のデバイスから企業の呼制御とモバイル ネットワークの呼制御の両方を利用できます。デュアルモード電話機では、可能な限り企業の WLAN を利用してコールの発信および受信を行い、企業の接続が利用できない場合にだけモバイル ボイス ネットワークを使用することによって、テレフォニー関連のコストを削減できます。また、デュアルモードの電話機とクライアントには、ハンドオフ メカニズムが備えられているため、ユーザが社内と社外の境界を越えて移動した場合に、通話中の音声コールにおいて、WLAN インターフェイスとモバイル ボイス インターフェイスを簡単に切り替えることができます。

Cisco Unified Mobile Communicator アプリケーションには、バックホール データ チャネルの使用によってユーザの携帯電話にエンタープライズ向けのユニファイド コミュニケーション機能を提供するモバイル クライアントが含まれます。データ チャネルはインターネット上のサービス プロバイダー データ サービスによって送信され、Cisco Adaptive Security Appliance（ASA）で終端処理されてから、企業の Unified Communications インフラストラクチャ内のさまざまなアプリケーションやコンポーネントとインターフェイスする Unified Mobility Advantage サーバに転送されます。音声サービスでは、公衆網およびモバイル ボイス ネットワークが利用されます。

Cisco Unified Mobile Communicator アプリケーションと統合可能なエンタープライズ アプリケーションおよび機能を次に示します。

- ユーザ認証およびディレクトリ ルックアップ用の Microsoft Active Directory を使用した LDAP ディレクトリ
- ユーザの企業ボイスメール ボックスのメッセージ待機インジケータおよび視覚ナビゲーション用の Cisco Unity または Unity Connection を使用したボイスメール
- 会議通知の受信用の Cisco Unified MeetingPlace を使用した会議とコラボレーション
- Cisco Unified Personal Communicator などの他のクライアントやアプリケーションとのプレゼンス情報の交換やバディ リストの同期化を可能にする、Cisco Unified Presence とのプレゼンス統合
- ユーザの卓上電話からのコール履歴ログの受信およびエンタープライズ IP テレフォニー インフラストラクチャ経由のダイヤリング用の Cisco Unified Communications Manager（Unified CM）を使用したエンタープライズ コール ログと Dial-via-office
- その他の Cisco Unified Mobile Communicator クライアントを使用したテキスト メッセージの送受信用のメッセージング

さまざまなエンタープライズ ユニファイド コミュニケーション アプリケーションとの統合機能の提供に加えて、Cisco Unified Mobile Communicator モバイル クライアントと Unified Mobility を統合してモバイル コネクトやシングル企業ボイスメール ボックスなどの機能を利用できます。

ダイレクト コネクト モバイル クライアントを使用すると、携帯電話から、モバイル データ ネットワーク経由で企業ネットワークにリモート接続、または企業 WLAN 経由でローカル接続して、Dial-Via-office および Voice over WLAN などの音声機能や、社内ディレクトリ アクセス、プレゼンスおよび Instant Massaging（IM; インスタント メッセージング）などのその他のユニファイド コミュニケーション サービスを利用できます。これらのダイレクト コネクト クライアントは、Cisco Unified

Mobile Communicator と同様の機能（Dial-via-office、社内ディレクトリアクセス、プレゼンスなど）、およびデュアルモード電話機やクライアントなどの音声 WLAN 機能を提供するため、モバイル ユーザは社内、社外に関係なくコラボレーション アプリケーションにアクセスでき、生産性を保つことができます。また同時に、社外からモバイル データ ネットワークを利用するか、社内で WLAN ネットワークを利用するかにかかわらず、モバイル デバイスからビジネス コールを発信および受信することを可能にします。

この項では、まず、Unified Mobility の特徴、機能、および設計と配置に関する考慮事項について説明します。Unified Mobility のさまざまなメリットとデュアルモード電話機とクライアントを統合することによってその機能が利用できるという事実を前提として、Cisco Mobile などのデュアルモード クライアント アプリケーションを検証します。デュアルモード モバイル電話機クライアントの説明に続き、Cisco Unified Mobile Communicator とダイレクト コネクト モバイル クライアントについて説明します。この項には、次のモビリティ アプリケーションおよび機能のアーキテクチャ、機能性、および設計と配置の意味に関する説明が含まれます。

- 「Cisco Unified Mobility」（P.25-37）
- 「デュアルモードの電話機とクライアント」（P.25-64）
- 「Cisco Unified Mobile Communicator」（P.25-85）
- 「ダイレクト コネクト モバイル クライアント」（P.25-99）

Cisco Unified Mobility

Cisco Unified Mobility は、Cisco Unified Communications Manager（Unified CM）に組み込まれたネイティブなモビリティ機能を意味し、モバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスの各機能が含まれます。

Unified Mobility の機能は、Unified CM の設定によって異なります。したがって、この設定だけでなく、論理コンポーネントの特性も理解することが重要です。

図 25-15 に、Unified Mobility に関する設定要件を示します。まず、ユーザに関しては、モビリティ ユーザの会社の電話機は、電話番号、パーティション、コーリング サーチ スペースなどの該当する回線レベル設定値を使用して設定されます。この他に、会社の電話機のデバイス レベルの設定には、デバイス プール、共通デバイス設定、コーリング サーチ スペース、メディア リソース グループ リスト、ユーザとネットワークの保留音源などのパラメータが含まれます。ユーザの会社の電話機に関するこれらの回線およびデバイス設定のすべてが、着信コールと発信コールのコール ルーティングや Music On Hold（MoH; 保留音）の動作に影響を与えます。

次に、Unified Mobility 機能が利用できるように、モビリティ ユーザごとのリモート接続先プロファイルを設定する必要があります。リモート接続先プロファイルは、ユーザの会社の電話回線と同じ電話番号、パーティション、およびコーリング サーチ スペースを使用して回線レベルで設定します。これによって、リモート接続先プロファイルと会社の電話機の間で回線が共有されます。リモート接続先プロファイル設定には、デバイス プール、コーリング サーチ スペース、コーリング サーチ スペースの再ルーティング、およびユーザとネットワークの保留音源に関するパラメータが含まれます。リモート接続先プロファイルは、その設定にユーザの回線レベルの会社の電話機の設定が反映されますが、回線レベルの設定とプロファイル レベルの設定を組み合せることによって、ユーザのリモート接続先電話機に継承されるコール ルーティングおよび MoH 動作が決定される仮想電話機と見なす必要があります。リモート接続先プロファイルと会社の電話機の間で共有されるユーザの会社の電話番号を使用すれば、その番号に電話することによってユーザのリモート接続先に転送できます。

図 25-15　Cisco Unified Mobility の設定アーキテクチャ

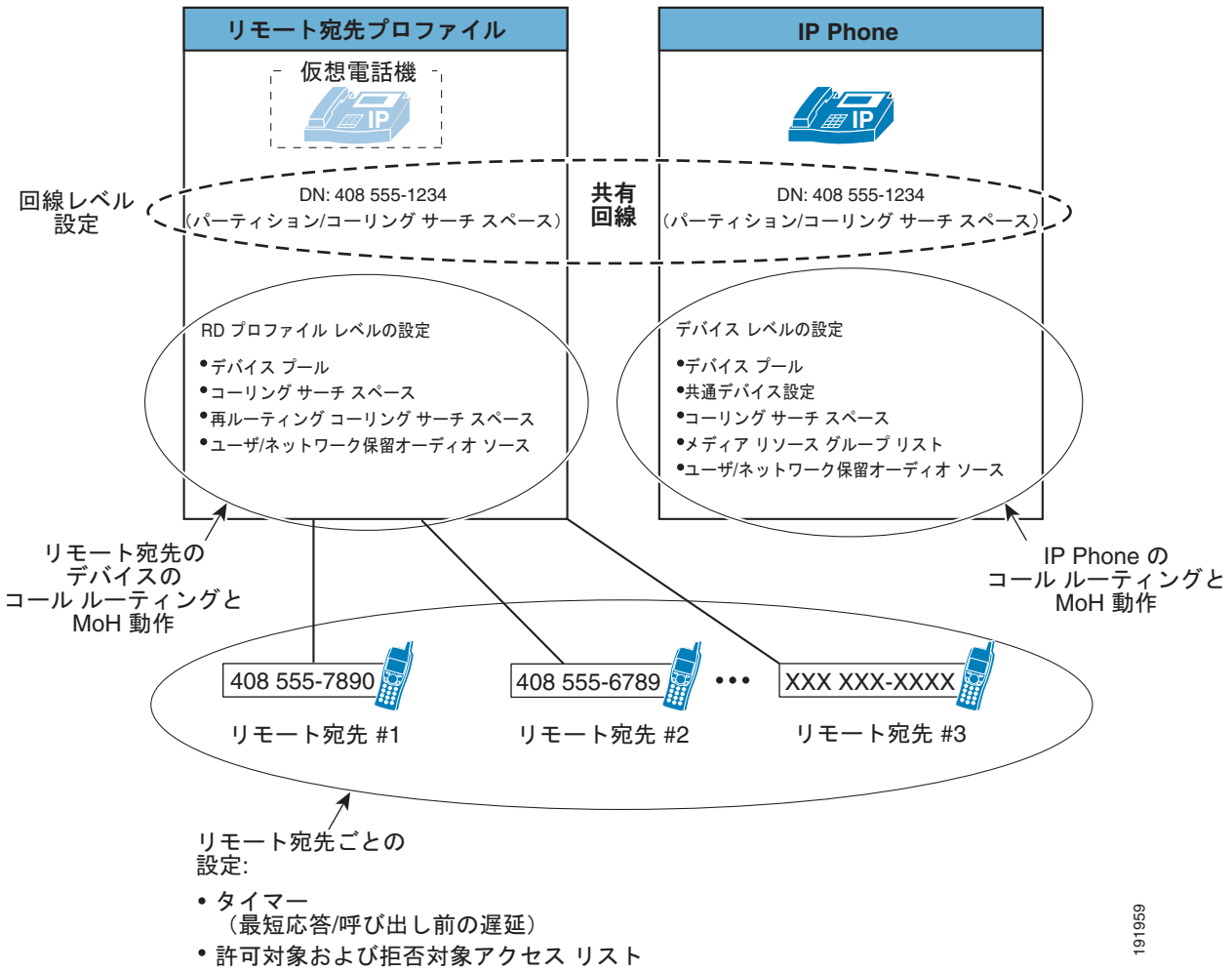


図 25-15 に示すように、モビリティ ユーザは、1 つまたは複数のリモート接続先をリモート接続先プロファイルに関連付けることができます。リモート接続先は、ユーザを呼び出すための単一の公衆網電話番号を表しています。ユーザは、最大で 10 個のリモート接続先を定義できます。リモート接続先ごとにコール ルーティング タイマーを設定して、コールを特定のリモート電話に転送する時間だけでなく、コールを転送する前に待機する時間とリモート電話でコールを受ける準備ができるまでの時間を調整できます。また、モビリティ ユーザは、リモート接続先ごとに、リモート電話に転送する特定の電話番号からのコールを許可または拒否するフィルタを設定できます。

（注）　Cisco Unified Communications Manager Business Edition では、モビリティ ユーザ 1 人につき最大 4 つのリモート接続先がサポートされています。

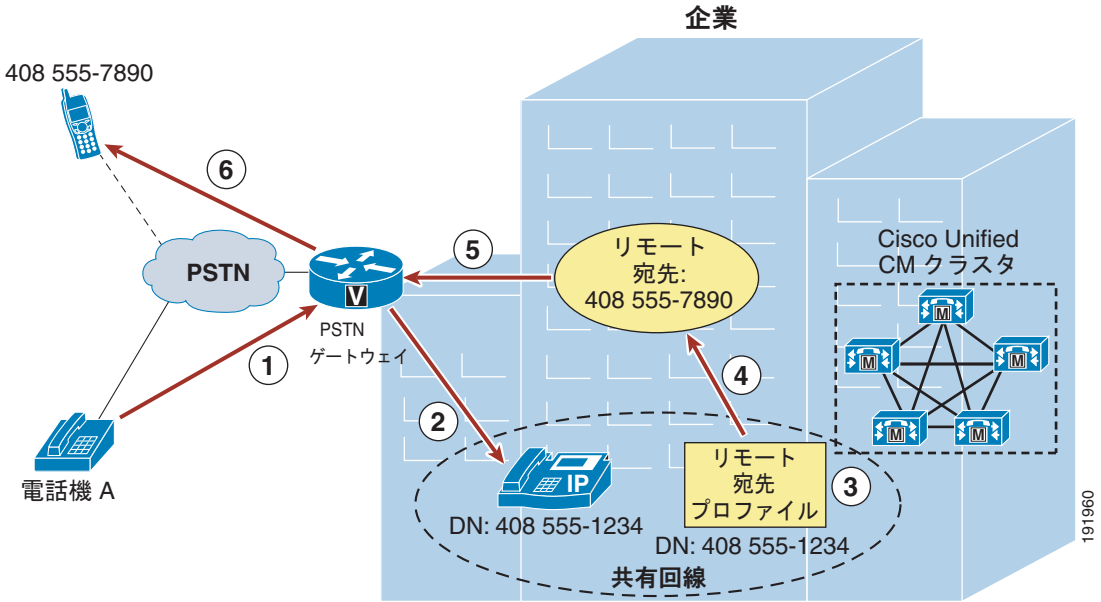
モバイル コネクト

モバイル コネクト機能を使用すれば、企業ユーザへの着信コールをそのユーザのデスクトップフォンだけでなく、最大 10 個の設定可能なリモート接続先に転送できます。一般的に、ユーザのリモート接続先は携帯電話です。コールがデスクトップフォンとリモート接続先電話機の両方に転送されれば、ユーザはどちらかの電話機で応答できます。ユーザは、リモート接続先電話機のいずれかまたは IP デスクトップフォンでコールに応答したときに、そのコールを別の電話機でハンドオフするか、ピックアップするかを選択できます。

モバイル コネクトの機能

図 25-16 に、基本的なモバイル コネクトのコール フローを示します。この例では、公衆網上の 電話機 A からモバイル コネクト ユーザの会社の電話番号（DN）408-555-1234 に電話をかけます（ステップ 1）。コールが会社の公衆網ゲートウェイから Unified CM を経由して DN 408-555-1234 の IP 電話機に転送され（ステップ 2）、この電話が鳴り出します。コールは、同じ DN を共有するユーザのリモート接続先プロファイルにも転送されます（ステップ 3）。次に、コールがユーザのリモート接続先プロファイルに関連付けられたリモート接続先（この場合は 408-555-7890）に発信されます（ステップ 4）。リモート接続先への発信コールが公衆網ゲートウェイを介してルーティングされます（ステップ 5）。最後に、番号が 408 555-7890 のリモート接続先公衆網電話機で呼出音が鳴ります（ステップ 6）。どちらの電話機でも応答できます。

図 25-16　　モバイル コネクト



通常、モバイル コネクト ユーザの設定済みリモート接続先は、Global System for Mobile Communications（GSM）またはセルラー ネットワーク上の携帯電話です。ただし、公衆網による到達可能な任意の接続先をユーザのリモート接続先として設定できます。さらに、モバイル コネクト ユーザは 10 件までリモート接続先を設定できるため、着信コールは最大で 10 台の公衆網電話機とユーザのデスクトップフォンを呼び出すことができます。デスクトップフォンまたはリモート接続先電話機のいずれかでコールに応答すると、他のリモート接続先またはデスクトップフォン（デスクトップフォンで応答しなかった場合）に転送されたすべてのコール レッグがクリアされます。リモート接続

先で着信コールに応答した場合は、2 つのゲートウェイ ポートを使用している会社の公衆網ゲートウェイ内で音声メディア パスがヘアピンされます。モバイル コネクト機能を配置する場合はこの利用を考慮する必要があります。

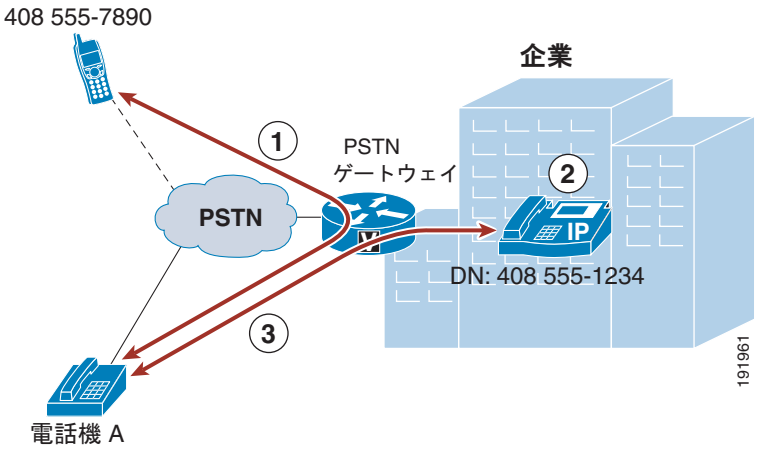
（注）　Cisco Unified Communications Manager Business Edition システムのモビリティ ユーザには、最大 4 つのリモート接続先を設定できます。

（注）　図 25-16 に示すようにモバイル コネクトを動作させるには、[End User] 設定ページでユーザ レベルの [Enable Mobility] チェックボックスがオンになっており、少なくとも 1 つのユーザの設定済みリモート接続先で [Enable Mobile Connect] チェックボックスがオンになっていることを確認します。

デスクトップフォンのピックアップ

図 25-17 に示すように、ユーザがリモート接続先デバイスでモバイル コネクトに応答した場合（ステップ 1：この場合は 408 555-7890）は、ユーザはデスクトップフォンの [Resume] ソフトキーを押すだけで、いつでもリモート接続先でコールをいったん切ってから、デスクトップフォンでピックアップできます（ステップ 2：この場合は DN 408 555-1234）。電話機 A を使用している元の発信者とデスクトップフォンとの間でコールが再開されます（ステップ 3）。

図 25-17　　デスクトップフォンのピックアップ



デスクトップフォンのピックアップは、設定済みのリモート接続先電話機で会社の固定コールの通話が行われた後、その電話が切られた場合にいつでも実行できます。

（注）　会社の固定コールとは、会社の公衆網ゲートウェイ経由で接続された少なくとも 1 つのコール レッグがあり、リモート接続先から会社の DID に発信された、あるいはモバイル コネクト、モバイル ボイス アクセス、エンタープライズ機能アクセス、または Intelligent Session Control によって発信されたすべてのコールを指します。

デスクトップフォンでコールをピックアップまたは保留解除するためのオプションは、一定時間しか使用できません。そのため、モバイル コネクト ユーザは、必ず、着信電話機が切れていることを確認してから、リモート接続先電話機を切るようにしてください。これによって、他の誰かがデスクトップフォンでコールを保留解除できないことが保証されます。デフォルトで、リモート接続先電話機が切られてから 10 秒間はコールをデスクトップフォンでピックアップできます。ただし、この時間は設定可

能であり、[End User] 設定ページで Maximum Wait Time for Desk Pickup パラメータを変更することによって、ユーザごとに 0 ～ 30,000 ミリ秒に設定できます。デスクトップフォンのピックアップは、リモート接続先電話機で通話切替保留機能を呼び出した後でも実行できます。ただし、このような場合は、Maximum Wait Time for Desk Pickup パラメータの設定が、ピックアップに使用できる時間に影響しません。通話切替保留されたコールは、リモート電話機とデスクトップフォンのどちらかで手動で保留解除されるまで、保留のままで、デスクトップフォンでピックアップできます。

デスクトップフォンのピックアップを実行するもう 1 つの方法に、通話切替セッション ハンドオフ機能を使用する方法があります。この通話切替機能は、セッション ハンドオフのデフォルトのエンタープライズ機能アクセス コードである *74 を手動で入力することによって呼び出します。これにより、Unified CM への DTMF シーケンスが生成されます。この機能が呼び出されると、Unified CM からユーザの会社のデスクトップフォンに新しいコールが送信されます。ユーザは、セッション ハンドオフを完了させるために、この新しいコールがデスクトップフォンの点滅表示または呼出音によって通知されたらこのコールに応答する必要があります。

デスクトップフォンのピックアップを行う場合にこの方法を使用すると、他の方法（携帯電話でコールを切断する方法や通話切替保留機能を使用する方法など）と比較して、ユーザと遠端の電話機との間の会話がハンドオフ プロセス中にも維持されるという利点があります。*74 シーケンスを入力すると、ハンドオフ コールがユーザのデスクトップフォンに送信されるため、ユーザは会話を継続できます。ユーザがデスクトップフォンでコールに応答すると、コール レッグが切り替えられて、遠端へのコール レッグが、デスクトップフォンに作成された新しいコール レッグに接続されます。これにより、音声パスが切断されずに、またはほぼ瞬間的にカットスルーされます。モバイル デバイスの元のコール レッグは、後でクリアされます。

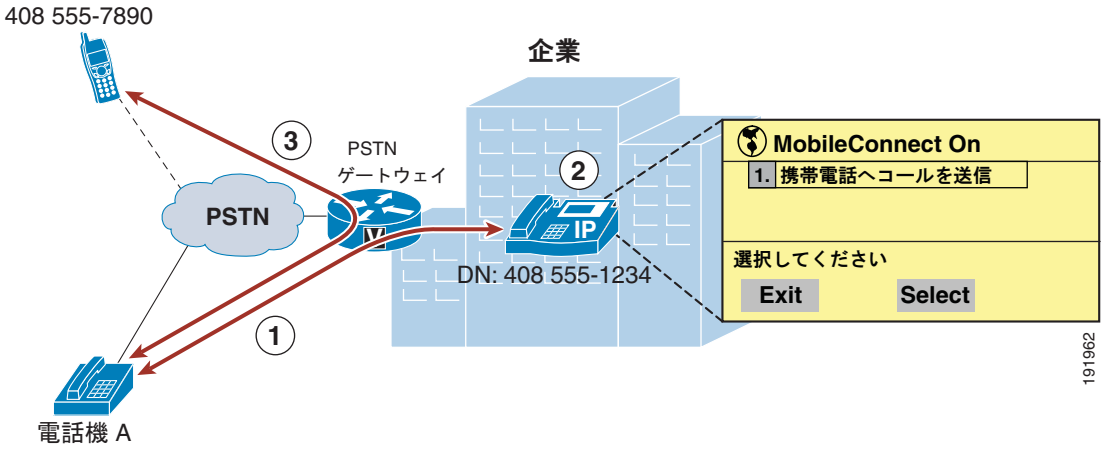
コールを切断してデスクトップフォンのピックアップを呼び出す方法では、エンド ユーザの Maximum Wait Time for Desk Pickup の設定によってデスクトップフォンでコールをピックアップできる時間が決定されます。一方、セッション ハンドオフでは、Session Handoff Alerting Timer サービス パラメータによって、デスクトップフォンでどの程度の時間呼出音または点滅表示によってコールが通知された後にハンドオフ コールがクリアされるかが決定されます。デフォルトのハンドオフ アラート時間は 10 秒です。また、セッション ハンドオフでは、デスクトップフォンに設定されたどの自動転送設定も関与しません。その結果、ハンドオフ機能では、ボイスメールやその他の自動転送宛先への転送は行われません。Session Handoff Alerting Timer 期間を経過してもコールに応答しないと、コールはクリアされて、ユーザのデスクトップフォン回線から Remote In Use 状態が削除されます。ただし、このシナリオでは、携帯電話の元のコールは維持されます。

セッション ハンドオフおよびその他の通話切替機能の詳細については、「通話切替機能」（P.25-42）を参照してください。

リモート接続先電話のピックアップ

図 25-18 に、モバイル コネクトのリモート接続先電話機のピックアップ機能を示します。電話機 A からモバイル コネクト ユーザの会社の DN 408 555-1234 が呼び出され、そのコールがユーザのデスクトップフォンで応答されて通話中である場合（ステップ 1）は、ユーザが [Mobility] ソフトキーを押す必要があります。この電話機でモバイル コネクト機能が有効になっており、リモート接続先ピックアップが使用できる場合、ユーザは [Select] ソフトキーを押します（ステップ 2）。ユーザのリモート接続先電話機に対するコール（この場合は 408 555-7890）が実行され、リモート電話機が鳴り出します。リモート電話機でコールが応答されると、電話機 A と、番号が 408 555-7890 のモバイル コネクト ユーザのリモート電話機との間でコールが再開されます（ステップ 3）。

図 25-18　リモート接続先電話のピックアップ



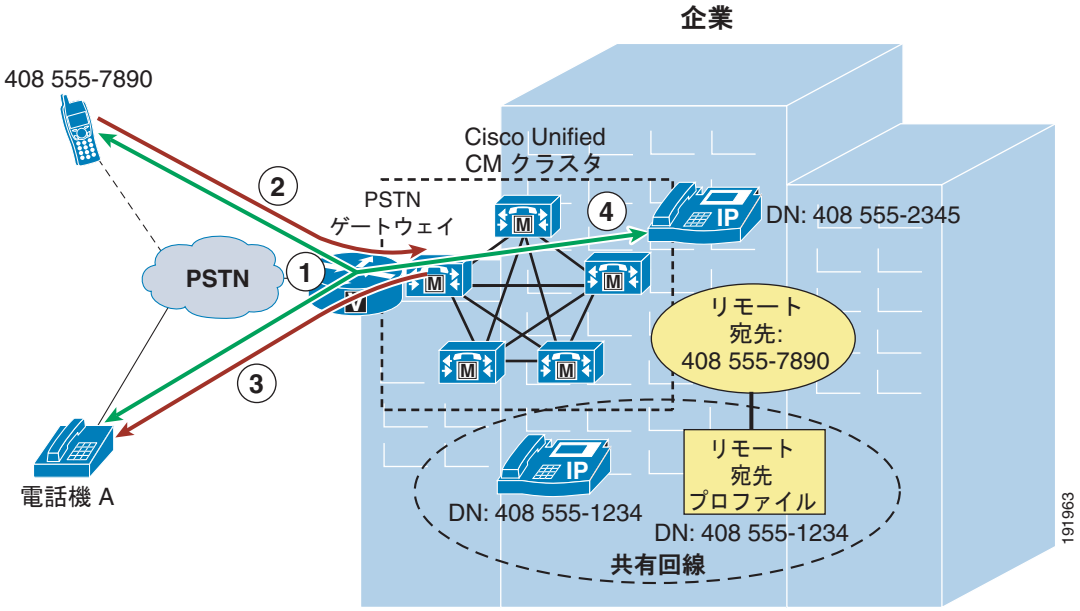
モバイル コネクト ユーザに対して複数のリモート接続先が設定されている場合は、[Select] ソフトキーを押したときに各リモート接続先が呼び出され、ユーザは好きな電話機をピックアップできます。

（注）　図 25-18 に示すように、リモート接続先電話機のピックアップを動作させるには、1 つ以上のユーザの設定済みリモート接続先で [Mobile Phone] チェックボックスがオンになっていることを確認してください。加えて、[Mobility] ソフトキーをすべてのモビリティ ユーザの関連するデスクトップフォン ソフトキー テンプレートに追加する必要があります。[Mobile Phone] チェックボックスをオンにして、Mobility ユーザが [Mobility] ソフトキーを使用できるようにしなければ、リモート接続先電話機のピックアップ機能が使用できません。

通話切替機能

図 25-19 に示すように、ユーザがリモート接続先デバイスでモバイル コネクト コールに応答（ステップ 1：この場合は 408 555-7890）したら、会社の公衆網ゲートウェイ経由でリモート接続先電話機から Unified CM に DTMF 番号を送信することによって、保留、保留解除、転送、会議、ダイレクト コール パーク、セッション ハンドオフなどの通話切替機能を呼び出すことができます（ステップ 2）。通話切替機能の保留、転送、会議、またはダイレクト コール パークが呼び出されると、Unified CM から電話の相手に MoH が送信されます（ステップ 3：この場合は電話機 A）。通話中のコールを別の電話機やダイレクト コール パーク番号に転送したり、会社の会議リソースを使用して新しい電話機で会議に参加できます（ステップ 4）。

図 25-19　モビリティ通話切替機能



Unified CM に転送された一連の DTMF 番号によって、リモート接続先電話機で通話切替機能が呼び出されます。Unified CM で受信されるこれらの番号シーケンスが、設定済みの保留、独占保留、保留解除、転送、会議、およびセッション ハンドオフ用のエンタープライズ機能アクセス コードと照合され、該当する機能が実行されます。

（注）　ダイレクト コール パークの通話切替機能を有効にするには、ダイレクト コール パーク番号とコール パーク取得プレフィックスを使用して Cisco Unified CM を設定する必要があります。

（注）　転送、会議、およびダイレクト コール パークの通話切替機能を実行するために、コールに応答して、ユーザ入力（PIN 番号、通話切替機能アクセス コード、およびターゲット番号を含む）を取得し、必要なコール レッグを作成して転送、会議、またはダイレクト コール パークの処理を完了させる、システム設定のエンタープライズ機能アクセス DID への別のコール レッグがリモート接続先電話機で生成されます。

通話切替セッション ハンドオフ機能では、遠端は保留されないため、MoH は遠端に転送されません。モバイル ユーザがデスクトップフォンでハンドオフ コールに応答するまでの間、元の音声パスが維持されます。ユーザがコールに応答すると、コール レッグが会社のゲートウェイで切り替えられ、音声パスが引き続き維持されます。

通話切替機能は、手動で機能アクセス コードを入力し、適切なキー シーケンスを入力することによって呼び出されます。表 25-2 に、通話切替機能を呼び出すためのキー シーケンスを示します。

表 25-2　手動通話切替機能のキー シーケンス

通話切替機能	エンタープライズ機能アクセス コード（デフォルト）	手動キー シーケンス
保留	*81	入力：*81
独占保留	*82	入力：*82
保留解除	*83	入力：*83
転送	*84	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *84 # <*Transfer_Target/DN*> # 4. 転送ターゲットでの応答時（打診転送の場合）またはリングバック時（初期在席転送の場合）の入力：*84
ダイレクト コール パーク	該当なし	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *84 # <*Directed_Call_Park_Number*> # *84 # **（注）** パークされたコールを取得するには、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリングを使用してコールをダイレクト コール パーク番号に発信する必要があります。ダイヤルするダイレクト コール パーク番号が入力する際、適切なコール パーク取得プレフィックスを付加する必要があります。
会議	*85	1. 入力：*82（独占保留） 2. エンタープライズ機能アクセス DID への新しいコールの発信 3. 接続時の入力：<*PIN_number*> # *85 # <*Conference_Target/DN*> # 4. 会議ターゲットによる応答時の入力：*85
セッション ハンドオフ	*74	1. 入力：*74 2. デスクトップフォンに呼出音または点滅表示で通知されたら応答

（注） 保留や会議などの通話切替機能のためのメディア リソース割り当ては、リモート接続先プロファイル設定、またはデュアルモード電話機および Unified Mobile Communicator の場合にはデバイス設定で決定されます。リモート接続先プロファイル、デュアルモード デバイス、または Unified Mobile Communicator デバイスに設定されたデバイス プールの Media Resource Group List（MRGL; メディア リソース グループ リスト）が、会議通話切替機能のためのカンファレンス ブリッジの割り当てに使用されます。リモート接続先プロファイル、デュアルモード デバイス、または Unified Mobile

Communicator デバイスのユーザ保留音源とネットワーク保留 MoH 音源の設定、およびデバイス プールの Media Resource Group List（MRGL; メディア リソース グループ リスト）が、保留デバイスに送信する MoH ストリームの決定に使用されます。

シングル企業ボイスメール ボックス

Unified Mobility とモバイル コネクトを組み合せることによって、1 つのボイスメール ボックスで会社のすべてのビジネス コールに対応することもできます。これによって、ユーザは、会社の電話番号にかかってくる電話用に用意された複数のメールボックス（会社、携帯電話、自宅など）をチェックする必要がなくなります。この機能の実装を支援するために、[Remote Destination] 設定ページで通常の自動転送タイマーと組み合せて使用できる一連のタイマーが利用できます。これらのタイマーの目的は、コールが無応答呼び出しでボイルメール ボックスに転送されたときに、そのコールがリモート接続先のボイスメール ボックスではなく、会社のボイルメール ボックスに転送されることを保証することです。この動作は、次の 2 つの方法のどちらかで実現できます。

- デスクトップフォンの無応答転送時間をリモート接続先電話機よりも短くします。

  これを実現するために、Unified CM のグローバルな無応答転送タイマー フィールドまたは個々の電話回線の無応答呼び出し期間フィールドを、リモート接続先電話機のリモート接続先ボイスメール ボックスに転送されるまでの呼び出し期間より短い値に設定します。加えて、[Remote Destination] 設定ページの [Delay Before Ringing Timer] パラメータを使用して、リモート接続先電話機の呼び出しを遅らせることによって、リモート接続先電話機からそのボイスメール ボックスに転送されるまでの時間を延ばすことができます。ただし、[Delay Before Ringing Timer] パラメータを調整する場合は、グローバルな Unified CM 無応答転送タイマー（または回線レベルの無応答呼び出し期間フィールド）が、モビリティ ユーザが余裕を持ってリモート接続先電話機の呼び出しに応答できる値に設定されていることを確認する必要があります。[Delay Before Ringing Timer] パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 4,000 ミリ秒です。

- リモート接続先電話機のボイスメール ボックスに転送される前にその電話機の呼出音を停止します。

  この動作は、[Remote Destination] 設定ページの [Answer Too Late Timer] パラメータを、リモート接続先電話機が呼び出されてからボイスメール ボックスに転送されるまでの時間より短い値に設定することによって実現できます。これによって、コールがリモート接続先電話機のボイスメール ボックスに転送される前にその電話機の呼出音が停止します。[Answer Too Late Timer] パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 19,000 ミリ秒です。

ユーザのリモート接続先電話機が通話中でコール ウェイティングが使用できない場合、または、ユーザの携帯電話が圏外にある場合でもコールが会社のボイスメール ボックスに転送されることを保証するために、[Remote Destination] 設定ページの [Answer Too Soon Timer] パラメータを使用できます。コールがリモート接続先ボイスメールに転送され、すぐに応答された場合は、このパラメータによって、リモート接続先電話機に転送されたコール レッグが切断され、デスクトップフォンで応答する時間または会社のボイスメール システムでコールを処理する時間が増えることが保証されます。[Answer Too Soon Timer] パラメータは、リモート接続先ごとに設定することが可能で、デフォルト値は 1,500 ミリ秒です。

（注） モビリティ ユーザが、Answer Too Soon Timer が切れてから、手動でリモート接続先に宛先変更した着信コールは、最終的にモバイル ボイスメール ボックスに転送される可能性があります。この発生を防ぐには、ボイスメールに宛先変更する着信コールの呼び出しを無視または無効にするようにモビリティ ユーザに助言する必要があります。これによって、無応答コールは必ず、会社のボイスメール ボックスに転送されることが保証されます。

（注）　ほとんどの配置シナリオでは、[Delay Before Ringing Timer]、[Answer Too Late Timer]、および [Answer Too Soon Timer] のデフォルト値で十分であり、変更する必要はありません。

モバイル コネクトの有効化と無効化

モバイル コネクト機能は、次の方法のいずれかを使用して有効または無効にできます。

- [Cisco Unified CM Administration] ページまたは [Cisco Unified CM User Options] ページ

  管理者またはユーザが、[Mobile Connect] チェックボックスをオフにしてその機能を無効にするか、[Mobile Connect] チェックボックスをオンにしてその機能を有効にします。これをリモート接続先ごとに実行します。

- モバイル ボイス アクセスまたはエンタープライズ機能アクセス

  モビリティ対応ユーザが、モバイル ボイス アクセスまたはエンタープライズ機能アクセスにダイヤルインして、適切なクレデンシャルを入力後に、数字の 2 を入力して有効にするか、数字の 3 を入力して無効にします。モバイル ボイス アクセスでは、単一のリモート接続先またはすべてのリモート接続先のモバイル コネクトを有効/無効にするように促されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先のモバイル コネクトしか有効/無効にできません。

- デスクトップフォンの [Mobility] ソフトキー

  ユーザは、電話がオンフック状態のときに [Mobility] ソフトキーを押して、モバイル コネクトを有効にするか、無効にするかを選択します。この方法では、ユーザのリモート接続先のモバイル コネクトすべてが有効または無効にされます。

- モバイル クライアント

  Cisco Unified Mobile Communicator またはダイレクト コネクト モバイル クライアントを搭載したモバイル デバイスを使用するユーザは、クライアント設定でモバイル コネクトまたはシングル ナンバー リーチの設定を有効または無効に変更することによって、モバイル コネクト機能のステータスを切り替えることができます。この操作では、Cisco Unified Mobile Communicator またはダイレクト コネクト モバイル クライアントのモビリティ ID のみに対してモバイル コネクトが有効または無効になります。

モバイル コネクト コールの許可または拒否用のアクセス リスト

アクセス リストは、Cisco Unified CM 内で設定して、リモート接続先に関連付けることができます。アクセス リストは、モビリティ対応ユーザのリモート接続先に転送される着信コールを許可または拒否（着信コールの発信者 ID に基づく）するために使用されます。さらに、これらのアクセス リストは時刻に基づいて呼び出されます。

アクセス リストは、拒否または許可するモビリティ対応ユーザごとに設定されます。アクセス リストには、特定の番号または番号マスクで構成された 1 つ以上のメンバーまたはフィルタが含まれており、このフィルタが発信側の着信コールの発信者 ID と比較されます。発信者 ID と照合するための特定の番号文字列または番号マスクが含まれることに加えて、アクセス リストには、発信者 ID が使用できない、または、発信者 ID がプライベートに設定されている着信コール用のフィルタも含めることができます。拒否対象のアクセス リストには、アクセス リストに入力された番号からのコールは拒否されるが、その他の番号からのコールは許可されるように、リストの最後に暗黙の「すべて許可」が含まれています。許可対象のアクセス リストには、アクセス リストに入力された番号からのコールは許可されるが、その他の番号からのコールは拒否されるように、リストの最後に暗黙の「すべて拒否」が含まれています。

設定したアクセス リストを Remote Destination 設定画面で設定した Ring Schedule に関連付けると、設定した Ring Schedule と選択したアクセス リストの組み合せによって、リモート接続先ごとのモバイル コネクトの時刻コール フィルタリングが提供されます。Cisco Unified CM Administration イン

ターフェイスを使用している管理者または Cisco Unified CM User Options インターフェイスを使用しているエンド ユーザは、アクセス リストと Ring Schedule を設定してリモート接続先に関連付けることができます。

モバイル コネクトのアーキテクチャ

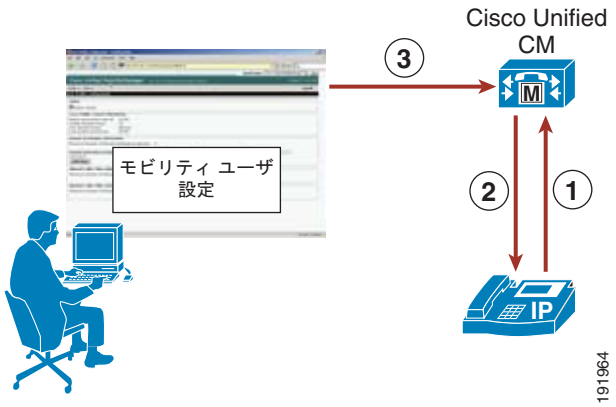
モバイル コネクト機能のアーキテクチャを理解することは、その機能を理解することと同様に重要です。図 25-20 に、モバイル コネクトに必要なメッセージ フローとアーキテクチャを示します。次の相互作用とイベントのシーケンスが、Unified CM、モバイル コネクト ユーザ、およびモバイル コネクト ユーザのデスクトップフォンの間で発生する可能性があります。

1. モバイル コネクト機能の有効化または無効化、あるいはリモート接続先電話機の通話中コールのピックアップを希望しているモバイル コネクト電話機のユーザが、デスクトップフォンの [Mobility] ソフトキーを押します（図 25-20 のステップ 1 を参照）。
2. Unified CM からモバイル コネクトのステータス（オンまたはオフ）が返されます。ユーザは、電話が接続状態であれば携帯電話にコールを転送するオプションを選択することも、電話がオンフック状態であればモバイル コネクトのステータスを有効/無効にすることもできます（図 25-20 のステップ 2 を参照）。
3. モバイル コネクト ユーザは、Unified CM User Options インターフェイスを使用して、次の URL にある Web ベースの設定ページ経由で独自のモビリティ設定を構成できます。

   http://<*Unified-CM_Server_IP_Address*>/ccmuser/

   ここで、<*Unified-CM_Server_IP_Address*> は、Unified CM パブリッシャ サーバの IP アドレスです（図 25-20 のステップ 3 を参照）。

図 25-20　　モバイル コネクトのアーキテクチャ



モバイル コネクトのハイ アベイラビリティ

モバイル コネクト機能には、次のコンポーネントが必要です。

- Unified CM サーバ
- 公衆網ゲートウェイ

各コンポーネントの冗長性または弾力性を向上させて、さまざまな障害シナリオでモバイル コネクトの機能が失われないようにする必要があります。

Unified CM サーバの冗長性

モバイル コネクト機能には、Unified CM サーバが不可欠です。Unified CM Group による電話機とゲートウェイの登録が冗長になっていれば、Unified CM サーバが故障してもモバイル コネクト機能は影響を受けません。

モバイル コネクト ユーザが Unified CM User Options Web インターフェイスを使用してモビリティ設定（リモート接続先とアクセス リスト）を構成できるようにするには、Unified CM パブリッシャ サーバが使用可能である必要があります。パブリッシャがダウンすると、ユーザはモビリティ設定を変更できなくなります。同様に、管理者も Unified CM でモビリティ設定を変更できなくなります。ただし、既存のモビリティ設定と機能は維持されます。最後に、システムでモバイル コネクトのステータスに対する変更を Unified CM パブリッシャ サーバ上に記録する必要があります。Unified CM パブリッシャが使用できない場合は、モバイル コネクトの有効化または無効化が使用できなくなります。

公衆網ゲートウェイの冗長性

モバイル コネクト機能は、新しいコール レッグを公衆網に拡張してモバイル コネクト ユーザのリモート接続先電話機に到達する能力に依存しているため、公衆網ゲートウェイの冗長性は重要です。公衆網ゲートウェイが故障したり、容量不足の場合は、モバイル コネクト コールを完了できません。通常は、会社の IP テレフォニー ダイヤル プランを通して、物理的なゲートウェイの冗長性とコールの再ルーティング機能だけでなく、予想されるコール アクティビティを処理する十分な容量が提供されることによって、公衆網アクセスに冗長性が提供されます。Unified CM が、コール ルーティングの弾力性を確保するための十分な容量、複数のゲートウェイ、およびルート グループとルート リストの構造で構成されていれば、この冗長性によってモバイル コネクト機能の持続性が保証されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス

モバイル ボイス アクセス（システム リモート アクセスとも呼ばれる）とエンタープライズ機能アクセス 2 ステージ ダイヤリングは、モバイル コネクト アプリケーションに組み込まれている機能です。両方の機能を使用すれば、モビリティ対応ユーザは、外出先でも、Unified CM に直接接続されているかのように電話をかけることができます。この機能は、従来のテレフォニー環境では、一般的に、Direct Inward System Access（DISA）と呼ばれています。これらの機能を通して、通話料金を抑えたり、モバイル ユーザごとに通話料を請求するのではなく、直接会社に請求するように配慮することによって、会社にメリットがもたらされます。加えて、これらの機能を使用すれば、ユーザは、発信者 ID を外部に送信するときに、携帯電話やリモート接続先の番号を隠すことができます。代わりに、発信者 ID として、ユーザの会社の電話番号が送信されます。これによって、ユーザへの返信コールは会社の電話番号にかけられるため、コールを会社で一括管理できます。また、モバイル ユーザは、これらの機能を使用して、通常は企業外部から到達不能な内部の内線番号や DID 以外の会社の電話番号にダイヤルできます。

モバイル ボイス アクセスには、H.323 または SIP VoiceXML（VXML）ゲートウェイで応答および処理されるシステム設定の DID 番号を呼び出すことによってアクセスします。VoiceXML ゲートウェイによって、モバイル ボイス アクセス ユーザに対する双方向音声応答（IVR）プロンプトが再生され、ユーザ認証と電話機のキーパッド経由でダイヤルされる番号入力が要求されます。

エンタープライズ機能アクセス機能には、前述した通話切替機能や会議機能だけでなく、2 ステージ ダイヤリング機能が含まれています。2 ステージ ダイヤリングは、IVR プロンプトを除いて、モバイル ボイス アクセスと同様の方法で動作します。システム設定のエンタープライズ機能アクセス DID が Unified CM によって応答されます。ユーザは、電話機のキーパッドまたはスマート フォン ソフトキーを使用して、認証とダイヤルする番号を入力します。これらの入力はプロンプトなしで受信されます。

モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングの両方の機能を使用すれば、ユーザは、入力番号に対するコールが接続されたときに、通話切替機能を呼び出したり、モバイル コネクト コールと同様にデスクトップフォンでコールをピックアップしたりできます。この動作は、コールが会社のゲートウェイに固定されることによって可能になります。

モバイル ボイス アクセス IVR VoiceXML ゲートウェイ URL

モバイル ボイス アクセス機能を使用するには、Unified CM VoiceXML アプリケーションを H.323 または SIP ゲートウェイ上にインストールする必要があります。このアプリケーションをロードするための URL は次のとおりです。

http://<*Unified-CM-Publisher_IP-Address*>:8080/ccmivr/pages/IVRMainpage.vxml

ここで、<*Unified-CM-Publisher_IP-Address*> は、Unified CM パブリッシャ ノードの IP アドレスです。

モバイル ボイス アクセス機能

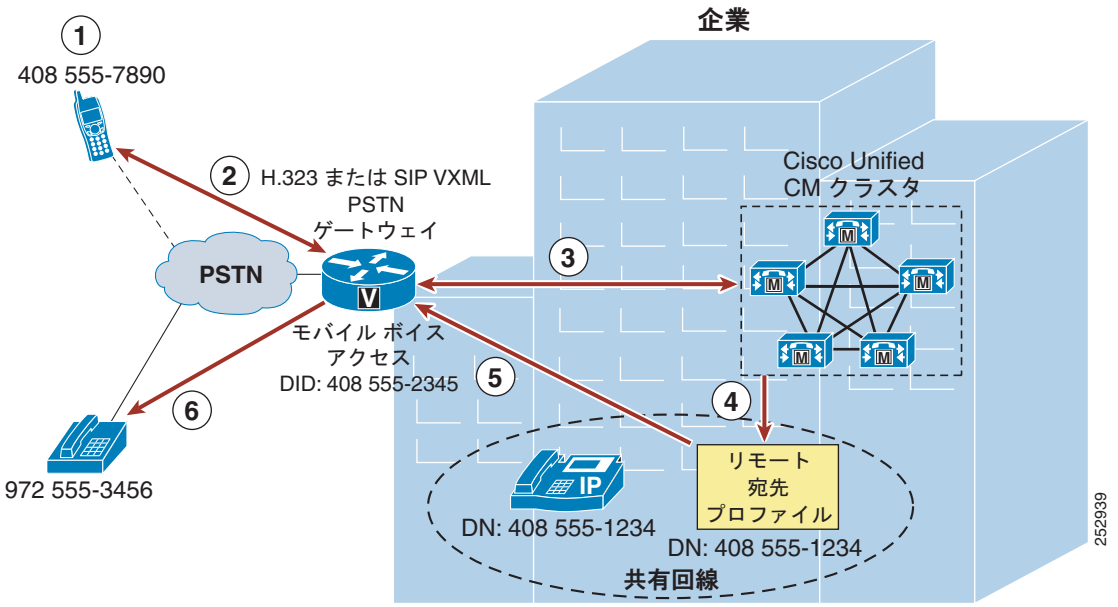
図 25-21 に、モバイル ボイス アクセスのコール フローを示します。この例では、モバイル ボイス アクセス ユーザが公衆網電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。

このコールは、VoiceXML ゲートウェイとしても機能する会社の公衆網 H.323 または SIP ゲートウェイに入ります。ユーザは、IVR 経由で、数字のユーザ ID（後ろに # 記号が続く）、PIN 番号（後ろに # 記号が続く）、および 1 の入力と、相手の電話番号が続くモバイル ボイス アクセス コールの発信を要求されます。この場合は、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します（ステップ 2）。

（注）　モバイル ボイス アクセス ユーザがかけている公衆網電話機が、そのユーザのモバイル コネクト リモート接続先として設定されており、Unified CM で着信コールの発信者 ID とこのリモート接続先を照合可能な場合は、数字のユーザ ID を入力する必要がありません。代わりに、PIN 番号の入力だけが要求されます。

その一方で、IVR プロンプトが Unified CM からゲートウェイに転送され、ゲートウェイでユーザに対してプロンプトが再生され、ゲートウェイでユーザの数字の ID と PIN 番号を含む入力が収集されます。この情報は、認証と 9 1 972 555 3456 へのコールを発信するために Unified CM に転送されます（ステップ 3）。ユーザの認証とダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイル経由のコールが発信されます（ステップ 4）。972 555-3456 への発信コールが、公衆網ゲートウェイ経由で経路設定されます（ステップ 5）。最後に、番号が 972 555-3456 の公衆網接続先電話機で呼出音が鳴ります（ステップ 6）。

図 25-21　モバイル ボイス アクセス



（注）　モバイル ボイス アクセスを図 25-21 のように動作させるには、システム全体の Enable Mobile Voice Access サービス パラメータが True に設定され、[End User] 設定ページでユーザごとに [Enable Mobile Voice Access] チェックボックスがオンになっていることを確認してください。

（注）　モバイル ボイス アクセス機能を使用するには、Unified CM Serviceability の設定ページで [Cisco Unified Mobile Voice Access Service] を手動でアクティブにする必要があります。このサービスは、パブリッシャ ノードでのみアクティブにできます。

ヘアピニングを使用したモバイル ボイス アクセス

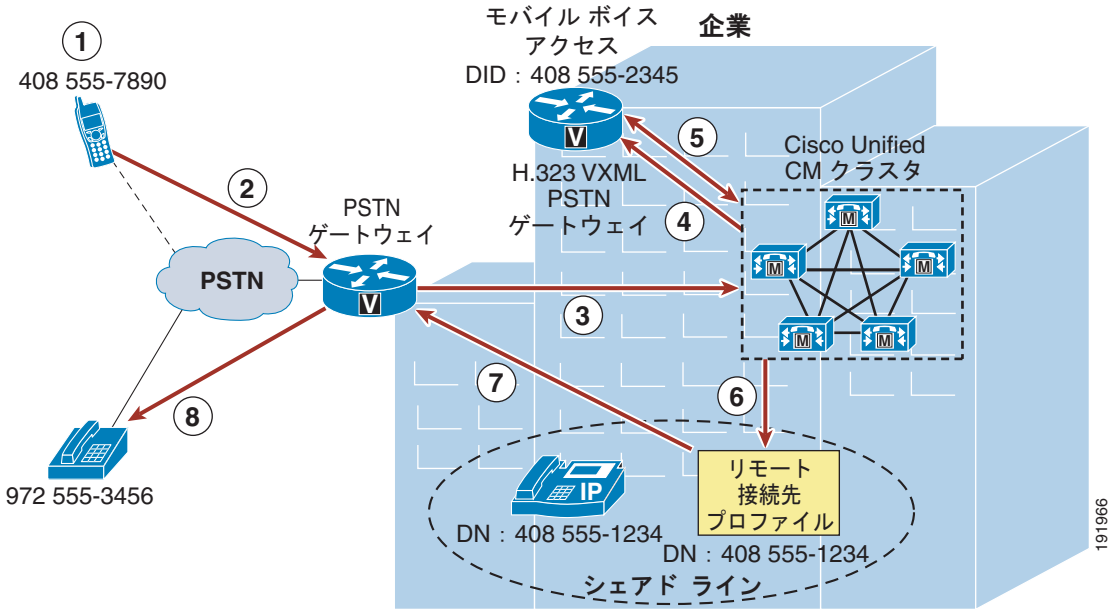
会社の公衆網ゲートウェイで H.323 または SIP が使用されていない配置では、H.323 を実行している別のゲートウェイ上のヘアピニングを使用することによってモバイル ボイス アクセス機能を提供することもできます。ヘアピニングを使用したモバイル ボイス アクセスの場合は、VoiceXML 機能を別の H.323 ゲートウェイに持たせる必要があります。図 25-22 に、ヘアピニングを使用したモバイル ボイス アクセスのコール フローを示します。この例では、前の例と同じく、モバイル ボイス アクセス ユーザが公衆網電話機（408 555-7890）からモバイル ボイス アクセス会社の DID DN 408-555-2345 にダイヤルします（ステップ 1）。コールが、会社の公衆網ゲートウェイに入ってきて（ステップ 2）、コール処理のために Unified CM に転送されます（ステップ 3）。Unified CM が着信コールを H.323 VoiceXML ゲートウェイにルーティングします（ステップ 4）。IVR がユーザに、自分の数字のユーザ ID と PIN、およびモバイル ボイス アクセス コールを作成するための 1 を入力し、続けて接続先の電話番号を入力するように求めます。この場合も、ユーザが相手の番号として 9 1 972 555 3456（後ろに # 記号が続く）を入力します。

（注）　ヘアピニングを使用したモバイル ボイス アクセスでは、システムを呼び出しているユーザが発信者 ID によって自動的に特定されません。代わりに、PIN を入力する前に、手動でリモート接続先の番号を入力する必要があります。ユーザが自動的に特定されない理由は、ヘアピニングを使用する配置では、公

衆網ゲートウェイにおいて最初にコールを Unified CM にルーティングして、ヘアピンされるモバイル ボイス アクセス ゲートウェイに到達する必要があるためです。コールが最初に Unified CM にルーティングされるため、発信番号が携帯の番号から会社の電話番号に変換されてから、コールがモバイル ボイス アクセス ゲートウェイによって処理されます。このため、モバイル ボイス アクセス ゲートウェイでは、発信番号と設定されているリモート接続先の照合を行うことができず、ユーザはリモート接続先番号の入力を求められます。これは、ヘアピニングを使用する配置に特有の現象です。通常のモバイル ボイス アクセスのフローにおいては、モバイル ボイス アクセス機能はローカル ゲートウェイで利用できるため、公衆網ゲートウェイで最初にコールを Unified CM にルーティングしてからモバイル ボイス アクセスにアクセスする必要がありません。

その間に、H.323 VoiceXML ゲートウェイは、ユーザ入力を収集して Unified CM に転送し、転送された IVR プロンプトを PSTN ゲートウェイおよびモバイル ボイス アクセス ユーザに対して再生します。これを受けて Unified CM がユーザ入力を受信し、ユーザを認証し、ユーザ入力に基づいて適切な IVR プロンプトを H.323 VoiceXML ゲートウェイに転送します（ステップ 5）。ダイヤルする番号の受信後に、Unified CM でユーザのリモート接続先プロファイルを使用したコールが発信されます（ステップ 6）。972 555-3456 への発信コールが、公衆網ゲートウェイ経由で経路設定されます（ステップ 7）。最後に、番号が 972 555-3456 の公衆網接続先電話機で呼出音が鳴ります（ステップ 8）。

図 25-22　　ヘアピニングを使用したモバイル ボイス アクセス



（注）　モバイル ボイス アクセスをヘアピニング モードで配置する場合は、公衆網ゲートウェイでのモバイル ボイス アクセス DID と Cisco Unified CM 内のモバイル ボイス アクセス電話番号（**Media Resources - Mobile Voice Access**）を別々の番号として設定することを推奨します。そうすれば、Unified CM 内のトランスレーション パターンを使用して、モバイル ボイス アクセス DID の着信番号を設定済みのモバイル ボイス アクセス電話番号に変換できます。Unified CM 内で設定されたモバイル ボイス アクセス電話番号は管理者にしか表示されないため、DID と電話番号間の変換をエンド ユーザが意識する必要はなく、エンド ユーザのダイヤリング動作に変更は生じません。この方法は、マルチクラスタ環境でのモビリティ コール ルーティング問題を回避するために推奨されています。この推奨事項は、非ヘアピニング モードのモバイル ボイス アクセスには当てはまりません。

（注）　ヘアピニング モードのモバイル ボイス アクセスは、H.323 VXML ゲートウェイだけでサポートされています。

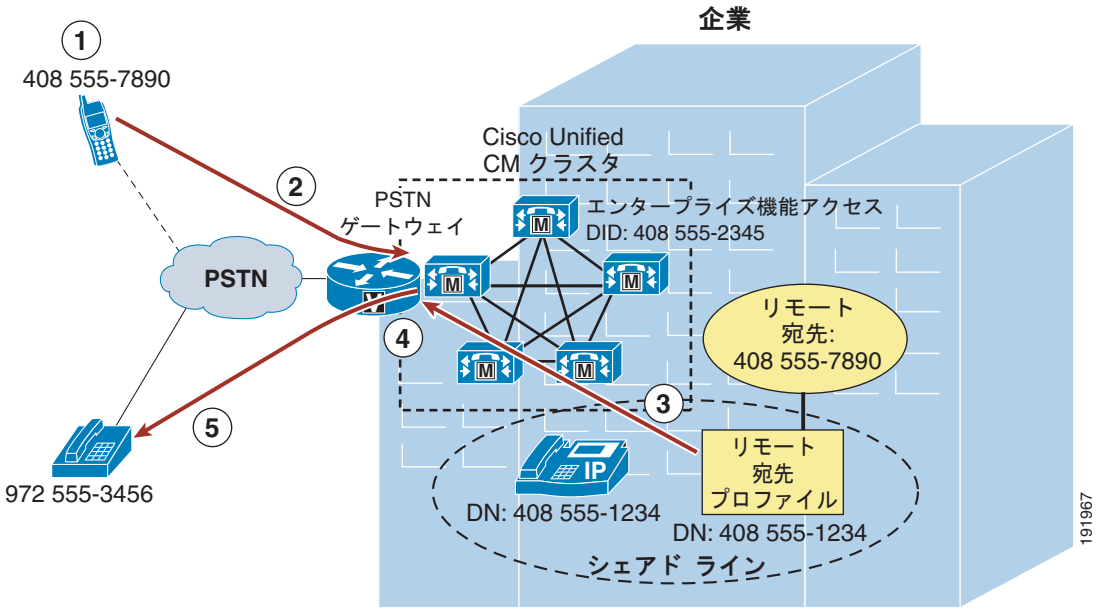
2 ステージ ダイヤリングを伴うエンタープライズ機能アクセス

図 25-23 に、エンタープライズ機能アクセス 2 ステージ ダイヤリングを示します。この例では、モビリティ ユーザがリモート接続先電話機（408 555-7890）からエンタープライズ機能アクセス DID 408 555-2345 にダイヤルします（ステップ 1）。コールが接続されると、Unified CM で認証されるユーザの PIN（後ろに # 記号が続く）で始まる DTMF 番号を公衆網ゲートウェイ経由で Unified CM に送信するためにリモート接続先電話機が使用されます。次に、2 ステージ ダイヤリング対象コールが試みられることを示す 1（後ろに # 記号が続く）と相手の電話番号が送信されます。この場合は、ユーザが接続先番号として 9 1 972 555 3456 と入力します（ステップ 2）。

（注）　モバイル ボイス アクセスとは違って、エンタープライズ機能アクセスでは、エンド ユーザ アカウントに対して発信者 ID と PIN を照合するためにリモート接続先として設定された電話機から、すべての 2 ステージ ダイヤリング対象コールを発信する必要があります。エンタープライズ機能アクセスにおいては、モビリティ ユーザが自身を識別するためのリモート接続先番号または ID をシステムに入力するための仕組みは用意されていません。同一性は、着信コールの発信者 ID と入力された PIN の組み合せを通してのみ確立できます。

次に、発信コールがユーザのリモート接続先プロファイル経由で開始され（ステップ 3）、公衆網番号 972 555-3456 へのコールが会社の公衆網ゲートウェイ経由で経路設定されます（ステップ 4）。最後に、公衆網電話機が呼び出されます（ステップ 5：この場合は 972 555-3456）。モバイル ボイス アクセスと同様に、各エンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールの音声メディア パスは、2 つのゲートウェイ ポートを使用している公衆網ゲートウェイ内でヘアピンされます。

図 25-23　　エンタープライズ機能アクセス 2 ステージ ダイヤリング機能



（注）　エンタープライズ機能アクセス 2 ステージ ダイヤリングを図 25-23 のように動作させるには、システム全体の Enable Enterprise Feature Access サービス パラメータが True に設定されていることを確認してください。

デスクトップフォンとリモート接続先電話機のピックアップ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能はモバイル コネクトと緊密に統合されているため、モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリング対象コールが確立されていれば、ユーザはモバイル コネクト機能を利用して、最初に着信した電話機をオン フックしてデスクトップフォンの [Resume] ソフトキーを押すだけで、または、通話切替保留機能を使用して、通話中のコールをデスクトップフォンでピックアップできます。さらに、その後で、ユーザの設定済みリモート接続先電話機で [Mobility] ソフトキーを押して Send Call to Mobile Phone を選択することによって、そのコールをピックアップできます。

モバイル コネクトの有効化と無効化

モバイル ボイス アクセスとエンタープライズ機能アクセスのユーザにまるで社内にいるかのように公衆網から電話がかけられる能力を提供することに加えて、H.323 または SIP VoiceXML ゲートウェイ上のモバイル ボイス アクセスで提供される機能とエンタープライズ機能アクセスで提供される機能によって、電話機のキーパッド経由でリモート接続先ごとのモバイル コネクト機能をリモートで有効または無効にできる能力もユーザに提供されます。1 を入力して電話をかけるのではなく、ユーザは、2 を入力してモバイル コネクト機能を有効にし、3 を入力してモバイル コネクト機能を無効にします。

モバイル ボイス アクセスを使用するにあたって、複数のリモート接続先を設定する場合は、モバイル コネクト機能を有効または無効にするリモート接続先の電話番号を入力するように要求されます。エンタープライズ機能アクセスでは、呼び出しているリモート接続先電話機のモバイル コネクトしか有効/無効にできません。

（注）　Enable Mobile Voice Access サービス パラメータが False に設定されており、2 ステージ ダイヤリング対象コールを行うことができない場合でも、モバイル ボイス アクセスでは、リモートからモバイル コネクトをユーザが有効または無効にする機能が提供されます。システムにモバイル ボイス アクセス電話番号が設定され、ユーザのアカウントでモバイル ボイス アクセスが有効にされて、Cisco Unified Mobile Voice Access サービスがパブリッシャ上で実行されている限り、発信側のユーザはモバイル コネクトを有効または無効にできます。

モバイル ボイス アクセスとエンタープライズ機能アクセスの番号拒否

管理者は、モバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリングのユーザが、それらの機能の使用中は特定の番号にダイヤルできないようにできます。オフネット コールに対してこれらの機能を使用している場合に特定の番号へのコールを制限または拒否するには、[System Remote Access Blocked Numbers] サービス パラメータ フィールドでそのような番号のカンマ区切りのリストを設定できます。このパラメータに拒否する番号を設定したら、モバイル ボイス アクセスまたはエンタープライズ機能アクセスが使用されている場合は、ユーザのリモート接続先電話機からそれらの番号にダイヤルできなくなります。管理者が拒否したい番号には、911 などの緊急電話番号を含めることができます。拒否する番号を設定する場合は、会社のユーザが該当するプレフィックスまたは振り分け用の数字を付けてダイヤルするようにそれらの番号が設定されていることを確認してください。たとえば、緊急電話番号を拒否対象とし、システム ユーザが緊急電話番号をダイヤルするときは 9911 を使用しなければならない場合は、[System Remote Access Blocked Numbers] フィールドに設定する番号を 9911 にする必要があります。

モバイル ボイス アクセスおよびエンタープライズ機能アクセスのアクセス番号

Unified CM システムでは、1 つのモバイル ボイス アクセス電話番号と 1 つのエンタープライズ機能アクセス番号だけを設定することもできますが、これらの内部で設定された番号にアクセス可能な外部番号を複数使用できます。たとえば、米国の New York に配置されたシステム、San Jose のリモート サイト、および London の海外サイトがある場合を考えます。システムのモバイル ボイス アクセス電話番号が 555-1234 に設定されている場合でも、各ロケーションのゲートウェイを設定して、ローカル DID 番号またはフリーダイヤル DID 番号をこのモバイル ボイス アクセス電話番号にマッピングできます。たとえば、New York のゲートウェイの DID である +1 212 555 1234 と +1 800 555 1234 の両方をモバイル ボイス アクセス番号にマッピングし、さらに San Jose のゲートウェイの DID +1 408 666 5678 および London のゲートウェイの DID +44 208 777 0987 もシステムのモバイル ボイス アクセス番号にマッピングできます。システム管理者は、複数のローカル DID 番号またはフリーダイヤル DID 番号を用意することによって、2 ステージ ダイヤリング対象コールが常にローカルまたはフリーダイヤルのコールとしてシステムに発信されるようにでき、さらにテレフォニー関連コストを削減できます。

リモート接続先の設定と発信者 ID の照合

モバイル ボイス アクセス機能およびエンタープライズ機能アクセス 2 ステージ ダイヤリング機能に加えて、通話切替機能の転送と会議のユーザを認証するときに、発信元のリモート接続先電話機の発信者 ID がシステム内で設定されたすべてのリモート接続先に対して照合されます。この発信者 ID の照合は、リモート接続先番号の設定方法、システム上で Application Dial Rules が設定されているかどうか、Matching Caller ID with Remote Destination パラメータが Partial Match と Complete Match のどちらに設定されているかなどの複数の要因に左右されます。

この照合の特性を制御するために、次の 2 つのアプローチを検討してください。

Application Dial Rules の使用

このアプローチでは、発信者 ID が公衆網から供給されているかのようにリモート接続先を設定します。たとえば、リモート接続先電話機の発信者 ID を公衆網から 4085557890 として供給する場合は、[Remote Destination] 設定ページでこの番号を設定する必要があります。モバイル コネクト コールを適切にこのリモート接続先に経路設定するには、Application Dial Rules を使用して必要な公衆網アクセス コードなどの数字を前に付加する必要があります。たとえば、公衆網にかける場合は 9 が必要で、長距離電話にかける場合は 1 が必要な場合は、[Prefix With Pattern] フィールドを 91 に設定した Application Dial Rules を作成する必要があります。このアプローチを使用する場合は、[Matching Caller ID with Remote Destination] パラメータを [Complete Match] のデフォルト設定のままにする必要があります。

（注） Application Dial Rules はモバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスのコールに適用されるだけでなく、Cisco WebDialer、Cisco Unified CM Assistant、および Cisco Unified Personal Communicator アプリケーションから発信されたコールにも適用されます。したがって、すべてのアプリケーションを通してダイヤリング動作が期待どおりに機能するように、これらの規則を慎重に設定する必要があります。

Application Dial Rules の代わりとして、適切な公衆網振り分け用数字を先頭に付加するために、Cisco Unified CM ルート リストおよびルート グループ構造内部のトランスレーション パターンまたは数字プレフィックス メカニズムを使用できます。

部分発信者 ID 照合の使用

このアプローチでは、リモート接続先が、システムから公衆網にダイヤルされたかのように設定されます。たとえば、リモート接続先の番号が 14085557890 で、システムから公衆網にアクセスするために 9 を入力する必要がある場合は、[Remote Destination] 設定ページでこの番号を 914085557890 に設定

する必要があります。このアプローチでは、Application Dial Rules を必要としませんが、[Matching Caller ID with Remote Destination] サービス パラメータを [Partial Match] に設定し、[Number of Digits for Caller ID Partial Match] をリモート接続先発信者 ID に対して照合すべき連続桁数を表す数字に設定する必要があります。たとえば、リモート接続先の発信者 ID が 14085557890 で、リモート接続先が 914085557890 に設定されている場合は、[Number of Digits for Caller ID Partial Match] を 10 または 11 に設定するのが理想的です。この例では、このパラメータをさらに少ない桁数に設定できます。ただし、システム内のすべての設定済みリモート接続先を一意的に識別できるように十分な連続桁数が照合されることを保証してください。部分発信者 ID 照合を使用したときに完全な一致が見つからず、複数の設定済みリモート接続先が一致した場合は、システムで一致するリモート接続先番号が存在しないものとして処理されます。したがって、モバイル ボイス アクセスの場合は、PIN を入力する前にリモート接続先番号 /ID を手動で入力する必要があります。エンタープライズ機能アクセスには、ユーザがリモート接続先番号を入力するメカニズムがありません。そのため、この機能を使用する場合は、一致が一意的にしか発生しないことを確認してください。

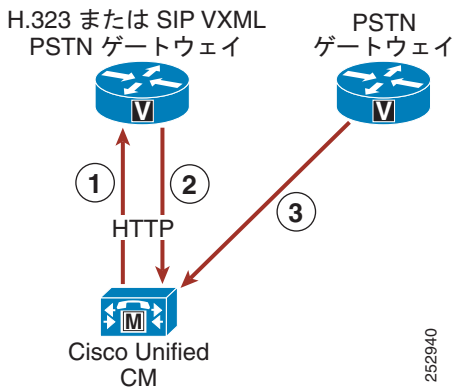
（注）　公衆網サービス プロバイダーが可変長の発信者 ID を送信する場合は、着信コールごとの一意的な発信者 ID の一致が保証できない可能性があるため、部分発信者 ID 照合の使用は推奨できません。このようなシナリオでは、完全発信者 ID 照合の使用を推奨します。

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ

モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャを理解することは、それらの機能性を理解することと同じくらい重要です。図 25-24 は、モバイル ボイス アクセスとエンタープライズ機能アクセスに必要なメッセージ フローとアーキテクチャを示しています。Unified CM、公衆網ゲートウェイ、および H.323 または SIP VXML ゲートウェイの間には、次の一連の対話とイベントが発生します。

1. Unified CM から HTTP 経由で IVR プロンプトとインストラクションが H.323 または SIP VXML ゲートウェイに転送されます（図 25-24 のステップ 1 を参照）。これによって、VXML ゲートウェイで着信モバイル ボイス アクセス発信者に対してこれらのプロンプトを再生できます。
2. H.323 または SIP VXML ゲートウェイでは、HTTP を使用してモバイル ボイス アクセス ユーザの入力が Unified CM に戻されます（図 25-24 のステップ 2 を参照）。
3. 公衆網ゲートウェイでは、リモート接続先電話機からのエンタープライズ機能アクセス 2 ステージ ダイヤリングおよび通話切替機能に関するユーザまたはスマート フォンのキー シーケンスに応答して DTMF 番号が転送されます（図 25-24 のステップ 3 を参照）。

図 25-24　モバイル ボイス アクセスとエンタープライズ機能アクセスのアーキテクチャ



（注）　図 25-24 では公衆網ゲートウェイとは別のボックスとして H.323 または SIP VoiceXML ゲートウェイが描かれていますが、これはアーキテクチャ上の要件ではありません。公衆網ゲートウェイで H.323 または SIP 以外のプロトコルを実行する必要がなければ、VoiceXML 機能と公衆網ゲートウェイ機能を同じボックスで処理できます。H.323 または SIP ゲートウェイは、モバイル ボイス アクセス VoiceXML 機能に不可欠です。

モバイル ボイス アクセスおよびエンタープライズ機能アクセスのハイ アベイラビリティ

モバイル ボイス アクセス機能とエンタープライズ機能アクセス機能には、モバイル コネクト機能と同じコンポーネントと冗長性メカニズムが必要です（「モバイル コネクトのハイ アベイラビリティ」（P.25-47）を参照）。Unified CM Group は、公衆網ゲートウェイ登録の冗長性に欠かせません。同様に、公衆網の物理ゲートウェイとゲートウェイ接続の冗長性を提供する必要があります。公衆網と会社間の冗長なアクセスは、ゲートウェイが故障した場合に、リモート接続先電話機からモバイル ボイス アクセス機能とエンタープライズ機能アクセス機能にアクセスするために必要です。ただし、必要に応じて、H.323 または SIP VoiceXML ゲートウェイに対して物理的な冗長性を提供できますが、Unified CM 上には、Cisco Unified Mobile Voice Access サービス用の冗長性メカニズムがありません。このサービスは、パブリッシャ ノードでしか有効にして実行することができません。そのため、パブリッシャ ノードが無効な場合は、モバイル ボイス アクセス機能が使用できません。エンタープライズ機能アクセスと 2 ステージ ダイヤリング機能には、このようなパブリッシャとの依存関係がないため、モビリティ ユーザに同等の機能性（IVR プロンプトが再生されない）を提供できます。

Cisco Unified Mobility の配置の設計

Cisco Unified Mobility ソリューションでは、Cisco Unified CM を介してモビリティ機能が提供されます。機能には、モバイル コネクト、モバイル ボイス アクセス、およびエンタープライズ機能アクセスが含まれます。この機能を配置する場合は、ダイヤル プランの意味、ガイドラインと制約事項、および性能と容量に関する考慮事項を理解しておくことが重要です。

Cisco Unified Mobility のダイヤル プランに関する考慮事項

Unified Mobility を適切に設定してプロビジョニングするには、リモート接続先プロファイル設定のコール ルーティング動作とダイヤル プランの意味を理解しておくことが重要です。

リモート接続先プロファイルの設定

Unified Mobility を設定する場合は、[Remote Destination Profile] 設定ページにある次の 2 つの設定を考慮する必要があります。

- コーリング サーチ スペース

  この設定と電話番号または回線レベルのコーリング サーチ スペース（CSS）を組み合せて、モビリティ ダイヤル対象コール用にアクセス可能なパーティションが決定されます。この設定は、モバイル ボイス アクセスとエンタープライズ機能アクセス 2 ステージ ダイヤリングを含む、リモート接続先電話機からのモビリティ ユーザによるコールだけでなく、通話切替の転送機能と会議機能の組み合せによるコールにも影響します。この CSS と回線レベルの CSS の組み合せの中に、ユーザのリモート接続先電話機から発信されたビジネス コールのためにアクセスする必要のあるすべてのパーティションが含まれていることを確認してください。

- コーリング サーチ スペースの再ルーティング

  この設定によって、ユーザのリモート接続先電話機にコールが送信されたときにアクセスするパーティションが決定されます。このことは、すべてのモバイル コネクト コールに当てはまります。ユーザの会社の電話番号へのコールもモバイル コネクト経由でユーザのリモート接続先に送信される場合は、この CSS によってシステムからリモート接続先電話機に到達する方法が決定されます。したがって、CSS を通して、公衆網またはモバイル ボイス ネットワークに到達するために、適切なルート パターンとゲートウェイを含むパーティションにアクセスできる必要があります。

リモート接続先プロファイル ルーティング CSS を設定する場合は、この CSS 内のルート パターンが、ユーザのデスクトップフォンへの着信コールを経路設定するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることを推奨します。これによって、コールをリモート接続先に経路設定するときに、2 地点間の帯域幅不足によるコール アドミッション制御拒否が発生しなくなります。さらに、WAN 帯域幅が不十分な場合は、初期モバイル コネクト コールの経路設定後のコール アドミッション制御チェックで拒否されないため、同じコール アドミッション制御ロケーション内のゲートウェイに着信コール レッグと発信コール レッグを経路設定することによって、このコール中の以降のデスクトップフォンまたはリモート接続先のピックアップ動作で WAN 帯域幅のオーバーサブスクリプションが発生する可能性のあるコール アドミッション制御の必要がなくなることが保証されます。

同様に、発信モバイル ボイス アクセスまたはエンタープライズ機能アクセス 2 ステージ ダイヤリング コール ルーティング用のリモート接続先プロファイル CSS を設定する場合は、このコーリング サーチ スペース内のルート パターンが、モバイル ボイス アクセスまたはエンタープライズ機能アクセス DID への着信コール レッグを処理するゲートウェイと同じコール アドミッション制御ロケーションにあるゲートウェイを指すようにすることを推奨します。これによって、ダイヤル先番号への初期発信コール ルーティング中に帯域幅不足によるコール アドミッション制御拒否が発生しないことが保証されます。ただし、デスクトップフォンがモバイル ボイス アクセスまたはエンタープライズ機能アクセス DID が転送されるゲートウェイとは異なるコール アドミッション制御ロケーション内に存在する場合は、以降のデスクトップフォンのピックアップによって、WAN 帯域幅のオーバーサブスクリプションが発生する可能性があることに注意してください。

最後に、モビリティ対応ユーザへの着信公衆網コールは、必ず、会社のデスクトップフォンの DID に基づいてホーム ロケーション ゲートウェイに入るため、モビリティ対応ユーザが、別のサイトでのエクステンション モビリティ ログインまたは別のコール アドミッション制御ロケーションへのデスクトップフォンの物理的移動が原因でコール アドミッション制御ロケーションを移動していた場合は、着信コールが入るゲートウェイと同じコール アドミッション制御ロケーション内に配置された発信ゲートウェイを指すことがほとんど不可能になります。そのため、モビリティ対応ユーザがエクステンション モビリティを使用して、ホーム ロケーション外部のコール アドミッション制御ロケーション内の電話機にログインしたり、コール アドミッション制御ロケーション間でデバイスを物理的に移動したりするシナリオや配置は避けることを推奨します。このようなシナリオを回避または制限することができない場合は、コール アドミッション制御拒否が原因のコール レッグ障害またはデスクトップフォンやリモート接続先のピックアップ アクティビティが原因の WAN オーバーサブスクリプションが発生する確率が高くなります。

自動発信者 ID 照合とエンタープライズ コール アンカリング

理解しておく必要のある Unified Mobility ダイヤル プランのもう一つの側面は、設定済みのリモート接続先電話機からの着信コールに対する自動発信者 ID 識別に関するシステム動作です。着信コールがシステムに入ると、そのコールに対して提供された発信者 ID が設定済みのすべてのリモート接続先電話機と比較されます。一致するものが見つかった場合は、そのコールが自動的にその会社のものと固定されるため、ユーザは通話切替機能を呼び出したり、通話中のコールをデスクトップフォンでピックアップできます。この動作は、着信コールがモバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用したモビリティ コールとして開始されていない場合でも、モビリティ ユーザのリモート接続先電話機からの着信コールすべてに対して行われます。

（注）　設定済みのリモート接続先番号に対する自動着信コール発信者 ID 照合は、Matching Caller ID with Remote Destination サービス パラメータが Partial Match と Complete Match のどちらに設定されているかの影響を受けます。この設定に関する詳細については、「リモート接続先の設定と発信者 ID の照合」（P.25-54）を参照してください。

自動エンタープライズ コール アンカリングに加えて、設定済みのリモート接続先電話機から会社に電話がかかった場合の着信コール ルーティングと発信コール ルーティングも考慮する必要があります。設定済みのリモート接続先からのコールに対する着信コール ルーティングは、Inbound Calling Search Space for Remote Destination サービス パラメータの設定によって次の 2 つの方法のどちらかで発生します。デフォルトで、このサービス パラメータは、**Trunk or Gateway Inbound Calling Search Space** に設定されます。このサービス パラメータがデフォルト値に設定されている場合は、設定済みのリモート接続先からの着信コールが、公衆網ゲートウェイの着信コーリング サーチ スペース（CSS）またはコールが入るトランクを使用して経路設定されます。一方、Inbound Calling Search Space for Remote Destination パラメータが **Remote Destination Profile + Line Calling Search Space** に設定されている場合は、リモート接続先からの着信コールが、公衆網ゲートウェイの着信 CSS またはトランクをバイパスして、代わりに、リモート接続先プロファイル CSS（と回線レベル CSS の組み合せ）を使用して経路設定されます。

リモート接続先電話機からの着信コールの特性を考えると、このような着信コールへのアクセスを社内の電話機に到達させるために必要なすべてのパーティションに提供するためには、コーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切なコール ルーティングが保証されます。

（注）　設定済みのリモート接続先電話機からではない着信コールでは、必ず、トランクまたはゲートウェイ着信 CSS が使用されるため、Inbound Calling Search Space for Remote Destination サービス パラメータの影響を受けません。

モバイル ボイス アクセスまたはエンタープライズ機能アクセス コールの発信コール ルーティングでは、必ず、リモート接続先プロファイル回線 CSS とデバイス レベル CSS を連結したものが使用されるため、オフネットまたは公衆網アクセスに必要なすべてのルート パーティションへのアクセスを提供するためには、これらのコーリング サーチ スペースが適切に設定されていることを確認する必要があります。これによって、リモート接続先電話機からの適切な発信コール ルーティングが保証されます。

Intelligent Session Control

Intelligent Session Control 機能を使用すると、設定されたリモート接続先番号への社内からの直接コールを、自動的にコール アンカリングできます。通常、モビリティ コール アンカリングは、ユーザの会社の電話番号にかけられたコール、またはユーザの会社の電話番号からかけられたコールでだけ行われます。Intelligent Session Control 機能を有効にすると、社内からリモート接続先への直接コールが固定されます。また、Dial-via-office または 2 ステージ ダイヤリングによって外部から発信されたコールは、内部コールとしてルーティングされるため、これらのコールも固定されます。

この機能は、Reroute Remote Destination Calls to Enterprise Number サービス パラメータを True に設定することによって有効にします。デフォルトで、このサービス パラメータは False に設定されており、この機能は無効になっています。この機能を有効にすると、ダイヤルされたリモート接続先へのコールが公衆網経由でルーティングされるだけでなく、コールが自動的に会社のゲートウェイ内部で固定されます。このタイプのコールを固定することによって、着信側モバイル ユーザが通話切替機能およびデスクトップフォンのピックアップまたはセッション ハンドオフを呼び出すことができるようになります。

たとえば、Intelligent Session Control 機能が有効にされており、モビリティ対応ユーザのリモート接続先番号が携帯の番号に対応する 408 555 1234 として設定されているとします。別のユーザがデスクトップフォンからそのモビリティ対応ユーザのリモート接続先番号（408 555 1234）にダイヤルすると、そのコールは公衆網経由でリモート接続先にルーティングされ、同時に会社のゲートウェイで固定されます。コールがセットアップされて固定されると、着信側モビリティ対応ユーザは、保留、転送、会議などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできるようになります。

この同じ例で、Intelligent Session Control 機能が無効であるとすると、システム ユーザがこのモビリティ対応ユーザのリモート接続先に社内のデスクトップフォンから直接ダイヤルした場合、そのコールは公衆網経由で着信側リモート接続先にルーティングされますが、固定はされません。その結果、モバイル ユーザは、保留や転送などの通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできません。

この機能を有効にする場合は、ダイヤル プランの設定およびコール ルーティングへの影響を理解することが重要となります。この機能を呼び出すには、内部ユーザが公衆網のリモート接続先番号に到達するためにダイヤルする番号（必要なすべての公衆網振り分け用数字を含む）は、システムに設定されているリモート接続先（またはモビリティ ID）番号と一致する必要があります。たとえば、リモート接続先番号がシステムに 408 555 1234 と設定されており、通常、発信する番号に加えて公衆網振り分け用数字 91 を内部ユーザがダイヤルする必要がある場合は、再ルーティングおよびそれによるエンタープライズ コール アンカリングは実行されません。これは、ユーザが公衆網のリモート接続先に到達するために 91 408 555 1234 をダイヤルした一方、リモート接続先は 408 555 1234 と設定されており、これらの番号が一致しないためです。

この機能が適切に機能するには、設定されたリモート接続先と、公衆網のこのリモート接続先に到達するためにダイヤルする必要がある番号とが一致する必要があります。これらの番号が一致するようにするには、Matching Caller ID with Remote Destination サービス パラメータを **Partial Match** に設定します。このパラメータを Partial Match に設定し、Number of Digits for Caller ID Partial Match サービス パラメータを使用して部分一致対象桁数を指定することによって、ダイヤルされた番号に公衆網振り分け用数字が含まれていても、設定されたリモート接続先番号とダイヤルされた番号が一致します。

前の例を使用し、システムが 10 桁の部分一致を使用するように設定されているとすると、ダイヤルされた番号 9 1 408 555 1234 は、設定されたリモート接続先 408 555 1234 に一致します。これは、部分一致では、Number of Digits for Caller ID Partial Match に指定された桁数（この場合は 10 桁）が照合されるためです。2 つの番号は、右から左に向かって照合されます。ダイヤルされた番号 9 1 408 555 1234 の最後の 10 桁は 408 555 1234 であり、この 10 桁が、10 桁の設定されたリモート接続先（408 555 1234）に一致します。この例では、発信コールは社内で固定され、着信側モバイル ユーザは通話切替機能を呼び出したり、デスクトップフォンのピックアップまたはセッション ハンドオフを実行したりできます。

この機能を使用する場合、一見すると、必要なすべての公衆網振り分け用数字を含むリモート接続先番号またはモビリティ ID 番号を設定する方が簡単に見えます。しかし、必要な公衆網振り分け用数字を含む番号を設定し、発信者 ID の部分一致を設定していない場合、設定されたリモート接続先またはモビリティ ID からの着信コールに対して発信者 ID の自動照合およびエンタープライズ アンカリングを実行できません。前の例では、リモート接続先番号が 9 1 408 555 1234 と設定されており、発信者 ID の完全一致が使用されている場合、リモート接続先からの着信コールの発信者 ID は 408 555 1234 となり、これらの番号が一致せず、リモート接続先からの着信コールが想定どおりに固定されません。

このように発信コールでダイヤルされる Intelligent Session Control 機能を使用する場合には、番号と、着信コールの設定されたリモート接続先番号が異なる可能性があるため、公衆網に到達するために 1 つ以上の振り分け用数字が必要なすべての配置において、発信者 ID の（完全一致ではなく）部分一致を有効にすることを推奨します。これにより、公衆網振り分け用数字を使用してリモート接続先番号に直接発信されたコールが一致し、固定されるようになります。一方で、公衆網に到達するために振り分け用数字が必要なく、ユーザが完全な E.164 番号をダイヤルして公衆網にコールをルーティングできる場合には、発信者 ID と照合されるリモート接続先の番号が、公衆網のリモート接続先またはモビリティ ID に到達するために内部ユーザがダイヤルする番号と同じであるため、発信者 ID の完全一致設定を使用することを推奨します。

Intelligent Session Control 機能を有効にする場合は、再ルーティング機能の実行時の、会社の回線およびリモート接続先回線の動作を理解することも重要です。コールの再ルーティングでは、Do Not Disturb（DND）、Access Lists と Time of Day コール フィルタリング、および Delay Before Ringing Timer の各リモート接続先回線設定は無視されます。再ルーティングされるすべてのコールは、フィルタリングされずにすぐにルーティングされます。会社のデスクトップフォン回線設定も、デフォルトで無視されるか、またはバイパスされます。ただし、Ignore Call Forward All on Enterprise DN サービス パラメータを False に設定することによって、再ルーティング機能の実行時に会社のデスクトップフォン回線の Call Forward All 設定を有効にできます。このパラメータが False に設定されている場合、会社のデスクトップフォン回線に Call Forward All の接続先が設定されていると、再ルーティングの実行時にコールはリモート接続先にルーティングされません。代わりに、コールは Call Forward All の接続先にルーティングされます。デフォルトで、このサービス パラメータは True に設定されており、会社のデスクトップフォン回線の Call Forward All 設定は無視されます。

発信者 ID 変換

設定済みのリモート接続先番号によってクラスタに発信されたコールは、自動的に、発信者 ID または発番号が、発信元のリモート接続先電話機の番号から関連する会社のデスクトップフォンの番号に変更されます。たとえば、408 555-7890 という番号のリモート接続先電話機が設定され、555-1234 という番号の会社のデスクトップフォンに関連付けられている場合は、クラスタ内の任意の電話番号に向けられたユーザのリモート接続先電話機からのコールがすべて、自動的に、発信者 ID が 408 555-7890 のリモート接続先電話番号から 555-1234 の会社の電話番号に変更されます。これによって、アクティブ コールの発信者 ID 表示とコール履歴ログの発信者 ID に、ユーザの携帯電話の番号ではなく、会社の卓上電話の番号が反映され、すべての返信コールがユーザの会社の電話番号に対して発信され、このようなコールが会社に固定されることが保証されます。

同様に、リモート接続先電話機から外部の公衆網接続先へのコールと、モバイル ボイス アクセスやエンタープライズ機能アクセス 2 ステージ ダイヤリング経由で会社に固定されたコール、つまり、モバイル コネクトの結果として公衆網に分岐されたコールも、発信者 ID が発信元のリモート接続先電話機の番号から関連する会社の電話番号に変更されます。

最後に、発番号を会社の電話番号ではなく、会社の DID 番号として外部の公衆網電話機に供給する場合は、発信側のトランスフォーメーション パターンを使用できます。発信側のトランスフォーメーション パターンを使用して発信者 ID を会社の電話番号から会社の DID に変換することによって、外部の接続先からの返信コールは、完全な会社の DID 番号でダイヤルされていることから、その会社に固定されます。このような変換とダイヤル プランの意味については、「Cisco Unified Mobility 固有の考慮事項」（P.9-112）を参照してください。

Unified Mobility に関するガイドラインと制約事項

次のガイドラインと制約事項は、Unified CM テレフォニー環境内のモバイル コネクトの配置と動作に関連して適用されます。

- モバイル コネクトは、PRI TDM 公衆網接続でだけサポートされます。T1 接続または E1-CAS、FXO、FXS、および BRI 公衆網接続はサポートされません。この PRI 要件は、完全な機能サポートを保証するためには、Cisco Unified CM で公衆網からの迅速な応答と切断の指示を受信する必要があることに基づいています。応答指示は、モバイル コネクト コールが特定のリモート接続先で応答されたときに、Cisco Unified CM でデスクトップフォンとその他のリモート接続先の呼び出しを停止するために必要です。加えて、応答指示は、シングル企業ボイスメール ボックス機能をサポートするために必要です。最後に、切断指示はデスクトップフォンピックアップのために必要です。PRI 公衆網接続では、必ず、応答指示または切断指示が提供されます。
- Cisco IOS Unified Border Element によって Unified CM SIP トランクとサービス プロバイダー トランクとの間に境界ポイントが提供されており、通話切替機能（またはその他の DTMF 依存の機能）が使用されていない場合には、SIP トランク VoIP 公衆網接続でもモバイル コネクトがサポー

トされます。VoIP 公衆網接続では、通話切替機能はサポートされません。VoIP ベースの公衆網接続では、VoIP ベースの公衆網接続によって提供されるエンドツーエンドのシグナリング パスによって、Unified CM に迅速な応答と切断の指示を提供できます。

- モバイル コネクトでは、ユーザあたり最大 2 つの同時コールをサポートできます。それ以上の着信コールは、自動的に、ユーザのボイスメールに転送されます。
- モバイル コネクトは、Multilevel Precedence and Preemption（MLPP）と連動しません。コールが MLPP によって割り込まれた場合は、そのコールに対するモバイル コネクト機能が無効になります。
- モバイル コネクト サービスでは、ビデオ コールに応答できません。デスクトップフォンで受信されたビデオ コールは携帯電話でピックアップできません。
- Unified CM の強制承認コード（FAC）機能とクライアント識別コード（CMC）機能が、モバイル ボイス アクセスと連動しません。
- リモート接続先は、別のクラスタまたはシステム上の時分割多重（TDM）装置またはオフシステム IP 電話にする必要があります。IP 電話は、リモート接続先と同じ Unified CM クラスタ内に設定できません。

ガイドラインと制約事項の詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications Manager Features and Services Guide*』の最新版で Cisco Unified Mobility に関する情報を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Cisco Unified Mobility のキャパシティ プランニング

Cisco Unified Mobility では、次の容量がサポートされます。

- Cisco MCS 7845 サーバまたは同等 Open Virtual Archive（OVA）サーバを使用したクラスタあたり最大 15,000 人のモビリティ対応ユーザ。
- Cisco MCS-7835 または同等 OVA サーバを使用したクラスタあたり最大 10,000 人のモビリティ対応ユーザ。
- Cisco MCS 7825 または同等 OVA サーバを使用したクラスタあたり最大 4,000 人のモビリティ対応ユーザ。
- MCS 7845 ノードまたは同等 OVA サーバあたり最大 3,750 台のリモート接続先、またはクラスタあたり 15,000 台の接続先。
- MCS 7835 または同等 OVA サーバあたり最大 2,500 台のリモート接続先、またはクラスタあたり 10,000 台。
- MCS 7825 または同等 OVA サーバあたり最大 1,000 台のリモート接続先、またはクラスタあたり 4,000 台。

（注）　モビリティ対応ユーザは、リモート接続先プロファイルを持ち、1 つ以上のリモート接続先またはモビリティ ID が設定されているユーザとして定義されます。

サポートされるモビリティ対応ユーザの最大数は、ユーザごとに設定されたリモート接続先またはモビリティ ID の数に依存します。前述したモビリティ対応ユーザの最大数は、ユーザあたり 1 つのリモート接続先またはモビリティ ID を想定しています。ユーザあたりのリモート接続先数またはモビリティ ID 数が増加するほど、サポートされるモビリティ対応ユーザ数が減少します。

上の数字が最大容量です。ただし、結果的に、Cisco Unified Mobility のスケーラビリティと性能は、モビリティ ユーザ数、ユーザごとのリモート接続先数またはモビリティ ID 数、およびそれらのユーザの Busy Hour Call Attempt（BHCA）レートに依存します。ユーザあたりの複数のリモート接続先またはユーザあたりの高い BHCA によって、Cisco Unified Mobility の容量が減少します。

Cisco Unified Communications Manager Business Edition（Unified CMBE）システムでの Unified Mobility ユーザの容量は、ユーザあたりのリモート接続先数、およびサーバのハードウェアではなく Unified Mobility で有効にされているユーザの BHCA だけに依存します。したがって、Unified CMBE でサポートされるリモート接続先数は、これらのユーザの BHCA に直接依存します。Unified CMBE の Unified Mobility のサイジングのガイドラインは次のとおりです。

- ユーザあたり 5 台以上のリモート接続先を設定することはできません。Unified CMBE システムあたり最大 500 人のユーザがいる場合、リモート接続先の論理的限界は 2,000 台です。ただし、Unified CMBE あたりの最大 BHCA が 3,600 である場合は、システムで 2,000 台のリモート接続先をサポートできない可能性があります。代わりに BHCA 計算を使用して、システムによって処理可能なリモート接続先数を適切にサイジングする必要があります。
- 設定された各リモート接続先は、BHCA に影響があります。ユーザに設定されているリモート接続先ごとに、1 つずつの追加のコール レッグが使用されます。各コールは 2 つのコール レッグで構成されているため、1 つのリモート接続先の呼び出しが 1 つのコールの半分に相当します。そのため、リモート接続先の合計 BHCA は次の式で計算できます。

  リモート接続先の合計 BHCA =（ユーザ数）*（ユーザごとのリモート接続先数）*（ユーザ BHCA）* 0.5

次の例を参考にしてください。

それぞれが 5 BHCA の 300 人のユーザがいて、それぞれのユーザに 1 つずつのリモート接続先（全部で 300 台のリモート接続先）が割り当てられたシステムがあるとすると、リモート接続先の合計 BHCA の計算は次のようになります。

リモート接続先の合計 BHCA =（300 ユーザ）*（ユーザあたり 1 つのリモート接続先）*（ユーザあたり 5 BHCA）* 0.5 = 750 BHCA

この例でユーザの合計 BHCA は（300 ユーザ）*（ユーザあたり 5 BHCA）、つまり 1500 です。この値にリモート接続先の合計 BHCA である 750 を加算すると、システムの合計 BHCA 2250（ユーザの合計 BHCA 1500 + リモート接続先の合計 BHCA 750）が求まります。

上記の例のシステムで他のアプリケーションや追加の BHCA 変数が使用されている場合は、容量はさらに制限される可能性があります（詳細については、「Unified CMBE のキャパシティ プランニング」（P.8-29）を参照してください）。

（注） モビリティ ID は、システム内でリモート接続先と同様に設定され、リモート接続先と同じ容量になります。ただし、リモート接続先と違って、モビリティ ID は、リモート接続先プロファイルではなく、直接電話機に関連付けられます。モビリティ ID は、デュアルモードの電話機と Cisco Unified Mobile Communicator クライアントにのみ適用されます。

適切な Unified Mobility のサイジングを確実に行うには、Cisco Unified Communications Sizing Tool（Unified CST）を使用して、適切な Unified Mobility の容量とシステム全体の容量を決定します。Unified CST は、次の URL（適切なログイン アカウントが必要）で入手できます。

http://tools.cisco.com/cucst

Cisco Unified Mobility の設計上の考慮事項

Unified Mobility を配置する場合は、次の設計上の推奨事項に従ってください。

- 公衆網ゲートウェイ プロトコルで、アウトオブバンド DTMF リレーが使用できる、または、インバンド DTMF をアウトオブバンド DTMF に変換するための Media Termination Point（MTP; メディア ターミネーション ポイント）が割り当てられていることを確認します。公衆網接続用の Cisco IOS ゲートウェイを使用している場合は、アウトオブバンド DTMF リレーがサポートされます。ただし、サードパーティ製ゲートウェイでは、一般的なアウトオブバンド DTMF 方式がサポートされない可能性があるため、結果として、MTP が必要になる場合があります。エンタープライズ機能アクセス 2 ステージ ダイヤリング機能と通話切替機能を使用するには、Cisco Unified CM で DTMF 番号をアウトオブバンドで受信する必要があります。

  （注）　インバンド DTMF をアウトオブバンド DTMF に変換するために MTP 上でリレーする場合は、十分な MTP 容量が提供されることを確認してください。エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替機能の高い使用頻度が予想される場合は、ハードウェア ベースの MTP または Cisco IOS ソフトウェア ベースの MTP を推奨します。

- Unified Mobility を配置する前に、公衆網プロバイダーと連携して次のことを保証する必要があります。
  - 会社へのすべての着信コールに関する発信者 ID が、サービス プロバイダーから供給される。これは、エンタープライズ機能アクセス 2 ステージ ダイヤリングまたは通話切替転送、会議、およびダイレクト コール パーク機能が必要な場合の要件です。
  - 発信コールの発信者 ID は、サービス プロバイダーに制限されない。これは、モビリティ対応ユーザが、一般的な会社のシステム番号やその他の意味のない発信者 ID ではなく、リモート接続先にいる元の発信者の 発信者 ID を受信することが期待される場合の要件です。

    （注）　プロバイダーによっては、トランク上の発信コールの発信者 ID が、そのトランクで処理される DID に制限される場合があります。そのため、発信者 ID が制限されない別の PRI トランクをプロバイダーから入手する必要があります。無制限の PRI トランクを要求すると、プロバイダーによっては、このトランク経由で緊急電話番号にコールを送信または発信しないことが記された署名付きの同意書を要求される場合があります。

    （注）　プロバイダーによっては、[Redirected Dialed Number Identification Service (RDNIS)] フィールドまたは SIP の Diversion ヘッダーにトランクで処理される DID が含まれている限り、そのトランクには発信コールの発信者 ID を無制限で許可します。ゲートウェイまたはトランクの設定ページで [Redirecting Number IE Delivery] > [Outbound] チェックボックスをオンにすることによって、リモート接続先に分岐されたコールの RDNIS または SIP の Diversion ヘッダーにユーザの企業番号を取り入れることができます。RDNIS または SIP の Diversion ヘッダーに対応し、発信コールの発信者 ID を無制限で許可しているかどうかは、サービス プロバイダーに問い合せてください。

- 一般に、モビリティ コール フローには複数の公衆網コール レッグが含まれるため、Unified Mobility にとって公衆網ゲートウェイ リソースの計画と配置が極めて重要です。モビリティ対応ユーザ数が多い場合は、公衆網ゲートウェイ リソースを増やす必要があります。公衆網利用を制限または削減するために、次の方法が推奨されています。
  - モビリティ対応ユーザあたりのリモート接続先数を 1 つに制限します。これによって、着信コールをユーザのリモート接続先に転送するために必要な DS0 数が削減されます。コールがユーザの会社の電話番号に送られると、そのコールがリモート接続先のいずれかで応答されなくても、設定済みのリモート接続先ごとに 1 つずつの DS0 が消費されます。コールがリモート接続先で応答されなくても、リモート接続先あたり 1 つの DS0 が 10 秒間も使用される可能性があります。
  - アクセス リストを使用して、着信コールの発信者 ID に基づいて、特定のリモート接続先へのコールの拡張を拒否または制限します。時刻に基づいてアクセス リストを呼び出すことができるため、エンド ユーザまたは管理者がアクセス リストを頻繁に更新する必要がありません。
  - 不要になったモバイル コネクトを無効にしたり、会社の番号に電話がかけられた場合の DS0 の使用をさらに制限するようにエンド ユーザを教育します。モバイル コネクトが無効になっている場合は、着信コールでデスクトップフォンの呼出音が鳴りますが、誰も電話に出なければ、そのコールが会社のボイルメールに転送されます。
- ロケーション間の WAN 帯域幅の不足によってコール アドミッション制御が拒否される可能性と、デスクトップフォンのピックアップまたはリモート接続先のピックアップによって WAN 帯域幅のオーバーサブスクリプションが発生する可能性があるため、リモート接続先プロファイル CSS と CSS の再ルーティングを設定して、CSS 内のルート パターンが、着信コール レッグが到達するゲートウェイと同じコール アドミッション制御ロケーション内に配置されたゲートウェイを指すようにすることを推奨します。詳細については、「リモート接続先プロファイルの設定」（P.25-56）を参照してください。
- 公衆網にアクセスするために公衆網振り分け用数字をダイヤルする必要がある配置において Intelligent Session Control 機能を有効にする場合は、Matching Caller ID with Remote Destination サービス パラメータを **Partial Match** に設定し、適切な桁数（Number of Digits for Caller ID Partial Match サービス パラメータ）を設定して、設定されたリモート接続先またはモビリティ ID の部分一致が実行されるようにすることを推奨します。これにより、Intelligent Session Control 機能、およびモビリティの発信者 ID の自動照合機能とアンカリング機能が適切に機能するようになります。

デュアルモードの電話機とクライアント

モバイル ユーザ、携帯電話、携帯通信事業者サービスが普及するにつれて、単一のデバイスを使用して社内および社外の両方で音声サービスとデータ サービスを使用できることがますます魅力的なソリューションとなっています。企業においてデュアルモード電話機、およびそこで実行されるクライアントを使用すると、単一の携帯電話を使用して、社内にいるユーザに対してカスタマイズされた音声サービスとデータ サービスを提供し、さらに一般的な音声サービスとデータ サービス用のバックアップ プロバイダーとして携帯通信事業者ネットワークを利用できます。社内で音声サービスとデータ サービスを利用可能にし、デュアルモード電話機に対してネットワーク接続を提供することによって、企業はこれらのサービスをローカルでより安価な接続コストで提供できます。たとえば、企業ネットワーク上で発信される Voice over IP（VoIP）コールは、通常、モバイル ボイス ネットワーク上で発信される同じコールよりもコストが少なく済みます。

この項では、デュアルモード電話機のアーキテクチャについて説明します。また、企業の WLAN ネットワークとモバイル ボイス ネットワークとの間でアクティブな音声コールを移動する場合のハンドオフに関する考慮事項を含む、デュアルモードの電話機とクライアントによって提供される機能について

説明します。この項では、一般的なデュアルモード ソリューション アーキテクチャおよび機能について説明した後、次の特定のデュアルモード クライアントのさまざまな機能および統合に関する考慮事項について説明します。

- Cisco Mobile：iPhone モバイル デバイス対応のデュアルモード クライアントで、企業の WLAN ネットワーク上で VoIP コールを発信する機能、および社内ディレクトリとボイスメール サービスにアクセスする機能を提供します。
- Cisco Jabber：Android OS 2.2 を実行する Android モバイル デバイス対応のデュアルモード クライアントで、企業の WLAN ネットワーク上で VoIP コールを発信する機能、および社内ディレクトリにアクセスし、企業ボイスメール メッセージ待機インジケータやメッセージ カウントを受信する機能を提供します。
- Nokia Call Connect：Nokia モバイル デバイス対応のデュアルモード クライアントで、企業の WLAN ネットワーク上で VoIP コールを発信する機能、および社内ディレクトリやその他のアプリケーションおよびサービスにアクセスする機能を提供します。

さらに、この項では、デュアルモードの電話機とクライアントのハイ アベイラビリティおよびキャパシティ プランニングの考慮事項についても説明します。

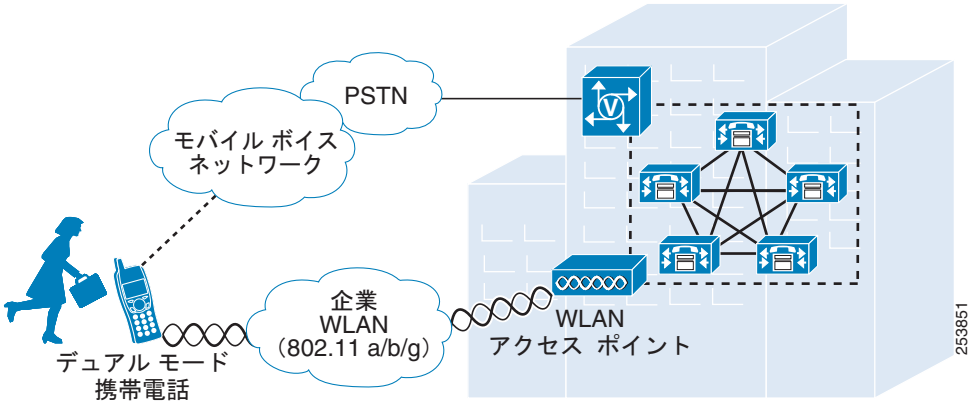
デュアルモード電話機のアーキテクチャ

デュアルモード電話機には、従来の携帯電話ネットワーク テクノロジーまたはモバイル ネットワーク テクノロジーを使用した音声とデータの携帯通信事業者ネットワークへの接続、および IEEE 802.11 標準を使用した Wireless Local Area Network（WLAN; 無線ローカル エリア ネットワーク）への接続の両方を可能にする、2 つの物理インターフェイスまたは無線機が備えられています。

（注）　この項で*デュアルモード電話機*という用語を使用する場合、802.11 に準拠した無線機、および音声とデータの通信事業者ネットワークへの接続用の携帯電話無線機を備えたデバイスを指します。Digital Enhanced Cordless Telecommunications（DECT）やその他の規格に準拠した無線機、または複数の携帯電話無線機を備えたデュアルモード デバイスは、この項のデュアルモード電話機には含まれません。

図 25-25 に、デュアルモード デバイスを Cisco Unified Communications システムに統合するための基本的なデュアルモード ソリューション アーキテクチャを示します。デュアルモード電話機が企業の WLAN に関連付けられて、デュアルモード クライアントが会社の電話機として Cisco Unified CM に登録されます。登録されると、デュアルモード デバイスは、基礎となる企業の Cisco IP テレフォニー ネットワークを利用して、コールを発信および受信します。デュアルモード電話機は、企業の WLAN 接続が利用できない場合にだけ、モバイル ボイス ネットワークを利用してコールを発信および受信します。デュアルモード電話機が企業の WLAN に関連付けられており、クライアントが Unified CM に登録されている場合、その電話機にはユーザの会社の電話番号を使用して到達できます。ユーザの会社の電話番号へのコールが着信すると、デュアルモード電話機の呼出音が鳴ります。ユーザが Cisco デスクトップ IP Phone を持っている場合は、デュアルモード クライアントを登録すると、ユーザの会社の電話番号でシェアド ライン インスタンスが使用可能になり、コールが着信すると、ユーザのデスクトップフォンとデュアルモード電話機の両方の呼出音が鳴ります。登録が解除されると、デュアルモード クライアントは、デュアルモード電話機で会社の電話番号に着信したコールを受信しなくなります。ただし、ユーザに対して Cisco Unified Mobility が有効になっており、ユーザの携帯の番号でモバイル コネクト（またはシングル ナンバー リーチ）がオンになっている場合には、会社の電話番号に着信したコールが受信されます。

図 25-25　デュアルモード電話機のアーキテクチャ



モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード電話機では、Dual Transfer Mode（DTM; デュアル転送モード）がサポートされている必要があります。デバイスで DTM がサポートされていると、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。

Voice over Wireless LAN ネットワークのインフラストラクチャ

さまざまなデュアルモード機能、およびこれらの機能がエンタープライズ テレフォニー インフラストラクチャに与える影響について考慮する前に、適切に調整され、QoS に対応し、ハイ アベイラビリティを備えた WLAN ネットワークを計画して配置することが重要です。デュアルモード電話機は、重要なシグナリング トラフィック、コールのセットアップやさまざまなアプリケーションへのアクセスのためのその他のトラフィック、およびリアルタイムの音声メディア トラフィックにおいて、基礎となる WLAN インフラストラクチャを利用するため、データ トラフィックおよびリアルタイムの音声メディア トラフィックの両方に最適化された WLAN ネットワークの配置が必要になります。WLAN ネットワークの配置が適切でないと、多くの干渉が発生し、容量が低下するため、音声品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように配置された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、デュアルモード電話機を配置する場合は、Voice over WLAN（VoWLAN）の配置が正常に行われるように、配置前、配置中、配置後に WLAN Radio Frequency（RF; 無線周波数）実地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。実稼動環境への配置の前に、WLAN の配置に対してデュアルモード電話機のデバイス タイプまたはクライアントごとにテストを実施して、統合および動作が適切に行われるようにする必要があります。サービス品質を含む最適な VoWLAN サービス（Cisco Unified Wireless Network など）が提供されるように配置および設定された WLAN を使用することによって、デュアルモード電話機を正常に配置できます。

Voice over WLAN 配置およびデバイスのローミングの詳細については、「ワイヤレス デバイスのローミング」（P.25-6）を参照してください。

（注）　ほとんどのデュアルモードの電話機とクライアントは、パブリックおよびプライベートの WLAN アクセス ポイントやホット スポットに接続し、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、このように接続した場合の音声品質は保証されません。デュアルモードの電話機とクライアントを接続する場合は、エンタープライズ クラスの音声に最適化された WLAN ネットワークを推奨します。ほとんどのパブリックまたはプライベートの

WLAN AP およびホット スポットは、データ アプリケーションおよびデバイスに合せて調整されています。ほとんどの場合、クライアントの容量がより大きくなるように、AP 無線機は最大パワーに調整され、動的パワー クライアントはネットワーク接続上の最大パワーに合せて調整されます。このような調整方法は、パケットのドロップや損失時に再送信ができるデータ アプリケーションにとっては理想的ですが、パケットのドロップが大量に発生する可能性があるため、音声アプリケーションでは音声品質が非常に悪くなる可能性があります。

デュアルモードの機能

デュアルモード デバイスには、さまざまな機能が用意されています。機能や動作はデバイスによって異なりますが、この項に説明する共通の動作はすべてのデュアルモード デバイスに当てはまります。

エンタープライズ コール ルーティング

デュアルモード電話機では、エンタープライズ テレフォニー インフラストラクチャおよび（少なくとも一部において）呼制御サービスが利用されるため、デュアルモード デバイスが社内にある場合のコール ルーティングの特性と動作を理解しておくことが重要です。

着信コール ルーティング

デュアルモード デバイスは、ユーザの会社の電話番号および内線番号として Unified CM に登録されるため、システムへの着信コールがそのユーザの会社の電話番号に着信した場合、デュアルモード デバイスの呼出音が鳴ります。これは、公衆網または他の Unified CM クラスタや企業 IP テレフォニー システムから発信された着信コール、および同じ Unified CM 内の他のユーザから発信された着信コールにおける動作です。デュアルモード ユーザは、会社の電話番号に関連付けられている他のデバイスまたはクライアントを持っている場合には、これらのデバイスもシェアド ラインとして呼び出されます。コールがいずれかのデバイスまたはクライアントで応答されると、他のすべてのデバイスおよびクライアントの呼出音は鳴りやみます。

ユーザに対して Cisco Unified Mobility が有効になっており、ユーザのデュアルモード電話機の携帯の番号でシングル ナンバー リーチが有効になっているシナリオにおいては、着信コールはデュアルモード電話機の電話番号に対応するモビリティ ID に転送される場合があります。ただし、この動作が行われるかどうかは、デュアルモード デバイスが社内にあるかどうか、および Unified CM に登録されているかどうかによります。デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、ユーザの会社の電話番号への着信コールは、デュアルモード デバイスのモビリティ ID に対応する内線番号でモバイル コネクトがオンになっている場合でも、モバイル コネクトによってこの ID には転送されません。Unified CM に登録されている場合にデュアルモード デバイスのモビリティ ID に会社の電話番号への着信コールが転送されない理由は、デバイスが社内にあり、WLAN ネットワークを利用できるということがシステムによって認識されるためです。したがって、企業の公衆網リソースの利用を少なくするために、Unified CM では、公衆網を経由してデュアルモード デバイスのモバイル ボイス ネットワーク インターフェイスにコールを転送する処理は行われません。代わりに、会社の電話番号に対応する WLAN インターフェイスだけが呼び出されます。

デュアルモード デバイスが社外にあるか、または Unified CM に登録されていない場合、ユーザに対して Unified Mobility が有効になっており、モビリティ ID でモバイル コネクトがオンになっていると、設定されたモビリティ ID に従って、会社の電話番号への着信コールがデュアルモード デバイスに転送されます。デュアルモードのデバイスおよびクライアントと Unified Mobility との統合の詳細については、「Cisco Mobile または Cisco Jabber と Cisco Unified Mobility との間の相互作用」（P.25-76）および「Nokia Call Connect と Cisco Unified Mobility との間の相互作用」（P.25-81）を参照してください。

いずれの場合も、デュアルモード デバイスの携帯電話番号に対して直接発信された着信コールは、プロバイダー ネットワークやデバイスの設定でモバイル ネットワーク経由でデバイスにコールを転送しないように設定されている場合を除き、モバイル ネットワーク経由でデュアルモード デバイスの携帯電話無線機に直接ルーティングされます。このようなコールは、ユーザの会社の電話番号に対して発信されたコールではないため、適切な動作です。これらのコールは個人的なコールであると見なされるため、会社経由でルーティングされません。

発信コール ルーティング

デュアルモード デバイスからの発信コールで使用されるインターフェイスは、ロケーション、およびその特定の時刻におけるデバイスの接続状況に応じて異なります。デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合、コールは、通常どおり携帯電話無線機インターフェイスからモバイル ボイス ネットワークにルーティングされます。ただし、社内にあり Unified CM に登録されている場合、デュアルモード デバイスからのすべてのコールは、エンタープライズ テレフォニー インフラストラクチャを利用して WLAN 無線インターフェイスから企業の WLAN ネットワークに発信される必要があります。一部のデュアルモード クライアントでは、企業ネットワーク接続が利用可能になったときにクライアントを自動的に Unified CM に登録するように、1 つ以上の設定を行う必要がある場合があります。デュアルモード クライアントが Unified CM に登録されていない場合、発信コールは常に企業ネットワークではなくモバイル ボイス ネットワークを使用して発信されます。

ダイヤル プラン

企業のダイヤル プランによって、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合のダイヤリング動作が決定されます。たとえば、企業のダイヤル プランの設定で、内部の内線番号に到達するために短縮ダイヤルの使用が許可されている場合、Unified CM に登録されているデュアルモード デバイスではこの短縮ダイヤルを利用できます。デュアルモード ユーザが発信コールにおいて社内で企業のダイヤリング手順を使用し、短縮ダイヤルおよびサイトベースの番号または公衆網振り分け用数字を利用してダイヤルできることは確かに便利ですが、携帯電話ユーザは、携帯電話において、モバイル ボイス ネットワークで発信コールに対して要求される完全な E.164 ダイヤル ストリングを使用して発信コールの番号をダイヤルするため、これは若干不自然なダイヤリング方式となります。

企業におけるエンド ユーザ ダイヤリング エクスペリエンスは、最終的には企業のポリシーおよび企業のテレフォニー配置の管理者によって決定されます。ただし、デュアルモード電話機では、必要なダイヤリング ストリングを正規化して、ユーザが社内または社外のいずれからでも同じ番号をダイヤルして特定の着信側接続先に到達できるようにすることを推奨します。モバイル ネットワークにおけるダイヤリングは、通常完全な E.164（先頭に「+」が付く場合と付かない場合があります）を使用して行われ、携帯電話の連絡先は通常完全な E.164 番号で保存されるため、デュアルモード電話機においては、企業のダイヤル プランは完全な E.164 番号または先頭に「+」を付けた完全な E.164 番号を使用できるように設定することを推奨します。Unified CM 内で、デュアルモード電話機のこのような発信ダイヤリングを処理するようにダイヤル プランが設定されている場合、ユーザは連絡先を E.164 形式で 1 セットだけ電話機に保存するだけで済みます。これらの連絡先からダイヤルする場合や、完全な E.164 番号を使用して手動でダイヤルする場合、デバイスが社内にあり Unified CM に登録されているか、またはデバイスが社外にありモバイル ボイス ネットワークにだけ接続されているかにかかわらず、コールは常に適切な接続先にルーティングされます。このように企業のダイヤル プランを設定することによって、ユーザはデバイスが社内の Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスを提供できます。

社内か社外かにかかわらずデュアルモード電話機からの正規化されたダイヤリングを可能にするには、次の考慮事項に注意して Unified CM でダイヤル プランを設定します。

- 企業のダイヤル プランで、デュアルモード電話機からの、通常モバイル ボイス ネットワークで使用されるダイヤル ストリングを処理できるようにします。たとえば、ダイヤル プランでは、携帯電話からモバイル ボイス ネットワークを経由して特定の電話機に到達するためにダイヤルされる +1 408 555 1234 や 408 555 1234 などのストリングを処理できるように設定する必要があります。
- 会社の他の電話番号へのコールにおいては、短縮ダイヤルが設定されているシステムでは、ダイヤル ストリングを変更して、必要に応じて会社の内線番号に再ルーティングできる必要があります。たとえば、企業のダイヤル プランが 5 桁の内部ダイヤルに基づいているとすると、会社の内線番号へのコール ルーティングが処理されるようにシステムを設定して、デュアルモード デバイスが社内にあり Unified CM に登録されているときにコールが発信された場合、+1 408 555 1234 や 408 555 1234 に発信されたコールが変更されて、51234 に再ルーティングされるようにする必要があります。

- 会社のデュアルモード デバイスへのすべての着信コールの発信番号または発信者 ID の先頭に適切な数字を付加して、不在コール、発信コール、および着信コールのコール履歴リストが完全な E.164 形式となるようにします。これにより、デュアルモード デバイスのユーザは、ダイヤル ストリングを編集することなくコール履歴リストからダイヤルできます。ユーザは、社内にいるかまたは社外にいるかにかかわらず、コール履歴リストから番号を選択してリダイヤルできます。たとえば、社内の 51234 からデュアルモード ユーザの会社の電話番号にコールが発信され、そのコールに応答がない場合、発信番号を操作して、デュアルモード デバイスの履歴リストに 408 555 1234 または + 1 408 555 1234 という形式のエントリが残るように Unified CM を設定する必要があります。この番号は、操作しなくても、デュアルモード デバイスが Unified CM に登録されている場合に社内でダイヤルすることも、社外でダイヤルすることもできます。

デュアルモード デバイスの正規化されたダイヤリングの例外の 1 つに、会社の内線番号または電話に内部からだけ到達可能なシナリオがあります（つまり、対応する外部から到達可能な DID 番号がない場合）。このような場合は、短縮形式を使用して、外部から到達できない番号をダイヤルできます（手動でダイヤルするか、または連絡先からダイヤルします）。これらの番号は外部では利用できず、社内からだけダイヤルできるため、連絡先リストにこれらの番号を保存する場合には、社内だけで使用できるという何らかのマークが必要となります。さらに、これらの内部専用番号からの着信コールの発信番号をコール履歴リストに保存する場合は、番号が変更されないようにする必要があります。これらの番号には、社内からだけ発信できるためです。すべてのコール履歴リストにおいて、これらの内線番号からのコールは番号を変更しないで保存する必要があります。このように変更しないで保存された番号、つまり短縮ダイヤル ストリングは、デバイスが社内にあり Unified CM に登録されているときにだけ正常にダイヤルできます。

緊急サービスおよびダイヤリングの考慮事項

デュアルモード電話機から 911、999、112 などの緊急サービス番号に対してコールを発信する場合、事態は少々複雑になります。デュアルモード デバイスは社内または社外に位置する可能性があるため、緊急時におけるデュアルモード電話機およびそのユーザの位置の通知について考慮する必要があります。携帯電話はすでにプロバイダー ネットワークの位置サービスを利用しています。これらの位置サービスは常に利用可能であり、通常は企業ワイヤレス ネットワークよりもはるかに正確に位置を特定できるため、緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。デュアルモード電話機から緊急コールを発信したり位置サービスを利用したりする場合にモバイル ボイス ネットワークだけが利用されるように、Unified CM 内でデュアルモード デバイスを設定して、911、999、112 などの緊急番号へのコールを許可するルート パターンにこれらのデバイスからアクセスできないようにします。さらに、デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。

会社の発信者 ID

デュアルモード デバイスが社内にあり、Unified CM に登録されている場合、デュアルモード電話機の WLAN インターフェイス経由で発信されるすべてのコールは、ユーザの会社の電話番号が発信者 ID として設定されてルーティングされます。これにより、遠端でコール履歴リストから発信される返信コールはユーザの会社の電話番号に対して発信されることになり、常に会社経由でルーティングされます。デュアルモード ユーザに対して Cisco Unified Mobility が有効になっており、デュアルモードの携帯の番号でモバイル コネクトがオンになっている場合、デュアルモード デバイスが社外にあるときには、会社の電話番号への返信コールも公衆網経由でデュアルモード デバイスに転送されます。

通話切替機能

デュアルモード電話機クライアントが社内にあり、テレフォニー エンドポイントとして Unified CM に登録されている場合、Unified CM でサポートされているコール シグナリング方式を使用して、保留、保留解除、転送、会議などのコール処理付加サービスを呼び出すことができます。Unified CM に登録された IP Phone やクライアントと同様に、これらのデバイスでは、Music On Hold（MoH; 保留音）、カンファレンス ブリッジ、メディア ターミネーション ポイント、トランスコーダなどの企業のメディア リソースを利用できます。

外部コール ルーティング

デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合、このデバイスでは、モバイル ボイス ネットワーク経由でだけコールを発信および受信できます。このため、デュアルモード電話機デバイスが登録されていない場合に発信または受信されるすべてのコールにおいて、Unified CM は関与しません。デュアルモード電話機で社外からコールが発信された場合、ネットワークに送信される発信者 ID は携帯の番号です。このため、応答されなかったコールへの返信コールは、会社経由でルーティングされるのではなく、デュアルモード デバイスの携帯の番号に直接発信されることになります。

デュアルモード電話機が Cisco Unified Mobility と統合されている場合は、デュアルモード デバイスが社外にあり Unified CM に登録されていない場合でも、エンタープライズ 2 ステージ ダイヤリング サービスを利用して会社経由でコールを発信できます。Unified Mobility の 2 ステージ ダイヤリングは、モバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用して実行され、ユーザは会社の DID 番号をダイヤルし、クレデンシャルを入力してから発信番号をダイヤルする必要があります。Unified Mobility の 2 ステージ ダイヤリング機能の詳細については、「モバイル ボイス アクセスとエンタープライズ機能アクセス」（P.25-48）を参照してください。

同様に、デュアルモード電話機が Unified Mobility と統合されている場合、ユーザは、会社の電話番号への着信コールをモバイル コネクト経由で携帯の番号で受信したり、DTMF キー シーケンスを使用して保留、保留解除、転送、会議などの通話切替機能を呼び出したり、デスクトップフォンのピックアップを実行してアクティブなコールを携帯電話から会社のデスクトップフォンに移動したりできます。

追加のサービスおよび機能

コール処理サービスや呼制御サービスに加えて、デュアルモードの電話機とクライアントでは、この項に説明する追加の機能およびサービスを提供できます。

コール ハンドオフ

デュアルモード電話機の配置における非常に重要な側面の 1 つに、ユーザが社内と社外の間を移動したり、ネットワーク接続が携帯電話無線機と WLAN 無線機との間で切り替わったりしたときのコール プリザベーションがあります。デュアルモード電話機のユーザは多くの場合移動するため、デュアルモード ユーザが社内と社外の間を移動するときにアクティブなコールが維持されることが重要です。このため、デュアルモード クライアントおよび基礎となる企業のテレフォニー ネットワークでは、何らかの形式のコール ハンドオフが可能である必要があります。

デュアルモード クライアント、および基礎となる IP テレフォニー インフラストラクチャの両方でサポートされる必要がある 2 種類のコール ハンドオフがあります。

- ハンドアウト

  コール ハンドアウトとは、アクティブなコールをデュアルモード電話機の WLAN インターフェイスからデュアルモード電話機の携帯電話インターフェイスに移動することを指します。このためには、コールが、会社の公衆網ゲートウェイ経由で、企業の WLAN ネットワークからモバイル ボイス ネットワークにハンドアウトされることが必要です。

- ハンドイン

  コール ハンドインとは、アクティブなコールをデュアルモード電話機の携帯電話インターフェイスからデュアルモード電話機の WLAN インターフェイスに移動することを指します。このためには、コールが、会社の公衆網ゲートウェイ経由で、モバイル ボイス ネットワークから企業の WLAN ネットワークにハンドインされることが必要です。

デュアルモード電話機のハンドオフ動作は、デュアルモード クライアントの特性およびその特定の機能に依存しています。手動ハンドオフ機能だけを提供するデュアルモード クライアントもあれば、ネットワークの状態に基づいて自動的にハンドオフを呼び出すことができるデュアルモード クライアントもあります。手動ハンドオフのシナリオにおいては、デュアルモード ユーザは、各自のロケーションおよび必要性に基づいてハンドオフ動作を行い、完了する必要があります。自動ハンドオフで

は、デュアルモード クライアントは企業の WLAN AP 信号の増幅または減衰を検知して、WLAN 信号の強度が減衰した場合にはハンドアウトを行う決定をしてハンドアウト動作を実行し、WLAN 信号が増幅した場合にはハンドインを行う決定をしてハンドイン動作を実行できます。

ハンドオフ動作は、電話のコールにおいてエンタープライズ IP テレフォニー インフラストラクチャを最大限に活用するために重要となります。また、これらの動作は、音声の継続性と良好なユーザ エクスペリエンスを提供し、ユーザが元のコールをいったん切ってから再度コールを発信し直す必要がないようにするためにも必要です。

社内ディレクトリ アクセス

一部のデュアルモード クライアントは、ディレクトリ ルックアップ検索や個人的なコンタクト リストを含む社内ディレクトリ サービスにアクセスできます。この機能はデュアルモードのデバイスおよびクライアントに必須の機能ではありませんが、デュアルモード電話機のユーザが携帯電話から社内ディレクトリ情報にアクセスできると、これらのユーザの生産性が向上します。

企業ボイスメール サービス

多くのデュアルモード クライアントでは、企業ボイスメール サービスにアクセスすることもできます。ほとんどのデュアルモード クライアントでは、ユーザの企業ボイスメール ボックスに未読のボイスメールが存在し、デュアルモード電話機が企業の WLAN ネットワークに接続されている場合に、企業のメッセージ待機インジケータを受信できます。さらに、デュアルモード クライアントを使用して、企業ボイスメール メッセージを取得することもできます。通常、企業ボイスメール メッセージは、ユーザがボイスメール システム番号にダイヤルし、必要なクレデンシャルを入力してから各自のボイスメール ボックスに移動して取得します。ただし、一部のデュアルモード クライアントは、ボイスメール ボックス内のすべてのメッセージのリストをダウンロードおよび表示し、デュアルモード電話機にダウンロードして再生する個別のメッセージを選択することによって、ボイスメール ボックスからボイスメール メッセージを取得する機能を備えています。この機能は、ビジュアル ボイスメールと呼ばれることもあります。デュアルモード電話クライアントおよび企業ボイスメール システムの両方において、ネットワーク経由でのボイスメール リストの提供およびメッセージのダウンロードが可能である必要があります。Cisco Unity および Cisco Unity Connection は両方ともビジュアル ボイスメールをサポートしており、デュアルモード クライアントでもこの機能がサポートされている場合にはボイスメール リストの提供およびボイスメールのダウンロードが可能です。

デュアルモード クライアント：Cisco Mobile および Cisco Jabber

この項では、Cisco Mobile および Cisco Jabber の特性と展開に関する考慮事項について説明します。

Cisco Mobile

Cisco Mobile は、Apple iPhone 対応のデュアルモード クライアントです。Apple の App Store からクライアント アプリケーションをダウンロードし、iTunes を使用して iPhone にインストールすると、iPhone を企業の WLAN ネットワークに関連付けて、SIP 対応の会社の電話機として Unified CM に登録できます。

Cisco Mobile デュアルモード iPhone クライアントに登録および呼制御サービスを提供するには、Unified CM 内でデバイスが **Cisco Dual-Mode for iPhone** デバイス タイプとして設定される必要があります。次に、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するように iPhone を設定する必要があります。WLAN にアクセスするように iPhone を設定すると、Cisco Mobile クライアントが起動されたときに、デバイスが Unified CM に登録されます。

Unified Mobility と統合し、ハンドオフ機能を利用するには、iPhone の携帯の番号を、Unified CM 内の Cisco Dual-Mode for iPhone デバイスに関連付けられたモビリティ ID として設定する必要があります。

Cisco Mobile 8.0 クライアントは、ファームウェア バージョン 3.0.1 以降が実行されている iPhone の 3G、3GS、または 4 モデルでサポートされています。アプリケーションのマルチタスキングやバックグラウンド処理をサポートする Cisco Mobile 8.1 クライアントは、ファームウェア バージョン 4 を実行している iPhone の 3GS と 4（および iPad と第 3 および第 4 世代の iPod Touch）でサポートされます。iPhone、iPad、および iPod Touch WLAN インターフェイスは、802.11b および 802.11g ネットワーク接続をサポートします。

Cisco Mobile クライアントでは、デュアルモード電話サービスだけではなく、企業の Microsoft Active Directory へのアクセスが設定されている場合にはディレクトリ検索サービスが、Cisco Unity Connection 上のユーザのボイスメール ボックスへのアクセスが設定されている場合にはビジュアル ボイスメール サービスが提供されます。

（注）　Cisco Mobile と iPhone 対応の Cisco Unified Mobile Communicator クライアントの両方を同時に配置する場合は、ユーザの企業ボイスメール ボックスにアクセスするように Cisco Mobile を設定しないでください。代わりに、Cisco Mobile クライアントを使用してビジュアル ボイスメール アクセスを行います。これは、Cisco Mobile クライアントの方が機能が豊富で、よりよいユーザ エクスペリエンスを提供できるためです。

Cisco Mobile クライアントは、「Cisco Mobile および Cisco Jabber のハンドオフ」（P.25-73）の項に説明されているように、手動でのハンドアウトだけを実行できます。

Cisco Mobile デュアルモード iPhone クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Web サイトで入手可能な Cisco Unified Mobile Communicator のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7271/tsd_products_support_series_home.html

Cisco Jabber 8.6

Cisco Jabber 8.6 は、Android モバイル デバイス対応のデュアルモード クライアントです。Android Market からクライアント アプリケーションをダウンロードし、Android デバイスにインストールすると、Android デバイスを企業の WLAN ネットワークに関連付けて、SIP 対応の会社の電話機として Unified CM に登録できます。

Cisco Jabber デュアルモード Android クライアントに登録および呼制御サービスを提供するには、Unified CM 内でデバイスが [Cisco Dual-Mode for Android] デバイス タイプとして設定される必要があります。次に、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するように Android デバイスを設定する必要があります。WLAN にアクセスするように Android デバイスを設定すると、Cisco Jabber クライアントが起動したときに、デバイスが Unified CM に登録されます。Unified Mobility と統合し、ハンドオフ機能を利用するには、Android の携帯の番号を、Unified CM 内で Cisco Dual-Mode for Android デバイスに関連付けられたモビリティ ID として設定する必要があります。

Cisco Jabber クライアントは、Samsung Galaxy S International（GT-I9000）スマートフォンおよび Samsung Galaxy Tab International（GT-P1000）でサポートされます。これらのデバイスでは、ファームウェア バージョン 2.2.1 以上が実行されている必要があります。公式にサポートされていませんが、Cisco Jabber for Android はバージョン 2.2 以上が実行している多くの Android デバイスで動作します。制限の度合いはデバイスによって異なります。ほとんどの Android デバイスの WLAN インターフェイスで、802.11b、802.11g、および 802.11n ネットワーク接続がサポートされています。

Cisco Jabber 8.6 クライアントでは、デュアルモード電話サービスだけでなく、企業の Microsoft Active Directory へのアクセスが設定されている場合にはディレクトリ検索サービスが、また、Cisco Unity Connection に統合されている場合には企業ボイスメール Message Waiting Indication（MWI; メッセージ待機インジケータ）とメッセージ数が提供されます。

「Cisco Mobile および Cisco Jabber のハンドオフ」（P.25-73）の項で説明しているように、Cisco Jabber 8.6 クライアントでは手動のハンドアウトだけを実行できます。

Cisco Jabber デュアルモード Android クライアント、追加の機能、およびサポートされているハードウェアとソフトウェアのバージョンの詳細については、次の Web サイトで入手可能な Cisco Jabber のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps11678/tsd_products_support_series_home.html

Cisco Mobile および Cisco Jabber のハンドオフ

Mobile 8.*x* および Cisco Jabber 8.6 などの Cisco デュアルモード クライアントを適切に展開するには、クライアント内部のハンドオフ動作の特性について理解することが重要です。Cisco Mobile 8.*x* iPhone および Cisco Jabber 8.6 デュアルモード クライアントによって使用されるハンドオフ方式は、Cisco Dual-Mode for iPhone または Cisco Dual-Mode for Android デバイスの設定ページの [Transfer to Mobile Network] 設定に基づきます。

[Transfer to Mobile Network] の設定に応じて、ハンドオフには次の 2 つの方式があります。

- 「モバイル ソフトキー方式のハンドオフ」（P.25-73）

  この方式では、[Transfer to Mobile Network] の設定を [Use Mobility Softkey (user receives call)] に設定する必要があります。このタイプのハンドオフでは、Unified CM システムは、公衆網を介してユーザのモバイル番号へのコールを発信します。このハンドオフ方式は、Cisco Mobile 8.*x* および Cisco Jabber 8.6 デュアルモード クライアントの両方でサポートされています。

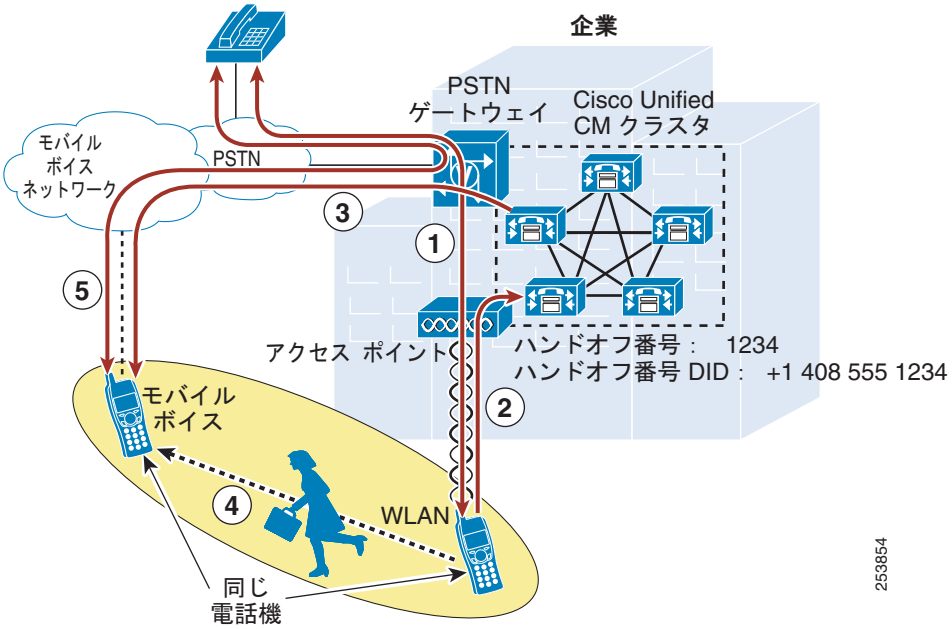
- 「ハンドオフ番号方式のハンドオフ」（P.25-74）

  この方式では、[Transfer to Mobile Network] の設定を [Use HandoffDN　Feature (user places call)] に設定する必要があります。このタイプのハンドオフでは、デュアルモード クライアントが、Unified CM システム内に設定されているハンドオフ番号にモバイル ボイス ネットワーク経由でコールを発信します。このハンドオフ方式は、Cisco Mobile 8.*x* デュアルモード クライアントのみでサポートされています。

モバイル ソフトキー方式のハンドオフ

図 25-26 に示す動作は、社内の iPhone または Android デュアルモード デバイスにおけるアクティブなコールが、手動で WLAN インターフェイスから会社の公衆網ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動される様子を示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録されたデュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Mobile または Cisco Jabber デュアルモード クライアント内のコール中メニューから [Use Mobile Network] ボタンを選択して、コールをハンドアウトする必要があることを Unified CM に通知する必要があります（ステップ 2）。次に、Unified CM から、このデュアルモード デバイスに対応する設定済みのモビリティ ID 番号に対して、会社の公衆網ゲートウェイを経由してコールが発信されます（ステップ 3）。このモビリティ ID へのコールは、モバイル ボイス ネットワーク（iPhone または Android デバイスの携帯電話インターフェイス）に対して発信されます。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。一方、Unified CM からの着信コールがモバイル ボイス ネットワーク インターフェイスで受信され、ユーザは手動でこのコールに応答し、ハンドアウトを完了する必要があります。携帯電話インターフェイスで着信コールが応答されると、WLAN を通過していた RTP ストリームが公衆網ゲートウェイにリダイレクトされ、デュアルモード クライアントと元の公衆網電話機との間のコールは会社のゲートウェイで固定されて、中断されずに継続します（ステップ 5）。

図 25-26　Cisco Mobile または Cisco Jabber デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）：モバイル ソフトキー方式



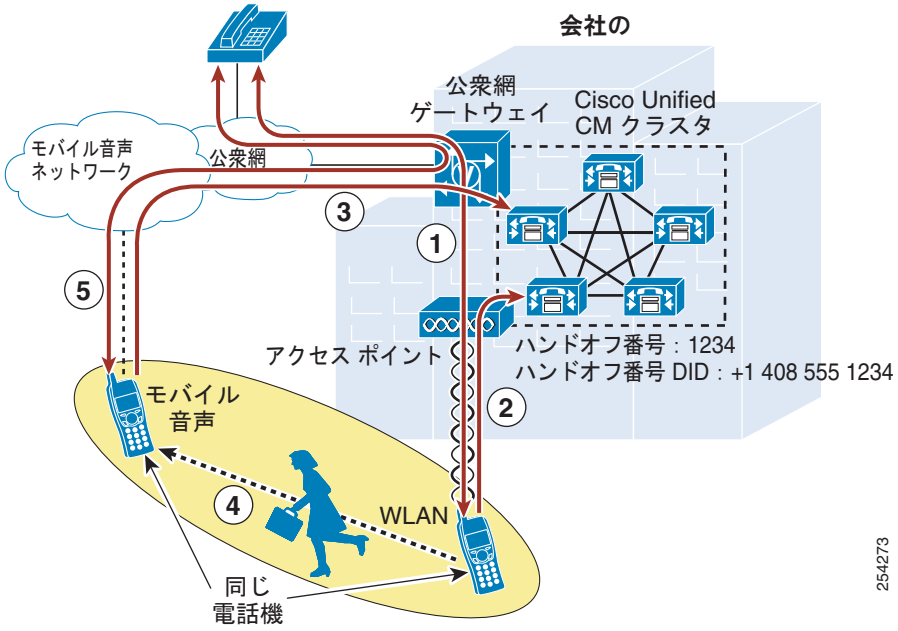
ハンドオフ番号方式のハンドオフ

図 25-27 に、社内の iPhone デュアルモード電話機におけるアクティブなコールが、手動で WLAN インターフェイスから会社の公衆網ゲートウェイ経由でモバイル ボイス ネットワークまたは携帯電話インターフェイスに移動される図 25-26 と同じハンドオフ動作を示します。ただし、このケースでは、ハンドオフ番号方式のハンドアウトが使用されます。

（注）　ハンドオフ番号方式のハンドアウトは、Cisco Jabber 8.6 ではサポートされていません。

図 25-27 に示すように、企業の WLAN に関連付けられ、Unified CM に登録された iPhone デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。これは手動のプロセスであるため、ユーザが Cisco Mobile デュアルモード クライアント内のコール中メニューから [Use Mobile Network] ボタンを選択して、コールをハンドアウトする必要があることを Unified CM に通知する必要があります（ステップ 2）。次に、Cisco Mobile クライアントが、Unified CM システム内で設定されているハンドオフ番号に向けて、モバイル ボイス ネットワークを介して携帯電話インターフェイスからコールを自動発信します（ステップ 3）。これで、ユーザは、社外に移動して、WLAN ネットワークのカバー領域から離れることができます（ステップ 4）。その間に、Cisco Mobile クライアントからの着信コールが Unified CM によって受信されます。着信したコールの発信番号がユーザに設定されているモビリティ ID と一致したと仮定すると、WLAN を通過した RTP ストリームが公衆網ゲートウェイにリダイレクトされ、Cisco Mobile デュアルモード クライアントと元の公衆網電話との間のコールは、会社のゲートウェイで固定されて、中断されることなく継続します（ステップ 5）。

図 25-27　Cisco Mobile デュアルモード ハンドアウト：ハンドオフ番号方式



（注）　ハンドアウトのハンドオフ番号方式では、Unified CM が、着信したコールの発信番号として、ハンドオフを試みている Cisco Dual Mode for iPhone デバイスの下で設定されているモビリティ ID 番号と一致する番号を公衆網ネットワークから受け取る必要があります。発信者 ID が iPhone から送信されない場合、公衆網プロバイダーが着信したコールの発信者 ID を会社に送信しなかったり、着信したコールの発信者 ID が設定されているモビリティ ID と一致しなかった場合は、ハンドアウト動作は失敗します。

（注）　Cisco Mobile および Cisco Jabber デュアルモード クライアントでは、ハンドインをサポートしていません。デュアルモード モバイル ボイス ネットワーク（携帯電話インターフェイス）と会社の電話（または会社のゲートウェイでコールが固定された公衆網電話機）との間で通話中のコールがアクティブである場合、コールをデュアルモード デバイスの WLAN インターフェイスに移動するには、コールをいったん切断し、デュアルモード クライアントが企業の WLAN に関連付けられて Unified CM に登録されてからリダイヤルするのが唯一の方法です。

Cisco Mobile デスクトップフォンの統合

Cisco Mobile iPhone デュアルモード クライアントを使用すると、アクティブまたは保留中の通話をデスクトップフォンからデュアルモード デバイスに転送できます。この機能を使用するには、デスクフォンのプライマリ回線の CTI モニタリングおよびコール パーク機能が必要です。

デスクトップフォンで提供される機能を使用するには、デスクトップフォンのプライマリ回線の CTI モニタリングがアクティブである必要があります。アクティブまたは保留中の通話が Cisco Mobile クライアントに検知されると、デュアルモード デバイスに通話を転送するかどうかをたずねられます。通話を転送する場合は、デスクトップフォンが自動的にコールをパークし、デュアルモード クライアントがパーク番号から自動的に通話を取得します。

デスクトップフォンの統合を有効にするには、ユーザのエンド ユーザ アカウントが CRI が有効なユーザ グループに割り当てられており、ユーザのデスクトップフォンで CTI 制御が可能になっていることを確認してください。また、Cisco デュアルモード iPhone デバイスの [CTI Control Username] フィールドを、ユーザのエンド ユーザ アカウント userID を使用して設定する必要があります。

Cisco Jabber デスクトップフォンの統合

Cisco Jabber Android デュアルモード クライアントを使用すると、Android デバイスから、デュアルモード デバイスと回線を共有する IP デスクトップフォンにアクティブ コールを移動できます。この機能を呼び出すには、Cisco Jabber クライアントを介してアクティブ コールを保留にします。保留にしたコールは、シェアド ラインの IP デスクトップフォンまたは Cisco Jabber クライアントで保留解除できます。

Cisco Mobile iPhone および Cisco Jabber Android デュアルモード クライアントの WLAN 設計上の考慮事項

Cisco Mobile および Cisco Jabber デュアルモード クライアントを展開する際には、次の WLAN ガイドラインを考慮してください。

- 可能な場合は、Cisco Mobile iPhone および Cisco Jabber Android デュアルモード クライアントが、デュアルモード デバイスの WLAN インターフェイス上で同じ IP アドレスを使用できるように、必ず社内のレイヤ 2 でだけローミングするようにしてください。デバイスの IP アドレスの変わり、サブネットの境界を越えるレイヤ 3 のローミングでは、コールがドロップされます。
- Cisco Mobile および Cisco Jabber デュアルモード クライアントは、どの AP でも同じ SSID が使用されている企業の WLAN ネットワーク上に展開してください。SSID が異なると、AP 間のローミングがはるかに低速になります。
- 企業内 WLAN 上のすべての AP が、その SSID をブロードキャストするようにしてください。SSID が AP によってブロードキャストされないと、他の WiFi ネットワークに参加するようにデバイスから要求される場合や、デバイスが自動的に他の WiFi ネットワークに参加する場合があります。この場合、コールは中断されます。

Cisco Mobile または Cisco Jabber と Cisco Unified Mobility との間の相互作用

iPhone 対応の Cisco Mobile および Android 対応の Cisco Jabber デュアルモード クライアントを Cisco Unified Mobility に統合することで、Cisco モバイル コネクト、通話切替 DTMF 機能、2 ステージ ダイヤリング、シングル企業ボイスメール ボックス、およびデスクトップフォンのピックアップを利用できます。

Unified Mobility と統合するには、Unified CM 内で、iPhone または Android デュアルモード携帯電話番号を Cisco Dual-Mode for iPhone または Cisco Dual-Mode for Android デバイスに関連付けられたモビリティ ID として設定する必要があります。システム内で携帯の番号をモビリティ ID として設定した後は、iPhone または Android デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合に、モバイル コネクトを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワーク経由で iPhone または Android デュアルモード デバイスに転送できます。デュアルモード デバイスが社内にあり、Unified CM に登録されている場合には、会社の電話番号への着信コールはデバイスのモバイル ボイス ネットワーク インターフェイスには転送されません。iPhone または Android デュアルモード デバイスが社内にある場合は、デバイスの WLAN インターフェイスだけが着信コールを受信します。これにより、会社の公衆網ゲートウェイ リソースの必要以上の消費を回避できます。

社外にあり、Unified CM に登録されていない場合、iPhone または Android デュアルモード デバイスでは、DTMF を使用して通話切替機能を呼び出したり、会社の任意の固定コールに対するデスクトップフォンのピックアップを実行したりできます。また、デュアルモード デバイスでは、コールを発信する場合にモバイル ボイス アクセスとエンタープライズ機能アクセスの 2 ステージ ダイヤリング機能を利用して、これらのコールを会社経由でルーティングし、会社の公衆網ゲートウェイに固定できます。

iPhone または Android デュアルモード デバイスにモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、それらの番号を Unified CM 内で Cisco Dual Mode for iPhone または Cisco Dual-Mode for Android デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先をデュアルモード デバイスに関連付ける場合に、リモート接続先プロファイルを設定する必要はありません。

Cisco Unified Mobility の機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobility」（P.25-37）を参照してください。

デュアルモード クライアント：Nokia Call Connect

Nokia Call Connect は、Nokia モバイル スマート フォン対応のデュアルモード クライアントです。クライアントを Nokia デバイスにインストールすると、企業の WLAN ネットワークに関連付けて、Skinny Client Control Protocol（SCCP）対応の会社の電話機として Unified CM に登録できます。

Nokia デュアルモード デバイスに登録および呼制御サービスを提供するには、Unified CM で Nokia S60 デバイス タイプがサポートされている必要があります。このデバイス タイプは、Nokia が提供する Cisco Option Package（COP）ファイルを Unified CM にロードすると使用可能になります。

Unified CM 内でデュアルモード デバイスを設定した後、Nokia Call Connect クライアントを Nokia デバイスにロードする必要があります。この作業は、USB、Bluetooth、または赤外線ポートを備えた、Nokia PC Suite を実行するコンピュータを使用して行うことができます。Nokia Call Connect Symbian Installation System（SIS）ファイルを Nokia デバイスにロードした後、企業の WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するようにデバイスを設定する必要があります。WLAN にアクセスするようにハンドセットを設定すると、Nokia Call Connect クライアントが起動されたときに、デバイスが Unified CM に登録されます。Nokia デュアルモード デバイスを Unified Mobility と統合して、ユーザがモバイル コネクトなどの機能を利用できるようにするには、Nokia の携帯電話番号をモビリティ ID として設定し、それを Unified CM 内の Nokia S60 デバイスに関連付けます。

（注）　Nokia Call Connect クライアントの SCCP 登録設定を [Always On] に設定して、Nokia デバイスが企業の WLAN ネットワークに関連付けられた場合に Unified CM への登録が試みられるようにすることを推奨します。また、Nokia デュアルモード電話機の優先コール タイプまたはデフォルト コール タイプの設定を [Internet Call] に設定して、Nokia Call Connect クライアントが Unified CM に登録された場合に、デバイスからの発信コールにおいて常にデュアルモード電話機の WLAN インターフェイス経由でルーティングが試みられるようにすることを推奨します。これらの推奨設定を行うことにより、Nokia デュアルモード電話機において、ビジネス コールの発信および受信時に可能な限りエンタープライズ IP テレフォニー インフラストラクチャを使用できます。

Nokia Call Connect 2.2 クライアントは、Nokia Symbian 3 ハンドセット（Nokia C7、E6、N8 を含む）および Nokia S60 3.2 ハンドセット（Nokia E52、E55、E72、E75 を含む）でサポートされています。E51、E61i、E63、E66、E71、および E90 を含む Nokia S60 3.1 ハンドセットもサポートされていますが、自動ハンドオフなどの高度な機能はサポートされない可能性があります。Nokia 携帯電話の WLAN インターフェイスでは、802.11b、802.11g、および一部の場合では 802.11n ネットワーク接続がサポートされています。

Nokia Call Connect クライアントでは、デュアルモード電話サービスだけでなく、Unified CM ディレクトリへのアクセスが設定された場合には、ディレクトリ検索サービスも提供されます。また、Cisco デスクトップ IP Phone でサポートされているような企業ベースの XML 電話サービスもサポートされます。

Nokia Call Connect 2.0 以降のクライアントでは、以降の項で説明する自動ハンドアウトおよびハンドインを実行できます。

Nokia Call Connect デュアルモード クライアント、サポートされているハンドセット、ソフトウェア バージョンの詳細、および最新のクライアントと COP ファイルについては、次の Web サイトを参照してください。

http://www.cisco.com/en/US/products/ps10589/tsd_products_support_series_home.html

Nokia Call Connect デュアルモード ハンドオフ

Nokia Call Connect デュアルモード クライアントを適切に配置するには、Nokia デュアルモード クライアント内でのハンドオフ動作の特性を理解することが必要です。

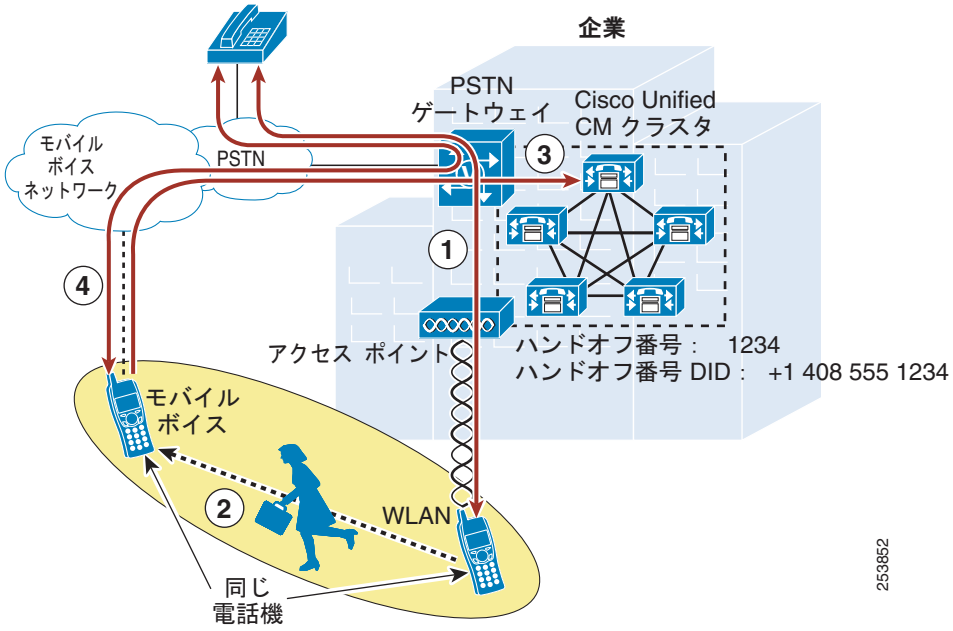
以降の例では、ハンドオフ番号は +1 408 555 1234 であるとします（これは、完全な E.164 形式のハンドオフ番号です）。Nokia Call Connect の Voice Call Continuity（VCC）設定の下の [Cellular Handover number] は、この番号に設定されています。

すべての着信コールは、アップストリーム ゲートウェイによって 4 桁に短縮されるため、Unified CM 内に設定するハンドオフ番号は 1234 です。Nokia Call Connect の VCC 設定の下の [VoIP Handover number] は、1234 に設定されています。

ハンドアウト（WLAN から携帯電話へ）

図 25-28 は、社内の Nokia デュアルモード電話機におけるアクティブなコールが、WLAN インターフェイスから会社の公衆網ゲートウェイ経由でモバイル ボイス ネットワーク（デバイスの携帯電話インターフェイス）に移動されるハンドアウト動作を示しています。図に示すように、企業の WLAN に関連付けられ、Unified CM に登録された Nokia デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。Nokia デュアルモード ユーザが社外への移動を開始します（ステップ 2）。WLAN 信号強度が 1,000,000 マイクロ秒（1 秒、VCC の [WLAN HO hysteresis] 設定のデフォルト値）にわたって -78 dBm（VCC の [WLAN HO threshold] 設定のデフォルト値）未満に減衰すると、モバイル ボイス ネットワークおよび公衆網経由で会社の公衆網ゲートウェイに対して +1 408 555 1234（VCC の [Cellular Handover number] 設定、Unified CM で設定されたハンドオフ番号に対応）へのサイレント バックグラウンド コールが開かれ、Unified CM に送信されます（ステップ 3）。このコールが受信されると、発信番号と、システムに設定されているすべてのモビリティ ID が照合されて、一致するものがある場合には、WLAN を通過していた RTP ストリームが公衆網ゲートウェイにリダイレクトされ、デュアルモード デバイスと元の公衆網電話機との間のコールは会社のゲートウェイで固定されて、中断されずに継続します（ステップ 4）。

図 25-28　Nokia Call Connect デュアルモード ハンドアウト（WLAN からモバイル ボイス ネットワークへ）

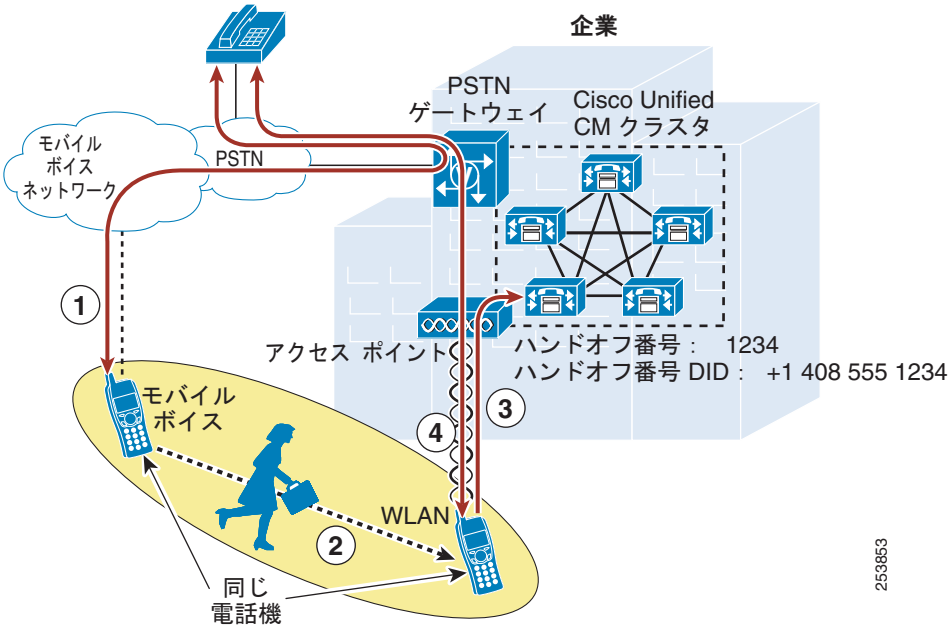


Nokia Call Connect デュアルモード クライアントでは、[Switch to Cellular] または [Handover to GSM] コール中メニュー オプションを使用した手動でのハンドアウトもサポートされています。これらの手動でのハンドアウト方法が利用可能であるかどうか、およびその動作は、デバイス タイプとファームウェアのバージョンに応じて異なります。バージョン 3.1 以前のバージョンのファームウェアが実行されているデバイスでは、[Switch to Cellular] メニュー オプションを選択すると、アクティブなコールが、会社の公衆網ゲートウェイ経由でデバイスのモバイル ボイス ネットワーク インターフェイスにブラインド転送されます。バージョン 3.2 以降のバージョンのファームウェアが実行されているデバイスでは、[Handover to GSM] メニュー オプションを選択すると、[WLAN HO threshold] および [WLAN HO hysteresis] の各 VCC 設定を使用しないで、図 25-28 のステップ 3 に示すように Unified CM のハンドオフ番号を使用した手動ハンドオフが実行されます。

ハンドイン（携帯電話から WLAN へ）

図 25-29 は、社外の Nokia デュアルモード電話機におけるアクティブなコールが、モバイル ボイス ネットワーク インターフェイスから会社の公衆網ゲートウェイ経由でデバイスの WLAN インターフェイスに移動されるハンドイン動作を示しています。図に示すように、モバイル ボイス ネットワーク上の Nokia デュアルモード デバイスと、公衆網ネットワーク上の電話機との間に既存のコールがあります（ステップ 1）。Nokia デュアルモード ユーザが社内に移動し（ステップ 2）、バックグラウンドでデバイスが WLAN インフラストラクチャに関連付けられて、Unified CM に登録されます。登録後、デバイスは、VCC の [WLAN HO hysteresis high] 設定に指定された時間（デフォルトで 60 秒）だけ待機し、1234（VCC の [VoIP Handover number] 設定、Unified CM で設定された Unified CM ハンドオフ番号に対応）へのサイレント バックグラウンド コールを開いたあと、Unified CM に送信します（ステップ 3）。このコールが受信されると、発信元である会社の電話番号と、システムに設定されている Nokia S60 デュアルモード電話機が照合されて、一致するものがある場合には、モバイル ボイス ネットワーク、公衆網、および会社の公衆網ゲートウェイを通過していたコールが WLAN ネットワークにリダイレクトされ、デュアルモード デバイスと元の公衆網電話機との間のコールは中断されずに継続します（ステップ 4）。

図 25-29　Nokia Call Connect デュアルモード ハンドイン（モバイル ボイス ネットワークから WLAN へ）



Nokia Call Connect の VCC 設定の詳細については、次の Web サイトで入手可能な『*Nokia Call Connect for Cisco User's Guide*』を参照してください。

http://europe.nokia.com/support/download-software/nokia-call-connect-for-cisco

Nokia Call Connect デュアルモード クライアントの WLAN 設計上の考慮事項

Nokia Call Connect デュアルモード クライアントを配置する際には、次の WLAN ガイドラインを考慮してください。

- Voice Continuity Configuration（VCC）設定の下の [WLAN HO Threshold] の設定は、ユーザが WLAN カバレッジ エリアから出たときに自動ハンドオフの遅延を経験しない限り、デフォルト設定（Nokia Call Connect 2.1 以降の場合は 73）のままにしておいてください。
- [WLAN HO Threshold] を低い値に調整すると、ユーザが WLAN カバレッジ エリアを離れたときの高速自動ハンドオフを保証できます。
- [WLAN HO Threshold] の調整は、WLAN Access Point（AP）間のローミングのトリガーしきい値にも影響します。[WLAN HO Threshold] の設定値を下げると、AP 間のローミングしきい値も低くなり、結果、AP 間のローミングが高速になります。ユーザが WLAN 上で低い音声品質を経験している場合、および AP 間のローミングが低速すぎる場合には、この設定を低く調整することを検討してください。ただし、この値を下げると自動ハンドオフも高速になることを念頭に置いておいてください。

Nokia Call Connect の VCC 設定の詳細については、次の Web サイトで入手可能な『*Nokia Call Connect for Cisco User's Guide*』を参照してください。

http://europe.nokia.com/support/download-software/nokia-call-connect-for-cisco

Nokia Call Connect と Cisco Unified Mobility との間の相互作用

Nokia Call Connect デュアルモード クライアントは、Cisco Unified Mobility と統合して、Cisco モバイル コネクト、通話切替 DTMF 機能、2 ステージ ダイヤリング、シングル企業ボイスメール ボックス、およびデスクトップフォンのピックアップを利用できます。

Unified Mobility と統合するには、Unified CM 内で、Nokia デュアルモード電話機の携帯の番号を Nokia S60 デバイスに関連付けられたモビリティ ID として設定する必要があります。システム内で携帯の番号がモビリティ ID として設定されると、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合に、モバイル コネクトを利用して、ユーザの会社の電話番号への着信コールをモバイル ボイス ネットワークを経由して Nokia デュアルモード デバイスに転送できます。Nokia デュアルモード デバイスが社内にあり、Unified CM に登録されている状況においては、会社の番号への着信コールはデバイスのモバイル ボイス ネットワーク インターフェイスには転送されません。Nokia デュアルモード デバイスが社内にある場合は、デバイスの WLAN インターフェイスだけが着信コールを受信します。これにより、会社の公衆網ゲートウェイ リソースの必要以上の消費を回避できます。

社外にあり、Unified CM に登録されていない場合、Nokia デュアルモード デバイスでは、会社の任意の固定コールに対して、DTMF を使用して通話切替機能を呼び出したり、デスクトップフォンのピックアップを実行したりできます。Nokia Call Connect 2.1 以降のクライアントは、社外にいるユーザが自身を会社の PSTN ゲートウェイにアンカーするために、会社を通じて発信コールを行いたいというシナリオのために、シスコ エンタープライズ機能アクセス 2 ステージ ダイヤリング機能のオートメーションを提供します。エンタープライズ機能アクセス 2 ステージ ダイヤリングの詳細については、「2 ステージ ダイヤリングを伴うエンタープライズ機能アクセス」（P.25-52）を参照してください。

Nokia Call Connect クライアントの 2 ステージ ダイヤリング機能が有効になっている場合は、そのデバイスによって携帯電話インターフェイスに対して発信されたすべてのコールが、Unified CM 内のエンタープライズ機能アクセス 2 ステージ ダイヤリング機能を利用します。Nokia Call Connect 内で設定されている 2 ステージ ダイヤリング番号 の値が、すべての発信携帯電話コールに対してクライアントがダイヤルする番号を決定します。この設定済みの番号は、Unified CM システム上のエンタープライズ機能アクセスの番号に対応している必要があります。Nokia Call Connect クライアント内で設定されている 2 ステージ ダイヤリング PIN の値が、コールがいったんエンタープライズ機能アクセスの番号に接続された後、Unified CM に送信される認証キー シーケンスを決定します。この設定済み PIN は、Unified CM 内のエンド ユーザ アカウントに下で設定されているとおりのユーザの PIN に対応している必要があります。Nokia Call Connect クライアントは、2 ステージ ダイヤル コールを支援するために、これら 2 つの設定に加えて、ユーザがダイヤルまたは選択した番号を使用します。

（注）　エンタープライズ機能アクセス 2 ステージ ダイヤリング オートメーションが使用できるのは、Nokia S60 3.2 ファームウェア バージョンでだけです。

また、Nokia デュアルモード ユーザは、IVR ベースの手動モバイル ボイス アクセス 2 ステージ ダイヤリング機能を利用して、会社を通じてコールをダイヤルし、それらのコールを会社のゲートウェイに固定できます。

Nokia デバイスが Cisco Unified Mobile Communicator クライアントも実行している場合は、ユーザにとって Dial-via-office での経験の方がはるかに優れているという理由で、ユーザは、エンタープライズ機能アクセスまたはモバイル ボイス アクセス 2 ステージ ダイヤリング方式の代わりに、そのクライアントで使用できる Dial-via-office 機能を利用できます。

Nokia デュアルモード デバイスに対してモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、これらの番号を Unified CM 内の Nokia S60 デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先を Nokia デバイスに関連付ける場合は、リモート接続先プロファイルを設定する必要はありません。

Unified Mobility の機能セット、および設計と配置の考慮事項の詳細については、「Cisco Unified Mobility」（P.25-37）を参照してください。

デュアルモード電話機のハイ アベイラビリティ

デュアルモード電話機は、その特性上ネットワーク接続に関して非常に高い可用性を備えていますが（企業の WLAN ネットワークが利用できない場合には、モバイル ボイス ネットワークを使用して音声サービスおよびデータ サービスを利用できます）、企業の WLAN および IP テレフォニー インフラストラクチャのハイ アベイラビリティについては考慮の余地があります。

まず、企業の WLAN は、冗長な WLAN アクセスが可能になるように配置する必要があります。たとえば、AP およびその他の WLAN インフラストラクチャ コンポーネントは、ワイヤレス AP の 1 つに障害が発生しても、デュアルモード デバイスのネットワーク接続には影響がないように配置する必要があります。同様に、常にデュアルモード デバイスがネットワークに安全に接続できるように、WLAN の管理およびセキュリティ インフラストラクチャも高い冗長性を備えた配置にする必要があります。

次に、Unified CM のコール処理サービスおよび登録サービスのハイ アベイラビリティについて考慮する必要があります。Unified CM のコール処理サービスを利用する企業内の他のデバイスと同様に、デュアルモード電話機も Unified CM に登録する必要があります。Unified CM クラスタのアーキテクチャにはプライマリおよびバックアップのコール処理サービスおよびデバイス登録サービスが用意されており、冗長な特性を持っているため、1 つの Unified CM サーバ ノードで障害が発生しても、デュアルモード デバイスの登録やコール ルーティングは引き続き利用可能です。

公衆網アクセスについても同様の事項を考慮する必要があります。IP テレフォニー配置と同様、複数の公衆網ゲートウェイおよびコール ルーティング パスを配置して、公衆網への可用性の高いアクセスを確保する必要があります。このことは、デュアルモード電話機の配置に固有の考慮事項ではありませんが、重要な考慮事項です。

デュアルモード電話機のキャパシティ プランニング

デュアルモード電話機におけるキャパシティ プランニングに関する考慮事項は、登録、コール処理、公衆網アクセスなどのサービスのために IP テレフォニー インフラストラクチャおよびアプリケーションを利用する他の IP テレフォニー エンドポイントまたはデバイスと同じです。

社内にデュアルモード電話機を配置する場合、Unified CM における登録の負荷および Unified Mobility の制限について考慮することが重要です。1 つの Unified CM サーバでは、最大 10,000 のデバイスの設定および登録を処理できます。デュアルモード電話機を展開する場合、サーバあたりでサポートされる最大デバイス数を考慮する必要があります。場合によっては、追加の負荷を処理するために、コール処理サブスクライバ ノードを追加で展開する必要があります。

また、「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）で説明したように、1 つの Unified CM クラスタ内のリモート接続先およびモビリティ ID の最大数は 15,000 です。ほとんどのデュアルモード デバイスは、モバイル コネクト、デスクトップフォンのピックアップ、2 ステージ ダイヤリングなどの機能を利用するために Unified Mobility と統合されるため、これらの各デュアルモード デバイスの携帯電話番号は Unified CM クラスタ内にモビリティ ID として設定する必要があります。これは、Unified Mobility との統合を容易にするため、場合によってはハンドオフを容易にするために必要です。したがって、デュアルモード電話機を Unified Mobility と統合する場合には、Unified CM クラスタにおけるリモート接続先およびモビリティ ID の全体的な容量を考慮して、十分な容量を確保することが重要です。追加のユーザまたはデバイスがシステム内の Unified Mobility にすでに統合されている場合は、これらのユーザまたはデバイスによって、デュアルモード デバイスで利用可能なリモート接続先およびモビリティ ID の空き容量が制限される可能性があります。

デスクトップフォンの統合を使用して iPhone 用に Cisco Mobile デュアルモード クライアントを配置する場合、CTI キャパシティも考慮する必要があります。この機能を使用するにはデスクトップフォンのプライマリ回線の CTI モニタリングが必要なため、デスクトップフォンの統合が有効になっている Cisco Mobile デュアルモードのユーザごとに Unified CM システムで CTI 接続が消費されます。この負荷は、システムの CTI キャパシティ全体に関連して考慮する必要があります。

デュアルモード電話機を配置する場合、Unified CM システムおよび公衆網ゲートウェイの全体的なコール処理容量も考慮する必要があります。デュアルモード デバイスの実際の設定および登録を処理する以外に、システムでは、これらの新しいデュアルモード電話機とユーザによって増加する BHCA の影響を吸収するために十分な容量も必要です。同様に、デュアルモード デバイスを処理するのに十分な公衆網ゲートウェイの容量を確保することも重要です。通常、デュアルモード デバイスを持つユーザは頻繁に移動することが多いため、Unified Mobility に統合されているデュアルモード デバイスではこのことは特に重要です。通常、頻繁に移動するユーザは、モバイル ユーザの会社の電話番号への着信コールによって公衆網への 1 つ以上のコールが発信されるモバイル コネクトなどのモビリティ機能や、会社の公衆網ゲートウェイを利用してユーザが会社経由でコールを発信する 2 ステージ ダイヤリングなどを使用することで、会社の公衆網ゲートウェイの負荷を高める傾向にあります。

上記の考慮事項は、デュアルモード電話機に固有のものではありません。これらの考慮事項は、デバイスやユーザが Unified CM に追加されることによって Unified Communications システム全体の負荷が高まるすべての状況に当てはまります。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を使用して、Unified CM を含む Cisco Unified Communications システムの容量を計算できます。このサイジング ツールでは、システム全体の容量を計算するための入力としてデュアルモード電話機デバイス数を受け取り、入力された数のデュアルモード デバイスおよびそれらのデバイスがシステムの全体的なサイズに与える影響に対応できる適切なシステム サイズを、デバイスの登録、コール処理（BHCA）、およびゲートウェイの利用負荷に基づいて計算します。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を http://tools.cisco.com/cucst で入手できます。

デュアルモード電話機の設計上の考慮事項

デュアルモードの電話機とクライアントを配置する場合には、次の設計上の考慮事項を遵守します。

- モバイル ボイス ネットワークとモバイル データ ネットワーク、および WLAN ネットワークの両方に同時に接続するために、デュアルモード電話機では、Dual Transfer Mode（DTM; デュアル転送モード）がサポートされている必要があります。これにより、デバイスの携帯電話無線機と WLAN インターフェイスの両方からデバイスに到達可能になり、両方のインターフェイスでコールを発信および受信できます。モバイル ボイス ネットワークおよびモバイル データ ネットワークでデュアル接続デバイスがサポートされていない場合には、適切なデュアルモード クライアント操作が実行できない場合があります。
- AP は、20 % 以上のセル オーバーラップを確保して配置する必要があります。このようにオーバーラップさせることによって、デュアルモード デバイスがロケーション内で移動した場合に AP 間で正常にローミングして、ボイス ネットワーク接続およびデータ ネットワーク接続を維持できます。
- パケット損失を最小限に抑えるために、AP は -67 dBm のセル パワー レベル境界（またはチャネル セル半径）で配置する必要があります。また、同一チャネルのセル境界の分離は、約 19 dBm にする必要があります。19 dBm の同一チャネル セル分離は、AP またはクライアントにおいて、同じチャネルに関連付けられている他のデバイスとの同一チャネル干渉が発生しないようにするために重要です。同一チャネル干渉が発生すると、音声品質が低下するためです。
- デュアルモードの電話機とクライアントを接続する場合は、エンタープライズ クラスの音声に最適化された WLAN ネットワークだけを使用することを推奨します。ほとんどのデュアルモードの電話機とクライアントは、パブリックおよびプライベートの WLAN アクセス ポイントやホット スポットに接続し、インターネットを経由して会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、このように接続した場合の音声品質は保証されません。

- Unified Mobility モバイル コネクト機能では、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合には、着信コールはデュアルモード デバイスの設定されたモビリティ ID には転送されません。これは、企業の公衆網リソースの利用を削減するための仕様です。デュアルモード デバイスは Unified CM に登録されるため、システムでは、デバイスが社内で到達可能であるかどうかを把握できます。社内で到達可能である場合は、コールを公衆網に転送してデュアルモード デバイスのモバイル ボイス ネットワーク インターフェイスを呼び出す必要性がありません。モバイル コネクトでは、デュアルモード デバイスが登録されていない場合にだけ、ユーザの会社の電話番号への着信コールが公衆網のモビリティ ID 番号に転送されます。
- デュアルモード電話機を配置する場合、必要なダイヤリング ストリングを正規化して、ユーザが社内または社外のいずれからでも同じ番号をダイヤルして特定の着信側接続先に到達できるようにすることを推奨します。モバイル ネットワークにおけるダイヤリングは、通常完全な E.164（先頭に「+」が付く場合と付かない場合があります）を使用して行われ、携帯電話の連絡先は通常完全な E.164 番号で保存されるため、デュアルモード電話機においては、企業のダイヤル プランは完全な E.164 番号または先頭に「+」を付けた完全な E.164 番号を使用できるように設定することを推奨します。このように企業のダイヤル プランを設定することによって、ユーザはデバイスが社内の Unified CM に登録されているかどうかを気にする必要がなくなるため、最善のエンド ユーザ ダイヤリング エクスペリエンスを提供できます。
- デュアルモード電話機のユーザが緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。これは、通常モバイル プロバイダー ネットワークでは、企業の WLAN ネットワークよりもはるかに信頼性のある位置情報が提供されるためです。デュアルモード電話機から緊急コールを発信したり位置サービスを利用したりする場合にモバイル ボイス ネットワークだけが利用されるように、Unified CM 内でデュアルモード デバイスを設定して、911、999、112 などの緊急番号へのコールを許可するルート パターンにこれらのデバイスからアクセスできないようにします。デュアルモード電話機のユーザに対して、すべての緊急コールを企業ネットワークではなくモバイル ボイス ネットワーク経由で発信するように指示します。
- デュアルモード デバイスにおいて、ビジネス コールの発信および受信時に可能なかぎりエンタープライズ IP テレフォニー インフラストラクチャが使用されるようにするために、次の Nokia Call Connect クライアント設定を行うことを推奨します。
  - Nokia Call Connect クライアントの SCCP 登録設定を [Always On] に設定して、Nokia デバイスが企業の WLAN ネットワークに関連付けられた場合に Unified CM への登録が試みられるようにします。
  - Nokia デュアルモード電話機の優先コール タイプまたはデフォルト コール タイプの設定を [Internet Call] に設定して、Nokia Call Connect クライアントが Unified CM に登録された場合に、デバイスからの発信コールにおいて常にデュアルモード電話機の WLAN インターフェイス経由でルーティングが試みられるようにします。
- デスクトップフォンの統合を使用した Cisco Mobile を配置する場合、Cisco Mobile ユーザのエンド ユーザ アカウントが CTI で有効になっている必要があります。また、デスクトップフォンが通話を自動でパークし、通話がデスクトップフォンから Cisco Mobile クライアントに転送された場合は常に Cisco Mobile クライアントが取得できるよう、コール パークをシステム レベルで設定する必要があります。Unified CM システム全体をサイジングする場合、この機能の CTI オーバーヘッドを考慮する必要があります。
- Cisco Mobile iPhone または Cisco Jabber Android デュアルモード クライアントを展開する際には、次の展開ガイドラインに従って WLAN ネットワークを設定してください。
  - 企業の WLAN 内のレイヤ 3 での Cisco Mobile iPhone および Cisco Jabber Android デュアルモード デバイスのローミングを最小限に抑えます。デバイスの IP アドレスが変わるレイヤ 3 のローミングでは、ローミング時間が長くなり、音声パケットがドロップされるほか、コールがドロップされる場合もあります。

  - 最も高速な AP 間ローミングを確保するために、企業の WLAN 内で Cisco Mobile および Cisco Jabber デュアルモード デバイスが使用するすべての AP に対して同一の SSID を設定します。
  - コール中に WLAN インフラストラクチャ内の他の AP に参加するように求められるとコールが中断されるおそれがあるので、これを防ぐために、会社のすべての WLAN AP を自身の SSID をブロードキャストするように設定します。
- Nokia Call Connect デュアルモード クライアントの配置には、Nokia Call Connect クライアント内の [WLAN HO Threshold] の設定を低くして、より高速な自動ハンドアウトを保証します。ただし、この設定を下げると AP 間のローミング速度も上がることを念頭に置いておいてください。

Cisco Unified Mobile Communicator

Cisco Unified Mobile Communicator は、携帯電話から Cisco Unified Communications アプリケーションにアクセスし、利用する機能をユーザに提供するモビリティ ソリューションです。Cisco Unified Mobile Communicator および Cisco Mobile グラフィカル クライアントは、Cisco Unified Mobility Advantage ソフトウェアを実行しているサーバと連動して、携帯電話の機能にアクセスし、制御するためのリッチ ユーザ インターフェイスを提供します。このシステムは既存の社内 LDAP ディレクトリに統合されるため、ユーザはすべてのデバイス上で単一のクレデンシャル セットを使用できます。また、Unified Mobile Communicator と Unified Mobility Advantage 間のすべてのトラフィックが、Secure Socket Layer（SSL）プロトコルによって保護されます。Unified Mobile Communicator は、携帯電話ユーザに次の機能を提供します。

- 社内および個人ディレクトリへのアクセス
- プレゼンスとバディの会社との同期化
- 社内ボイスメールへのビジュアル アクセス
- デスクトップフォンの不在コール、発信コール、および受信コールの履歴確認
- セキュア Store-and-Forward テキスト メッセージング
- 会議通知の受信
- Cisco Unified CM を使用した Dial-via-office

（注）　上記に記載されている機能が、サポート対象のすべてのハンドセットまたはモバイル オペレーティング システムで利用できる機能のすべてではありません。

（注）　引き続き、Cisco Unified Mobility Advantage 7.1(3) はサポートされ、Cisco Unified CM 8.*x* および他の Cisco Unified Communications システム 8.*x* アプリケーションと相互運用できます。この項のすべての説明は、Unified Mobility Advantage サーバの 7.1(3) に基づいています。このソリューションの具体的なハードウェアおよびソフトウェア要件の詳細については、http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html で入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage, Cisco Mobile, and Cisco Unified Mobile Communicator*』を参照してください。

Cisco Unified Mobile Communicator の電話サポートとデータ プラン要件

Cisco Unified Mobile Communicator クライアント アプリケーションはさまざまなモバイル デバイスで動作しますが、その洗練された機能性によって、サポートされる電話機が制限されるようなデバイス要件が最小限に抑えられています。

Cisco Unified Mobile Communicator は、次のモバイル オペレーティング システムまたはハンドセットで実行するように設計されています。

- Windows Mobile 6.0 または 6.1 Standard
- Nokia Symbian および Nokia S60 Third Edition（Nokia ハンドセット）
- ファームウェア バージョン 3.0.1 以降が実行されている Apple iPhone 3G または 3GS（iPhone ハンドセット）
- Research In Motion（RIM）Blackberry（Blackberry ハンドセット）

（注）　iPhone および Blackberry デバイス対応の Cisco Unified Mobile Communicator クライアントは、Cisco Mobile と呼ばれています。

ハンドセット モデルのサポートは、モバイル オペレーティング システム（OS）によって異なりますが、特定のハンドセット サポート認証は必要ありません。各モバイル OS について、シスコでは最低限の要件をサポートするハンドセットを必要とします。これらの要件はモバイル OS ごとに異なりますが、次のリストにハンドセットがサポート対象となるための一般的な要件を示します。

- モバイル OS の特定のバージョン（OS ごとに異なる）
- 特定のフォーム ファクタ、スクリーン サイズ、およびキーボード テクノロジー（オペレーティング システムごとに異なる）
- 認定された認証局（VeriSign または GeoTrust）からのルート認証のインストール
- サードパーティ アプリケーションのインストールまたは実行に対する制限なし

（注）　実際のユーザ エクスペリエンスはデバイスによって異なる可能性があります。

特定のハンドセット要件の詳細については、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

サポートされているデバイスの提供に加えて、ユーザは、サポートされているデータ プランでそのデバイスを使用する必要があります。クライアントは、モバイル データ ネットワークを使用して Cisco Unified Mobility Advantage サーバと通信します。クライアントとサーバは SSL を使用してすべてのデータ トラフィックを保護しますが、クライアントは、Unified Mobility Advantage 管理者がインストール中に指定したポート上でモバイル データ ネットワークを使用してサーバとの接続を開始します。

このポートが従来と異なる可能性があるため、クライアントは、モバイル データ ネットワークに無制限プランでアクセスできる必要があります。それに反して、多くのオペレータは、クライアントにポート 80 上の HTTP アクセスのみを許可するローエンドの「Web 専用」プランを提供します。この種のプランは、Unified Mobile Communicator と互換性がないため、機能しない可能性があります。代わりに、ユーザは、クライアントからサーバ上の任意のポートへの任意の TCP トラフィックを許可するプランに加入する必要があります。このプランは、VPN プランと呼ばれることがあります。ただし、Unified Mobility Advantage サーバが動的で変換済みのアドレスを適切にマップするため、クライアントはルーティング可能な IP アドレスや固定 IP アドレスを必要としません。

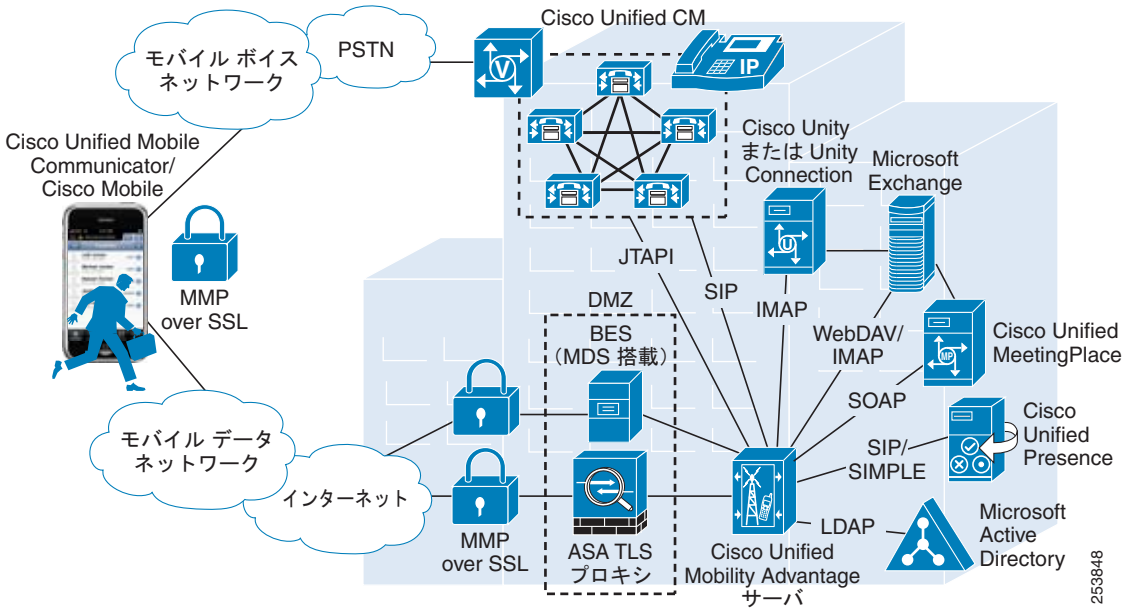
Cisco Unified Mobile Communicator クライアントはすべてのアプリケーション統合と機能を会社へのデータ接続に依存しているため、このデータ接続が極めて重要です。この重要な接続で消費される帯域幅には、かなりのばらつきがあります。これらの接続のさまざまな特性を考えると、分単位やバイト単位のプランではなく、無制限のデータ プランを強く推奨します。ただし、配置によっては、無制限のデータ プランに非常に多くのコストがかかる場合があります。帯域幅を見積もって計画する目的でシスコが行った調査によれば、Unified Mobile Communicator ユーザは、ビジュアル ボイスメール機能を使用しなければ、月平均で、約 5.6 MB の帯域幅を消費します。もちろん、帯域幅の消費は、エンド

ユーザの振る舞いによって大きく異なります。たとえば、大量のディレクトリ ルックアップを実行したり、大量のテキスト メッセージを送信したり、大量の Dial-via-office コールを発信したりするユーザは、このような機能をほとんど使用しないユーザよりも広い帯域幅を消費します。したがって、5.6 MB/月という平均値はほとんど参考になりません。ビジュアル ボイスメールを使用した場合は、1 分間のボイルメール メッセージで約 354 kb が消費されます。つまり、約 2 時間のビジュアル メッセージでこの月平均のすべてが消費される計算です。このことから、ビジュアル ボイスメールの使用中は帯域幅の要求が異常に高くなることが容易にわかります。

Cisco Unified Mobile Communicator のアーキテクチャ

このソリューションは、Cisco Unified Mobile Communicator、Adaptive Security Appliance (ASA) TLS プロキシ、および Cisco Unified Mobility Advantage サーバという主要な 3 つのコンポーネントで構成されています（図 25-30 を参照）。図 25-30 に示すように、Cisco Unified Mobility Advantage サーバは既存の Unified Communications アプリケーションおよび企業システムにアクセスします。

図 25-30　Cisco Unified Mobile Communicator のアーキテクチャ



モバイル デバイス上で Unified Mobile Communicator が起動するとユーザ セッションが開始されます。アプリケーションが開始すると、Microsoft Active Directory パスワードの入力が要求されます（プロビジョニング中にデバイスがユーザ アカウントに関連付けられるため、クライアントはユーザ ID を収集する必要がありません）。次に、クライアントが、モバイル データ ネットワークを使用して ASA TLS プロキシへの SSL 接続を開始します。この接続は、インターネットからの着信接続としてプロキシで検出されます。この接続に使用されるプロトコルは、Mobile Multiplexing Protocol（MMP）です。このプロトコルは、ハンドセットのバッテリ寿命を節約するように最適化されています。MMP プロトコルは、標準ベースの SSL パケットにカプセル化されます。

SSL 接続が確立されると、ASA から Unified Mobility Advantage サーバに要求が渡され、そこでユーザが LDAP ディレクトリに対して認証されます。SSL トラフィックを運搬する TCP 接続はクライアントによって維持されるため、サーバはアドレス変換や動的クライアント アドレスなどに関係なく、トラフィックをクライアントに委ねることができます。クライアントの接続期間を通して、ASA TLS プ

ロキシがクライアントからの着信パケットを復号し、厳格なパケット検査を実施してパケットが有効で許可されたユーザからのものであることを保証します。検査に合格したパケットは、ASA プロキシが再び暗号化して、Cisco Unified Mobility Advantage サーバに渡します。

Unified Mobile Communicator クライアント ユーザを認証するための LDAP クレデンシャルの使用に加えて、Unified Mobility Advantage サーバでもその他のバックエンド アプリケーション システムに接続するためにクレデンシャルが使用されます。たとえば、Microsoft Exchange サーバにユーザとして接続し、カレンダー、個人連絡表、および会議通知にアクセスするためにこの情報が使用されます。

ASA を TLS プロキシとファイアウォールの両方として配置するか、ASA を DMZ 内の TLS プロキシとしてだけ配置して外部ファイアウォールに依存するかに関係なく、2 つのポートを設定して、それらを外向きのファイアウォールまたはインターフェイス（インターネットと DMZ 間）と内向きのファイアウォールまたはインターフェイス（DMZ と会社間）の両方に対して開く必要があります。外部と内部の両方のファイアウォールに対して、次の一連の範囲に含まれるポートを開く必要があります。

- 外部ファイアウォール ポート
  - 5400 ～ 5500 の範囲のクライアント接続ポート（TCP/SSL）
  - 9000 ～ 9100 の範囲のプロビジョニング ポート（HTTP）
- 内部ファイアウォール ポート
  - 5400 ～ 5500 の範囲のクライアント接続ポート（TCP/SSL）
  - 9000 ～ 9100 の範囲のプロビジョニング ポート（HTTP）

（注） デフォルトのクライアント接続ポート（TCP/SSL）は 5443 で、デフォルトのプロビジョニング ポート（HTTP）は 9080 です。

（注） iPhone または Blackberry ハンドセットだけを配置している場合、これらのハンドセットはプロビジョニング ポートを介して Cisco Unified Mobile Communicator クライアントをダウンロードしないため、ファイアウォールのプロビジョニング ポートを開く必要はありません。このクライアントは、iPhone ハンドセットの場合は Apple App Store からダウンロードされ、Blackberry ハンドセットの場合は Blackberry Enterprise Server（BES）を介してハンドセットにプッシュされます。

Cisco Unified Mobile Communicator 環境に Blackberry ハンドセットを配置する場合、Cisco Mobile クライアントを実行する Blackberry デバイスは、社内に配置された Blackberry Enterprise Server（BES）経由で Cisco Unified Mobility Advantage サーバに接続する必要があるという点で、アーキテクチャ上の若干の変更があります。他の Cisco Unified Mobile Communicator クライアントおよび Cisco Mobile クライアントとは異なり、Blackberry クライアントから Unified Mobility Advantage サーバへの接続では、ASA 経由でのセキュリティは確保されません。その代わり、Blackberry デバイスと BES サーバとの間のセキュアな接続が使用され、BES サーバが Unified Mobility Advantage サーバと直接統合されます。BES サーバは、Mobile Data Service（MDS）とともに配置し、MDS で設定する必要があります。図 25-30 に示すように、BES サーバと ASA の両方を Unified Mobility Advantage サーバに統合して、Blackberry およびその他のサポートされているモバイル ハンドセットを同じシステム内に配置できます。Blackberry デバイス用に BES および MDS を Unified Mobility Advantage サーバに直接統合する方法の詳細については、次の Web サイトで入手可能なコンフィギュレーション ガイドの『*Enabling Support for Clients in Cisco Unified Mobility Advantage*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

Microsoft Active Directory（AD）環境では、LDAP サーバに関するサーバ固有の要件はありません。適切なドメインに属していればどのドメイン コントローラも動作します。Unified Mobility Advantage サーバからこのサーバに対して LDAP バージョン 3 の認証および検索要求が発行され、予期したとおりに AD ドメイン経由で伝播されます。Exchange サーバが複数存在する環境では、Cisco Unified Mobility Advantage サーバが AD に照会してユーザごとの適切なサーバを決定します。

Cisco Unified Mobile Communicator の機能

Cisco Unified Mobile Communicator は、ユーザが社外からモバイル デバイスを使用して社内のさまざまな Unified Communications アプリケーションにアクセスして利用できるようにします。次の企業アプリケーションを Unified Mobile Communicator ソリューションに統合できます。各アプリケーションからは後述するような機能が提供されます。

Cisco Unified Mobile Communicator ソリューションと統合できるサポート対象のアプリケーションおよびバージョンの全リストについては、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html

LDAP ディレクトリ

Cisco Unified Mobility Advantage サーバと Microsoft Active Directory が統合されます。Unified Mobile Communicator クライアント接続の認証に Active Directory が使用されるため、この統合が必要になります。ユーザの Active Directory アカウント パスワードが Cisco Unified Mobility Advantage サーバまたは Unified Mobile Communicator クライアントに保存されることはありません。クライアントの認証メカニズムの提供に加えて、クライアントからのディレクトリ ルックアップを解決し、ユーザがモバイル デバイスから社内ディレクトリを検索できるようにするためにも Active Directory が使用されます。図 25-30 に示すように、Active Directory との統合は LDAP 経由で行われます。

Cisco Unified CM

Cisco Unified Mobility Advantage サーバと Cisco Unified CM を統合することで、デスクトップフォン コール ログの同期化、Dial-via-office 機能、および Unified Mobility 統合を提供できます。この統合には、管理者が Unified CM に対していくつかの設定手順を実行する必要があります。エンタープライズ コール ログ統合では、Cisco Unified CM 内でアプリケーション ユーザ アカウントを設定して、Unified Mobile Communicator ユーザのデスクトップフォンをそのアカウントに関連付ける必要があります。このアカウントは、Unified Mobility Advantage サーバですべての Unified Mobile Communicator ユーザのデスクトップフォンをモニタして、不在コール、受信コール、および発信コールを収集するために使用されます。アプリケーション ユーザ アカウント数は最大 250 台のモニタ対象デバイスに制限され、Unified Mobility Advantage サーバの設定によって最大 4 つのアカウント名が許可されるため、最大 1,000 人のユーザが利用できます。Cisco Unified CM 内の各アプリケーション ユーザ アカウントを Standard CTI End Users グループと Standard CTI Enabled グループの両方に割り当てる必要があります。

Dial-via-office 機能と Unified Mobility との統合では、各ユーザの Unified Mobile Communicator デバイスを Cisco Unified CM 内のデバイスとして設定し、このデバイスにユーザの会社の電話番号（ユーザのデスクトップフォンと同じ電話番号）を設定して、ユーザの携帯電話の電話番号に設定されたモビリティ ID をこのデバイスに関連付ける必要があります。

エンタープライズ コール ログ統合、Dial-via-office、および Unified Mobility 統合の設定手順を含む、Unified CM との統合の詳細については、次の Web サイトで入手可能な Cisco Unified Mobility Advantage のインストールおよび設定マニュアルを参照してください。

http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html

デスクトップフォンのコール ログ統合

コール ログ統合を有効にされた Unified Mobile Communicator ユーザは、Unified Mobile Communicator クライアント上でデスクトップフォンからのコール履歴リスト（不在コール、発信コール、および着信コール）を確認できます。

図 25-30 に示すように、Unified Mobility Advantage サーバと Unified CM の間で JTAPI 接続が確立されます。この JTAPI 接続では、CTI を使用してユーザのデスクトップフォンのプライマリ回線に対する着信コールと発信コールがモニタされます。コール ログは、デスクトップフォンから Unified Mobile Communicator クライアントの方向にのみ同期化されることに注意してください。Unified Mobile Communicator クライアントからデスクトップフォンの方向には同期化されません。

Dial-via-office

Dial-via-office 機能を使用すれば、Cisco Unified CM テレフォニー インフラストラクチャと会社の公衆網ゲートウェイを使用して、Cisco Unified Mobile Communicator クライアントを実行している携帯電話からコールを開始できます。図 25-30 に示すように、この機能は、Unified Mobility Advantage サーバと Unified CM 間の SIP 接続上の SIP シグナリングによって実現されます。

Unified Mobile Communicator ユーザが携帯電話から発信したすべてのコールに対して、Unified Mobility Advantage 管理者が Dial-via-office の使用を命令できます。ただし、設定されている緊急番号または直接通話番号へのコールでは、Dial-via-office 命令が無視されます。管理者は、Unified Mobile Communicator ユーザに、Dial-via-office 機能を使用するかどうかといつ使用するかを決めさせることもできます。このとき、エンド ユーザは、コール（モバイル ボイス ネットワークに送信される設定済みの緊急電話番号または直接通話番号へのコール以外）の発信時に必ず Dial-via-office を使用する、または、コールごとにプロンプトを出力するように電話機を設定できます。

Cisco Unified Mobile Communicator ソリューションでサポートされている Dial-via-office には、次の 2 つのタイプがあります。

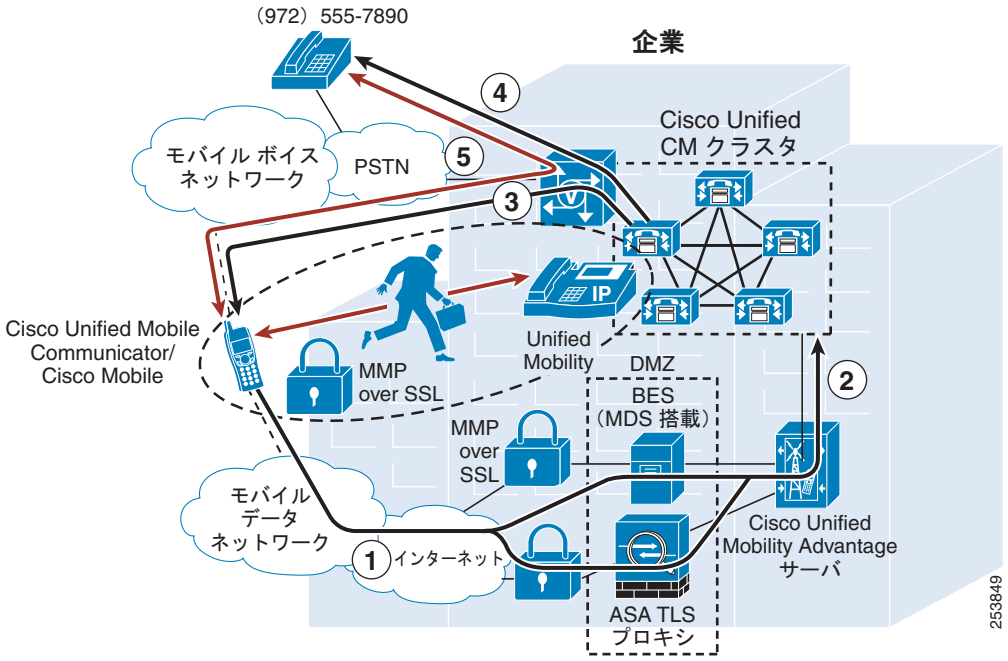
- 「Dial-via-office リバース コールバック」（P.25-90）
- 「Dial-via-office 転送」（P.25-91）

Dial-via-office リバース コールバック

図 25-31 に、Dial-via-office リバース コールバックのコール フローを示します。この例では、Unified Mobile Communicator ユーザが、公衆網電話機（972-555-7890）に電話をかけようとしています。ユーザが、番号をダイヤルするか、コンタクト リストまたはディレクトリ リストから番号を選択すると、会社と Cisco Unified Mobility Advantage サーバへのデータ接続上で SIP INVITE が生成されます（ステップ 1）。この SIP INVITE は、MMP プロトコルにカプセル化され、クライアントと Cisco Unified Mobility Advantage サーバ間の（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によって送信されます。この要求は、SIP 接続経由で Cisco Unified Mobility Advantage サーバから Cisco Unified CM に転送されます（ステップ 2）。次に、Unified CM によって、会社の公衆網ゲートウェイを使用して、ユーザの携帯電話番号へのコールバックが生成されます（ステップ 3）。Unified CM からの着信コールがモバイル デバイスで自動応答されると、ユーザが呼び出した番号または選択した番号にコールが転送されます（ステップ 4：この場合は 972-555-7890）。コールが遠端で応答されると、会社の公衆網ゲートウェイでコールが固定されます（ステップ 5）。コールが会社のゲートウェイに固定されたため、ユーザは、このコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility の通話切替機能を呼び出すことができます。

（注）　ユーザの携帯電話からのすべての音声またはメディアは、必ずモバイル ボイス ネットワーク上を通過します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

図 25-31　Cisco Unified Mobile Communicator、Dial-via-office リバース コールバック



Cisco Unified Mobile Communicator に Dial-via-office リバース コールバック機能が搭載されたほか、Unified Mobile Communicator クライアント設定内でコールバック先の代替番号を指定するオプションも追加されました。たとえば、コールバックを携帯電話で受信するのではなく、会議室の電話に転送できます。

（注）　Dial-via-office リバース コールバック機能の呼び出し時に、Unified CM からのコールバックがユーザ指定の代替番号に転送された場合は、そのコールをデスクトップフォンでピックアップしたり、通話切替機能を呼び出すことはできなくなります。

Dial-via-office リバース コールバックは、Windows Mobile、Nokia、および Blackberry のモバイル ハンドセットでサポートされています。

Dial-via-office 転送

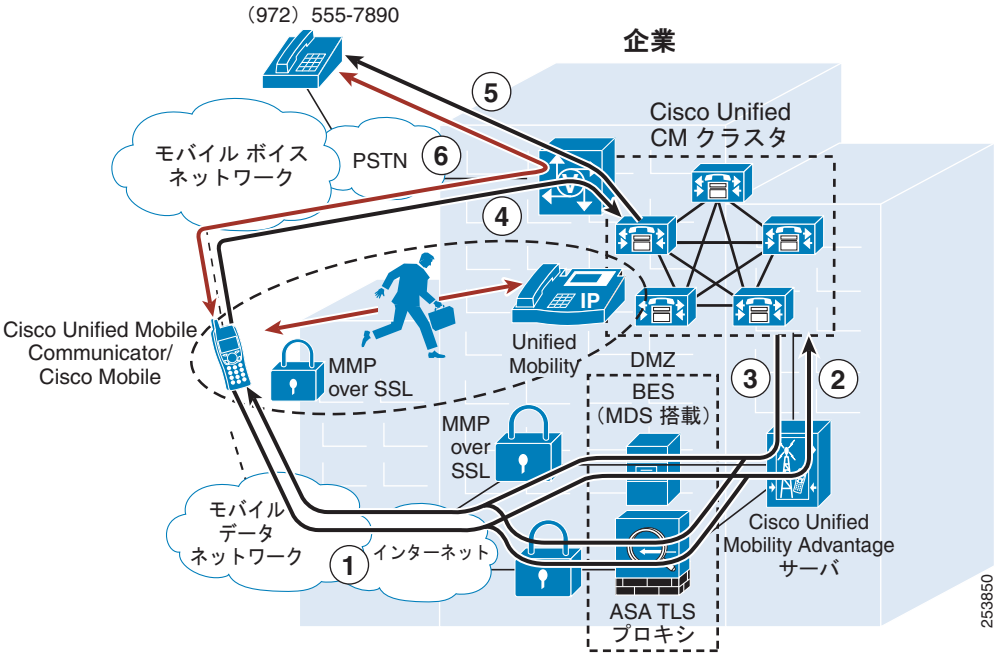
図 25-32 に、Dial-via-office 転送のコール フローを示します。この例では、Unified Mobile Communicator ユーザが、公衆網電話機（972-555-7890）に電話をかけようとしています。ユーザが、番号をダイヤルするか、コンタクト リストまたはディレクトリ リストから番号を選択すると、会社と Cisco Unified Mobility Advantage サーバへのデータ接続上で SIP INVITE が生成されます（ステップ 1）。この SIP INVITE は、MMP プロトコルにカプセル化され、クライアントと Cisco Unified Mobility Advantage サーバ間の（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によって送信されます。この要求は、SIP 接続経由で Cisco Unified Mobility Advantage サーバから Cisco Unified CM に転送されます（ステップ 2）。次に Unified CM から、設定されているシステム全体のエンタープライズ機能アクセス番号を使用して Cisco Unified Mobility Advantage サーバに応答があり、そこから（クライアント タイプに応じて）ASA または BES サーバ経由のセキュアな接続によってユーザのモバイル デバイスに転送されます（ステップ 3）。モバイル デバイスで番号が受信されると、Cisco Unified Mobile Communicator クライアントは、モバイル デバイスからエンタープライズ機能アクセス番号へのコールを自動的に発信します（ステップ 4）。Unified CM でこのコールが受信されると、ユーザに設定されたモビリティ ID に対して着信コールの発信者 ID が照合されます。

着信コールの発信者 ID がユーザに設定されたモビリティ ID と一致すると、システムから、ユーザがダイヤルまたは選択した番号にコールが発信されます（ステップ 5。この場合は 972-555-7890）。コールが遠端で応答されると、会社の公衆網ゲートウェイでコールが固定されます（ステップ 6）。コールが会社のゲートウェイに固定されたため、ユーザは、このコール中の任意の時点で Unified Mobility のデスクトップフォン ピックアップ機能を使用したり、Unified Mobility の通話切替機能を呼び出すことができます。

（注） Dial-via-office 転送コールを正常に実行するには、Unified CM で公衆網ネットワークから受信する着信コールの発信者 ID が、Dial-via-office コールを発信する Unified Mobile Communicator デバイスに設定されたモビリティ ID 番号と一致する必要があります。公衆網から着信コールの発信者 ID が送信されない、あるいはその発信者 ID がユーザに設定されたモビリティ ID と一致しない場合、Dial-via-office 転送コールは失敗します。

（注） ユーザの携帯電話からのすべての音声またはメディアは、必ずモバイル ボイス ネットワーク上を通過します。メディアが会社へのデータ接続を通過することはありません。モバイル データ ネットワーク接続は、コール シグナリング トラフィックとその他のアプリケーションの相互作用以外には使用されません。

図 25-32　Cisco Unified Mobile Communicator、Dial-via-office 転送



（注） バージョン 3.1 よりも前の iPhone ファームウェアでは、Dial-via-office 転送コールは、ユーザが手動で操作してコールを完了する必要があります。バージョン 3.1 よりも前の iPhone ファームウェアでは、Dial-via-office コールは自動的に完了しません。図 25-32 のステップ 3 で、ユーザに対してクライアントにダイアログボックスが表示されます。ステップ 4 でエンタープライズ機能アクセス番号へのコールを発信するには、ユーザは [Call] を選択する必要があります。

Cisco Unified Mobile Communicator から、Dial-via-office 転送コール用に Unified CM によって送信されるエンタープライズ機能アクセス番号にダイヤルできるようにするには、送信される番号が完全な E.164 番号であり、モバイル ボイス ネットワークを介してダイヤルできることが必要です。Unified CM 内の [Enterprise Feature Access Directory Number] フィールド（[Call Routing] > [Mobility Configuration] の下）で設定された番号が完全な E.164 番号ではない場合、管理者は、Cisco CallManager サービスの Dial-via-Office Forward Service Access Number サービス パラメータに、Unified CM 内で設定されたエンタープライズ機能アクセス ディレクトリ番号に対応する完全な E.164 番号を設定する必要があります。[Dial-via-Office Forward Service Access Number] サービス パラメータが設定されていないと、Unified CM から、設定されたエンタープライズ機能アクセス番号がそのまま送信されます。この番号は完全な E.164 番号ではないため、Cisco Unified Mobile Communicator から Unified CM システムへのコール（図 25-32 のステップ 4）は失敗し、Dial-via-office 転送機能は動作不能になります。

たとえば、エンタープライズ機能アクセス ディレクトリ番号が Unified CM 内で 51234 として設定されているとします。[Dial-via-Office Forward Service Access Number] が設定されていない場合、Unified CM はそのエンタープライズ機能アクセス番号 51234 を Unified Mobility Advantage に転送し、その結果、Unified Mobile Communicator デバイスのコール ダイアログに 51234 と表示されます。ユーザが [Call] オプションを選択すると、電話機からモバイル ボイス ネットワークを介して 51234 へのコールが試行されますが、このコールは失敗します。ただし、[Dial-via-Office Forward Service Access Number] が 9195551234 と設定されている場合には、Unified CM から Unified Mobility Advantage にエンタープライズ機能アクセス番号 9195551234 が転送されます。これにより、ユーザが [Call] オプションを選択すると、コールは適切にモバイル ボイス ネットワークと公衆網を介して企業にルーティングされます。

Dial-via-office 転送は、Cisco Mobile、つまり iPhone および Blackberry 対応の Cisco Unified Mobile Communicator クライアントでサポートされています。

Nokia Call Connect と Cisco Unified Mobile Communicator との間の相互作用

Nokia Call Connect デュアルモード クライアントは、Nokia 対応の Cisco Unified Mobile Communicator クライアントと並行して使用できます。両方のクライアントが配置された場合、Nokia デバイスからエンタープライズ IP テレフォニー インフラストラクチャを利用して社内でコールを発信および受信できるだけでなく、ディレクトリ ルックアップ、デスクトップフォンのコール ログ統合、プレゼンス、ビジュアル ボイスメール、テキスト メッセージング、Dial-via-office などの Unified Mobile Communicator の機能を利用することもできます。Nokia Call Connect デュアルモード クライアントと Unified Mobile Communicator を統合するには、Unified CM 内の Nokia S60 デバイスの設定ページの [Enable Cisco Unified Mobile Communicator] チェックボックスをオンにします。

Unified CM 内で設定すると、両方のクライアントを Nokia デュアルモード デバイス上で実行できるようになります。ただし、Dial-via-office 機能に対する影響を理解することが重要です。2 つのクライアント内の他のすべての機能は通常どおり動作しますが、Nokia Call Connect クライアントが同じデバイスにインストールされている場合には、Dial-via-office 機能の動作は若干異なります。Unified Mobile Communicator 内の Dial-via-office 機能は、モバイル ボイス ネットワーク（携帯電話インターフェイス）経由でルーティングされたコールに対してだけ実行されます。このため、Nokia Call Connect クライアントから WLAN インターフェイス経由で発信されたコールでは、Dial-via-office は実行されません。この場合コールはすでにエンタープライズ IP テレフォニー インフラストラクチャ経由で発信されているため、これは適切な動作です。

ただし、モバイル ボイス ネットワーク（携帯電話インターフェイス）経由で発信されたコールでは、Unified Mobile Communicator クライアント内の Dial-via-office 設定、または Cisco Unified Mobility Advantage サーバの Dial-via-office 設定に応じて、Dial-via-office 機能が実行されるかどうかが決まります。Unified Mobility Advantage サーバの管理者がユーザに対して Dial-via-office の使用を強制した場合、Unified Mobile Communicator クライアントでは、デバイスの携帯電話インターフェイスから発信されたすべてのコールで Dial-via-office の呼び出しが試みられます。このような状況においては、ユーザは、Unified Mobile Communicator クライアントで設定パラメータ [Allow dial via office for] を [Call from this app] に設定して、Unified Mobile Communicator クライアントから直接発信されたコー

ルでだけ Dial-via-office が呼び出されるようにする必要があります。クライアントをこのように設定することによって、ユーザは、Unified Mobile Communicator クライアントの外部で携帯電話インターフェイス経由でコールが発信された場合に Dial-via-office 機能が実行されないようにできます。たとえば、Nokia Call Connect クライアントで企業の WLAN からモバイル ボイス ネットワークへのコールのハンドアウトが試みられている場合には、Nokia デバイスで Dial-via-office を実行することは望ましくありません。ハンドアウト時には、Nokia デュアルモード デバイスの携帯電話インターフェイスから Unified CM ハンドオフ番号に対してコールが発信されます。Dial-via-office が実行されると、追加の不要なコール レッグが作成されて、元のコールのハンドオフに失敗する可能性があります。

同様に、管理者が個々の Unified Mobile Communicator ユーザにクライアント内で独自の Dial-via-office 設定を行うことを許可している場合、ユーザはクライアントを設定して、携帯電話インターフェイス経由でコールの発信が試みられるたびに、直接コールを発信するか、または Dial-via-office を使用して発信するかを選択できるようにできます。Unified Mobile Communicator の [When dialing] 設定を [Let me choose] に設定し、[Allow dial via office for] 設定を [Call from this app] に設定することによって、ユーザは、Dial-via-office が使用されるタイミングについて、各自の意思を最大限反映できます。いずれの場合でも、ユーザは、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合にだけ Dial-via-office を使用する必要があります。

Cisco Unified Mobile Communicator のソリューション、機能セット、および設計と配置の考慮事項の詳細については、「デュアルモードの電話機とクライアント」（P.25-64）を参照してください。

Unified Mobility の統合

コール ログ統合と Dial-via-office のための Unified CM との統合に加えて、Unified Mobile Communicator ユーザは、Unified Mobility と統合してモバイル コネクトを利用できます。これによって、ユーザの会社の電話番号への着信コールを携帯電話に転送できるようになります。Cisco Unified Mobile Communicator クライアントと Unified Mobility の統合は、Unified CM 内で Cisco Unified Mobile Communicator デバイスに直接関連付けられた設定済みのモビリティ ID を経由して実現されます。Unified CM 内のモビリティ ID の設定は、リモート接続先と同じです。また、リモート接続先番号と発信者 ID の照合の設定に関するガイドライン（「リモート接続先の設定と発信者 ID の照合」（P.25-54）を参照）がすべて、モビリティ ID の設定にも適用されます。Unified Mobile Communicator クライアント インターフェイス内でユーザは、[General] 設定メニューで [Moblie Connect (Single Number Reach)] を有効または無効にできます。

Cisco Unified Presence

Unified Mobile Communicator ユーザが企業ネットワークに対して自分のプレゼンス ステータスや利用可能性を更新できるように、Unified Mobility Advantage サーバと Cisco Unified Presence を統合できます。同様に、Unified Mobile Communicator クライアントは、ユーザのバディ リスト、ディレクトリ リスト、コンタクト リスト、ボイスメール メッセージ リスト、およびコール履歴ログ内で他の社内クライアントに関するプレゼンス情報を受信します。プレゼンス ステータスとバディ リストは、Unified Mobile Communicator クライアントとユーザの Cisco Unified Personal Communicator クライアントの間で同期化されます。Unified Mobile Communicator ユーザは、クライアント上で自分の利用可能性を調整したり、Microsoft Exchange パーソナル カレンダーの利用可能性とデスクトップフォンの回線状態に基づく利用可能性の自動更新を利用できます。図 25-30 に示すように、Cisco Unified Presence との統合は、Unified Mobility Advantage サーバと Cisco Unified Presence サーバ間の SIP/SIMPLE 接続を通して実現されます。

（注）　Cisco Mobile、つまり iPhone 対応の Unified Mobile Communicator クライアントには、プレゼンス ステータスは表示されず、プレゼンス ステータスのアップデートの送受信もサポートされていません。

Cisco Unity と Unity Connection ボイスメール

Unified Mobility Advantage サーバを Cisco Unity（Unified Messaging または Integrated Messaging モード）および Cisco Unity Connection ボイスメール システムに統合することにより、Unified Mobile Communicator クライアントにユーザの会社のボイスメール ボックスに関する Message Waiting Indication（MWI; メッセージ待機インジケータ）を提供できます。この統合によって、ユーザは、モバイル デバイスを使用して視覚的にボイスメール ボックスをナビゲートすることもできます。ボイスメール ボックス内のすべてのメッセージのリストをナビゲートできます。このリストには次の情報が含まれています。

- メッセージが残された時間
- メッセージ長
- メッセージを残した人物の発信者 ID または名前（可能な場合）
- メッセージの優先順位指定
- メッセージを残した人物の現在のプレゼンスまたは利用可能性の指定（その人物が会社のプレゼンス インフラストラクチャにプレゼンス ステータスを提供している場合）

ユーザがリストからメッセージを選択すると、Unified Mobile Communicator クライアントによってデータ接続を通してメッセージがダウンロードされます。ユーザは、ボイスメール システム上でそのメッセージを再生して、削除または保存できます。Cisco Unified Mobile Communicator クライアントによるボイスメール メッセージのステータスに対する変更（メッセージに対する再生済みのマーキングやメッセージの削除など）は、ボイスメール システムに伝播され、ユーザのデスクトップフォンと Cisco Unified Personal Communicator などのその他のクライアントに適切に反映されます。ボイスメール メッセージは任意の順序でナビゲートできます。図 25-30 に示すように、Unified Mobility Advantage サーバと Cisco Unity または Unity Connection は IMAP プロトコルを使用して統合されます。

Cisco Unified MeetingPlace

Unified Mobile Communicator ユーザが MeetingPlace 会議の開催通知または招待を受信できるように、Unified Mobility Advantage サーバと Cisco Unified MeetingPlace を統合できます。この会議通知には、会議の議題、日時、ダイヤルイン番号、および会議 ID が含まれています。ユーザは、ダイヤルイン番号をクリックすれば呼び出すことができます。

（注）　クリックツージョインは、Cisco Mobile、つまり iPhone および Blackberry 対応の Cisco Unified Mobile Communicator だけでサポートされています。その他すべての Cisco Unified Mobile Communicator クライアントについては、コールが接続された後、ユーザが手動で会議 ID を入力する必要があります。

Cisco Unified MeetingPlace との統合は、Unified Mobility Advantage サーバから会議システムで使用されている Microsoft Exchange サーバへの直接接続を経由して実現されます。図 25-30 に示すように、この接続では、Web-based Distributed Authoring and Versioning（WebDAV）プロトコルが使用されます。

Cisco Unified Mobile Communicator クライアント（Cisco Mobile を含む）で会議通知を受信するには、システム管理者は Cisco Unified MeetingPlace 会議通知電子メール テンプレートを変更して、各会議通知に **cump://** のプレフィックスが付いたリンクを含める必要があります。Cisco Unified Mobility Advantage サーバでは、ユーザの Exchange メールボックス内に含まれるすべての会議通知でこのリンクが検索されます。会議通知にこのリンクが含まれていない場合、会議の通知はクライアント

で受信されず、表示もされません。Cisco Unified MeetingPlace 会議通知電子メール テンプレートで必要な変更の詳細については、次の Web サイトで入手可能な『*Configuring Features in Cisco Unified Mobility Advantage: Meeting Features*』を参照してください。

http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html

MeetingPlace との統合により、会議通知がサポートされるだけでなく、パスワードや会議 ID の入力を必要としない会議へのクリックツージョインも可能です。図 25-30 のとおり、このクリックツージョイン機能は、MeetingPlace サーバの Web Services API への SOAP コールによって実施されます。

（注）　クリックツージョインは、Cisco Mobile、つまり iPhone および Blackberry 対応の Unified Mobile Communicator クライアントだけでサポートされています。

Cisco WebEx によって Cisco Unified MeetingPlace 会議の Web 共有機能が提供される配置においては、iPhone Cisco Mobile クライアントは、iPhone で Cisco WebEx Meeting Center アプリケーションを相互に起動します（このアプリケーションがデバイスにインストール済みであることが前提です）。この相互起動が動作するには、Cisco Unified MeetingPlace システムが Cisco WebEx と正常に統合されている必要があります。

Microsoft Exchange

Cisco Unified MeetingPlace の会議統合に関する Microsoft Exchange との通信に加えて、Cisco Unified Mobility Advantage サーバと Microsoft Exchange を WebDAV 経由で統合すれば、Exchange に保存されたユーザの個人的なコンタクト リストの維持管理が容易になります。Exchange との統合によって、ユーザのプレゼンス ステータスを Exchange カレンダーの利用可能性に基づいて自動的に更新することもできます。Microsoft Exchange はオプションのコンポーネントであり、会議通知、個人的なコンタクト リスト、またはカレンダー統合が必要である場合にだけ必要です。

安全なテキスト メッセージング

前述したアプリケーションと機能の統合に加えて、Unified Mobile Communicator ユーザは、Unified Mobile Communicator クライアントを使用している他のユーザに安全なテキスト メッセージを送信することもできます。このメッセージ交換は、Cisco Unified Mobility Advantage サーバ内でネイティブに実施されます。これらのメッセージは、モバイル データ接続を使用して交換されるため、SMS プロバイダーの利用料がかかります。

（注）　Cisco Mobile、つまり iPhone 対応の Unified Mobile Communicator クライアントでは、Cisco Unified Mobility Advantage サーバを使用した安全なテキスト メッセージングをサポートしていません。

Cisco Unified Mobile Communicator のハイ アベイラビリティ

Cisco Unified Mobile Communicator クライアントは、アプリケーションの相互作用と機能を Cisco Unified Mobility Advantage Server にバックホールされるモバイル データ ネットワーク上のデータ接続に完全に依存しています。このデータ接続が、モバイル データ ネットワーク内の障害、モバイル データ ネットワークとの接続切断、または ASA TLS プロキシや BES サーバ、Cisco Unified Mobility Advantage サーバの故障が原因で失われた場合は、企業アプリケーションにアクセスできなくなります。この種の障害が発生した場合、ユーザは、Unified Mobile Communicator にアクセスしてさまざまなアプリケーション統合を利用できなくなります。たとえば、ディレクトリ ルックアップの実行、他

のクライアントへのテキスト メッセージの送信、ビジュアル ボイスメールへのアクセス、個人連絡先へのアクセス、メッセージ待機インジケータの受信、会議通知の受信、バディ リストとプレゼンス情報の更新または同期化、Dial-via-office 機能を使用した発信などができなくなります。

（注）　Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage 間のデータ接続または Cisco Unified Mobility Advantage と Cisco Unified CM 間の接続に障害がある場合、クライアントは、Dial-via-office が強制されていても、直接通話に戻ります。

会社へのデータ接続が使用できない場合は、Unified Mobile Communicator から提供される機能を利用できなくなりますが、モバイル ボイス ネットワークを使用してモバイル デバイスで電話をかけたり、電話に出ることができます。加えて、Unified CM 上でユーザと携帯電話が Unified Mobility に統合されている場合は、モバイル コネクト機能だけでなく、モバイル ボイス アクセスやエンタープライズ機能アクセスなどの機能も使用できます。

Cisco Unified Presence、Cisco Unified CM、Cisco Unity および Unity Connection などの企業アプリケーションに不具合がある場合は、構成によりそれらのアプリケーションの特性に応じて特定の機能が利用できなくなります。ただし、ほとんどの場合、Unified Mobility Advantage サーバ内に複数のアダプタを設定できますし、さまざまなアプリケーションに対する冗長性が提供されていれば、アプリケーションまたはアプリケーション サーバに障害が発生しても機能性を維持できます。

Cisco Unified Mobile Communicator のキャパシティ プランニング

Cisco Unified Mobility Advantage サーバでは、次のユーザの容量をサポートしています。

- Cisco MCS 7845-H2/I2 では、最大 1,000 台の Unified Mobile Communicator クライアントをサポートする。
- Cisco MCS 7825-H4/I4 では、最大 500 台の Unified Mobile Communicator クライアントをサポートする。
- Cisco MCS 7825-H2/I2 または 7825-H3/I3 では、最大 250 台の Unified Mobile Communicator クライアントをサポートする。

1 箇所で 1,000 人を超える Unified Mobile Communicator ユーザをサポートするには、追加の Unified Mobility Advantage サーバをインストールする必要があります。ただし、1 台の Cisco Unified Mobility Advantage サーバに関連付けるように設定された Unified Mobile Communicator クライアントは、別のサーバ上のクライアントにテキスト メッセージを送信できません。

エンタープライズ コール ログ統合のために Unified Mobile Communicator と Cisco Unified CM を統合した場合は、Unified Mobility Advantage サーバと Unified CM CTIManager が連携してデスクトップフォンの回線をモニタします。コール ログ統合が有効にされた Unified Mobile Communicator ごとに、Cisco Unified Mobility Advantage サーバが CTIManager への CTI 接続を確立します。そのため、すべてのユーザに対してコール ログ統合が有効にされた MCS 7845 を実行しているフル実装の Unified Mobility Advantage サーバと一緒に Unified Mobile Communicator を配置した場合は、1,000 個の CTI 接続が消費されます。この理由から、Unified Mobile Communicator とコール ログ統合を配置する際は、次に示す CTI 接続に対するクラスタ全体の制限に関して、必要な CTI 接続の数を検討する必要があります。

- MCS 7845-I3 または同等 OVA サーバを使用する場合は、Unified CM クラスタごとに 40,000 個の CTI 接続。
- Cisco MCS 7845-H2/I2 または同等 OVA サーバを使用する場合は、Unified CM クラスタごとに 20,000 個の CTI 接続。
- Cisco MCS 7835-H3/I3 または同等 OVA サーバを使用する場合は、Unified CM クラスタごとに 10,000 個の CTI 接続。

- Cisco MCS 7835-H2/I2 サーバを使用する場合は、Unified CM クラスタごとに 8,000 個の CTI 接続
- Cisco MCS 7825-H5/I5 または同等 OVA サーバを使用する場合は、Unified CM クラスタごとに 4,000 個の CTI 接続。
- 現在サポートされているその他すべての Cisco MCS 7825 および MCS 7835 サーバを使用する場合は、Unified CM クラスタごとに 3,600 個の CTI 接続。

他のアプリケーション用の CTI 接続が必要な場合は、コール ログ統合を有効にする Unified Mobile Communicator ユーザの容量を制限できます。

Dial-via-office と Unified Mobility 機能のための Unified Mobile Communicator と Unified CM の統合では、各 Unified Mobile Communicator を Unified CM デバイスとして設定し、携帯の番号をモビリティ ID として設定する必要があります。したがって、これらの統合を実施する場合は、Unified CM 電話機とモビリティ対応ユーザの機能全体を検証する必要もあります。

Cisco Unified Mobile Communicator の設計上の考慮事項

Cisco Unified Mobile Communicator を配置する際は、次の設計上の考慮事項に従ってください。

- Cisco Unified Mobility Advantage サーバはすべての企業サービスおよびアプリケーションの統合ポイントであるため、セキュリティ上の理由から、このサーバは企業ファイアウォールの後ろに配置する必要があります。
- Cisco Adaptive Security Appliance（ASA）は、Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage サーバとの通信用のプロキシ サーバとして機能するため、企業 DMZ には ASA を配置する必要があります。
- 認証局から SSL 認証を取得する必要があります。この認証は、Cisco Unified Mobile Communicator クライアントと Cisco Unified Mobility Advantage サーバ間に流れるデータの暗号化を有効にするために必要です。
- 携帯電話にはルート認証のインポートに関する機能制限があるため、SSL 認証は、VeriSign または GeoTrust などの有名な認証局から取得する必要があります。VeriSign や GeoTrust からのルート認証は通常、ほとんどのモバイル ハンドセットで利用できます。
- 社内ファイアウォールのファイアウォール ポートを開いて、インターネット上の Cisco Unified Mobile Communicator クライアントから DMZ 内の ASA、および DMZ 内の ASA から社内の Cisco Unified Mobility Advantage サーバに接続できるようにする必要があります。次のファイアウォール ポートを開く必要があります。
  - クライアント接続ポート（SSL）: 5400 ～ 5500 の範囲の 1 つの TCP ポート（デフォルト ポートは 5443）
  - プロビジョニング ポート（HTTP）: 9000 ～ 9100 の範囲の 1 つの TCP ポート（デフォルト ポートは 9080）

（注） iPhone または Blackberry ハンドセットだけを配置している場合、これらのハンドセットはプロビジョニング ポートを介して Cisco Unified Mobile Communicator クライアントをダウンロードしないため、ファイアウォールのプロビジョニング ポートを開く必要はありません。このクライアントは、iPhone ハンドセットの場合は Apple App Store からダウンロードされ、Blackberry ハンドセットの場合は Blackberry Enterprise Server（BES）を介してハンドセットにプッシュされます。

- Cisco Unified Mobile Communicator ユーザを認証するため、Microsoft Active Directory が必要です。すべての Cisco Unified Mobile Communicator ユーザは Microsoft Active Directory 内に有効なアカウントを持つ必要があります。そうしないと、認証に失敗し、このソリューションが提供する機能やサービスを利用できません。
- 常に、適切なバックエンド企業アプリケーション サーバが配置され、必要な Cisco Unified Mobile Communicator ソリューション機能に基づいて適切に設定されていることを確認します。サポートされている機能および必要なバックエンド アプリケーション サーバの全リストについては、次の Web サイトで入手可能な『*Compatibility Matrix for Cisco Unified Mobility Advantage and Cisco Unified Mobile Communicator*』を参照してください。

  http://www.cisco.com/en/US/products/ps7270/products_device_support_tables_list.html
- Blackberry 対応の Unified Mobile Communicator クライアントである Cisco Mobile を配置する場合、Blackberry Enterprise Server（BES）および Mobile Data Services（MDS）も配置して、これを Unified Mobility Advantage サーバに直接統合する必要があります。Blackberry デバイス上の Cisco Mobile クライアントは、会社の ASA には接続せず、セキュアな Research In Motion（RIM）モバイル Network Operations Center（NOC; ネットワーク オペレーション センター）および NOC から会社の BES サーバへのセキュア接続を使用して Unified Mobility Advantage サーバに接続します。
- Nokia Call Connect デュアルモード クライアントと Cisco Unified Mobile Communicator Nokia クライアントの両方が同じハンドセットに配置されている状況においては、デュアルモード デバイスが社内にあり、Unified CM に登録されている場合に Dial-via-office を使用しないでください。次のことを推奨します。
  - 企業にデュアルモード電話機を配置する場合、Cisco Unified Mobility Advantage Server の管理者は、[Dial Via Office Policy] 設定を使用して Dial-via-office の使用を強制しないでください。代わりに、Dial-via-office を使用するかどうかをユーザが選択できるようにする必要があります。
  - Cisco Unified Mobility Advantage サーバの管理者によって Cisco Unified Mobile Communicator における Dial-via-office の使用が強制されている場合、ユーザは Unified Mobile Communicator クライアント内で [Allow dial via office for] 設定を [Call from this app] に設定して、Unified Mobile Communicator クライアント内から直接発信されたコールでだけ Dial-via-office の呼び出しが試みられるようにする必要があります。クライアントをこのように設定することによって、ユーザは、予期せず Dial-via-office が実行されないようにできます。Unified Mobile Communicator クライアントがフォアグラウンドで実行されていない場合、Dial-via-office は呼び出されません。
  - Unified Mobility Advantage の管理者によって Dial-via-office の使用が強制されていない場合、Unified Mobile Communicator ユーザは、[When dialing] 設定を [Let me choose] に、[Allow dial via office for] 設定を [Call from this app] に設定する必要があります。このように設定することによって、ユーザは、Dial-via-office が使用されるタイミングについて、各自の意思を最大限反映できます。いずれの場合でも、ユーザは、Nokia デュアルモード デバイスが社外にあり、Unified CM に登録されていない場合にだけ Dial-via-office を使用する必要があります。

ダイレクト コネクト モバイル クライアント

ダイレクト コネクト モバイル クライアントは、モバイル ユーザが携帯電話から Cisco Unified Communications アプリケーションにアクセスし、利用することを可能にするソリューションを提供します。Cisco Unified Mobile Communicator ソリューションと同様に、モバイル スマート フォンで動作するダイレクト コネクト クライアント アプリケーションは、企業内の 1 つまたは複数のアプリケーション サーバと連動して動作し、企業のボイスおよびコラボレーション アプリケーションにアクセスして利用するための高度なユーザ インターフェイスを提供します。ただし、Cisco Unified Mobile Communicator ソリューションとは異なり、ダイレクト コネクト モバイル クライアントは、Cisco

Unified Mobility Advantage などの中間サーバを介さずにバックエンド アプリケーション サーバと直接通信するので、「ダイレクト コネクト」と呼ばれます。ダイレクト コネクト モバイル クライアントは、各種のバックエンド企業アプリケーション サーバに備わっているスケーラビリティと信頼性を利用します。

ダイレクト コネクト モバイル クライアントは、コラボレーション アプリケーションにアクセスし、使用する機能を提供するばかりでなく、コールの発信および受信に Voice over WLAN（VoWLAN）機能も利用できるので、デュアルモード機能が実現します。Dial-via-office 操作と Voice over WLAN コールの両方をサポートする企業は、携帯電話ネットワークの音声トラフィックを企業データ ネットワークにオフロードしたり、市内通話やフリーダイヤル システムのアクセス番号を利用して会社経由の低コストのコール ルーティングを実現したりすることで、モバイル コールのコストを大幅に削減できます。

ここでは、ダイレクト コネクト モバイル クライアントのアーキテクチャと、Dial-via-office や XMPP ベースの IM およびプレゼンスなど、これらのクライアントが提供する共通の機能について説明します。この項では、一般的なダイレクト コネクト モバイル クライアントのアーキテクチャおよび機能について説明した後、Cisco Mobile 8.5 for Nokia ダイレクト コネクト モバイル クライアントのさまざまな機能および統合に関する考慮事項について説明します。

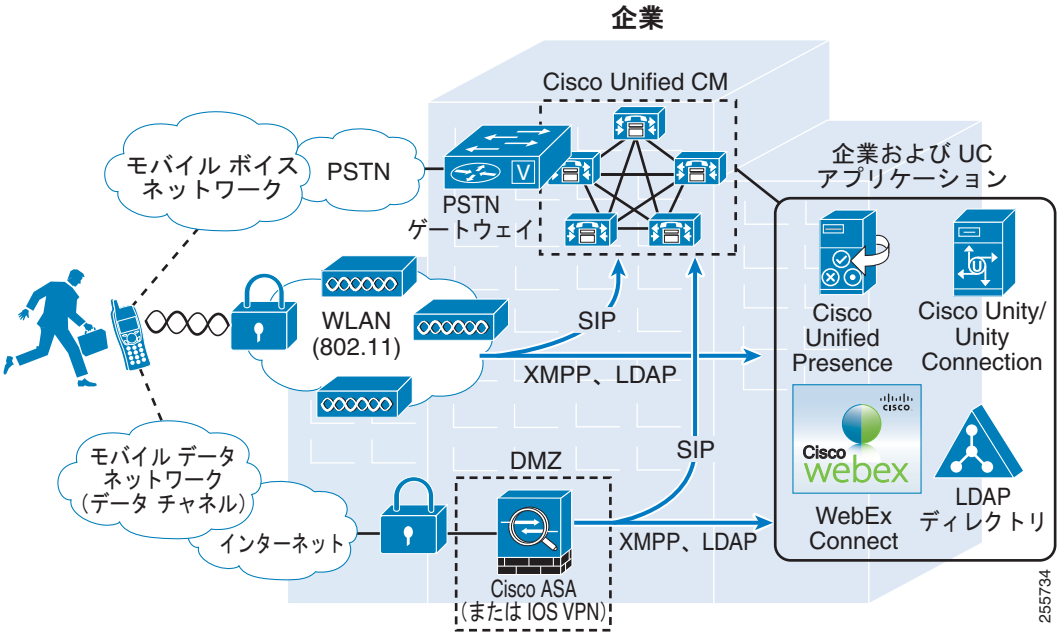
また、ダイレクト コネクト モバイル クライアントのハイ アベイラビリティおよびキャパシティ プランニングの考慮事項についても説明します。

ダイレクト コネクト モバイル クライアントのアーキテクチャ

ダイレクト コネクト モバイル クライアントは、会社へのリモート データ接続と IEEE 802.11 標準を使用した Wireless Local Area Network（WLAN）経由のオンプレミス データ接続の両方を可能にします。さらに音声接続も、モバイル ボイス ネットワークおよび公衆網経由または企業の WLAN インフラストラクチャ経由で有効になります。

図 25-33 は、モバイル スマート フォン デバイスを Cisco Unified Communications System に接続するための基本的なダイレクト コネクト ソリューション アーキテクチャを示しています。ダイレクト コネクト モバイル クライアントを使用すると、モバイル データ ネットワークを介してモバイル デバイスから企業に接続し、Cisco Unified CM、LDAP 社内ディレクトリ、および Cisco Unified Presence などのバックエンド アプリケーション サーバと通信することができます。さらに、モバイル デバイスがデュアルモード デバイスであれば、WLAN 経由で企業内部の同一のバックエンド アプリケーションおよびサービスに接続できます。

図 25-33　ダイレクト コネクト モバイル クライアントのアーキテクチャ



ダイレクトコネクト クライアントは会社の電話機として、モバイル データ接続を介してリモートから、または企業の WLAN に関連付けてローカルに、Cisco Unified CM に登録されます。登録されたダイレクト コネクト クライアントは、エンタープライズ テレフォニー インフラストラクチャを利用して、音声パスがモバイル ボイス ネットワークまたは公衆網を経由している場合は Dial-via-office を介して、または VoWLAN を介してコールを発信および受信します。また、保留、転送、会議などの付加的なコール機能を提供するため、およびモバイル コネクトを有効または無効にするために SIP（および場合によっては SCCP）シグナリングも利用できます。企業の WLAN 接続およびモバイル ボイス ネットワークを介した会社へのリモート データ接続が利用できない場合、携帯電話はモバイル ボイス ネットワークを利用してコールを発信および受信します。また、この場合、通話中の付加機能は、モバイル ボイス ネットワークおよび公衆網経由で DTMF 機能アクセス コードのみにより呼び出すことができます。

ダイレクト コネクト クライアント デバイスが企業の WLAN に関連付けられている場合、そのデバイスにはユーザの会社の電話番号を通じて到達できます。ユーザの会社の電話番号に着信コールがあると、WLAN に接続したデバイスの呼出音が鳴ります。ユーザが Cisco デスクトップ IP Phone を持っている場合は、ダイレクト コネクト クライアントを登録すると、ユーザの会社の番号でシェアド ライン インスタンスが使用可能になり、コールが着信すると、ユーザのデスクトップフォンと携帯電話の両方の呼出音が鳴ります。企業の WLAN に関連付けられていない場合や、モバイル データ ネットワーク経由でリモート接続されていない場合、クライアント デバイスは未登録となります。この場合、ユーザに対して Unified Mobility が有効になっており、携帯の番号でモバイル コネクト（またはシングル ナンバー リーチ）がオンになっているときに限り、ビジネス コールを受信できます。

同様に、ダイレクト コネクト クライアントを利用すると、リモート接続しているときはモバイル データ ネットワーク、ローカル接続しているときは企業の WLAN を使用して、XMPP 経由で IM およびプレゼンス サービスにアクセスしたり、LDAP 経由でディレクトリ サービスにアクセスすることができます。

ネットワーク接続：WLAN および VPN

ダイレクト コネクト モバイル クライアントは、WLAN およびモバイル データ ネットワークの両方を使用した企業ネットワークへの接続に対応します。モバイル データ ネットワーク経由で企業ネットワークに接続するには、通常、VPN セキュア接続が必要です。これらのクライアントに対してこのネットワーク接続を有効にするには、会社が利用を計画している接続方式に応じて、適切な WLAN、VPN、またはその両方のインフラストラクチャを装備することが重要です。

WLAN インフラストラクチャ

WLAN をネットワーク接続に利用する場合、適切に調整され、QoS に対応し、高い可用性を備えた WLAN ネットワークを展開することが不可欠です。ダイレクト コネクト モバイル クライアントは、基礎となる WLAN インフラストラクチャに全体的または部分的に依存して重要なシグナリングとリアルタイム音声メディア トラフィックの両方、および各種アプリケーションにアクセスするためのデータ トラフィックを伝送するため、データ トラフィックとリアルタイム音声トラフィックの両方に対して最適化された WLAN ネットワークを展開する必要があります。WLAN ネットワークの展開が適切でないと、多くの干渉が発生し、容量が低下するため、音声品質が低下するだけでなく、コールがドロップされたり、つながらなかったりする可能性もあります。このように配置された WLAN は、音声コールの発信および受信に使用できなくなります。したがって、展開されたダイレクト コネクト モバイル クライアントに WLAN 接続を利用する場合は、Voice over WLAN（VoWLAN）の展開が正常に行われるように、展開前、展開中、展開後に WLAN Radio Frequency（RF; 無線周波数）実地調査を実施して、適切なセル境界、設定、機能設定、容量、および冗長性を判断する必要があります。他の WLAN 対応クライアントと同様に、実稼動環境への展開の前に、WLAN の展開に対して各携帯電話機やクライアントをテストして、統合および動作が適切に行われるようにする必要があります。サービス品質を含む最適な VoWLAN サービス（Cisco Unified Wireless Network など）が提供されるように展開および設定された WLAN を使用することによって、ダイレクトコネクト電話機を正常に展開できます。

Voice over WLAN 配置およびデバイスのローミングの詳細については、「ワイヤレス デバイスのローミング」（P.25-6）を参照してください。

VPN インフラストラクチャ

モバイル データ ネットワークを介した接続に VPN ネットワーク接続を利用する場合は、企業のセキュリティ要件およびポリシーに沿った広帯域でセキュアな VPN インフラストラクチャを展開することが重要です。この接続を利用するユーザおよびデバイスの数に基づいた広帯域幅、信頼性の高い接続、および適切なセッションまたは接続容量をこの VPN インフラストラクチャで提供できるよう、慎重に計画することが必要です。

VPN 接続のタイプと方式はさまざまで、Cisco IOS VPN または Cisco Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）を利用する標準ベースの IPSec から、Cisco ASA を利用する Cisco AnyConnect まで各種のオプションがあります（図 25-33 を参照）。使用する VPN 方式のタイプは、多くの場合、展開するモバイル デバイスによって異なります。

セキュアなリモート VPN 接続ソリューションの詳細については、次の Web サイトで入手可能なセキュア モビリティのマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/products.html#mobi

（注）　ダイレクト コネクト クライアントおよびそれらのクライアントが動作するデバイスは、パブリックおよびプライベートの WLAN アクセス ポイントまたはホット スポットに接続し、インターネット経由で会社に接続して呼制御やその他の Unified Communications サービスを利用できますが、このように接続した場合の音声品質は保証されません。WLAN 経由でクライアントに接続して VoIP を利用するには、エンタープライズ クラスの音声に最適化された WLAN ネットワークを推奨します。ほとんどのパブリックまたはプライベートの WLAN AP およびホット スポットは、データ アプリケーションおよびデバイスに合せて調整されています。ほとんどの場合、クライアントの容量がより大きくなるよう

に、AP 無線機は最大パワーに調整され、動的パワー クライアントはネットワーク接続上の最大パワーに合せて調整されます。このような調整方法は、パケットのドロップや損失時に再送信ができるデータ アプリケーションにとっては理想的ですが、パケットのドロップが大量に発生する可能性があるため、音声アプリケーションでは音声品質が非常に悪くなる可能性があります。

ダイレクト コネクト モバイル クライアントの機能

ダイレクト コネクト モバイル クライアントには、さまざまな機能が用意されています。サポートされている機能および操作はクライアントごとに異なりますが、ここで説明する機能や動作はすべてのダイレクト コネクト モバイル クライアントに適用されます。

コール ルーティング

ダイレクト コネクト モバイル クライアントは、企業の電話インフラストラクチャを使用してコールを発信および受信できるので、ダイレクト コネクト モバイル クライアントの動作に関係しているコール ルーティングの特性を理解することが大切です。

着信コール ルーティング

ダイレクト コネクト モバイル クライアントを Unified CM に登録すると、Dial-via-office と VoWLAN コールの両方を利用できますが、ネットワーク接続によって着信コール ルーティングの動作がわずかに異なります。クライアントが WLAN 経由で Unified CM に接続および登録されている場合、そのクライアントは、登録されている IP デスクトップフォンのように（発信が社内か公衆網からかに関係なく）会社の番号への着信コールを受信します。ユーザがデスクトップ フォンを所有している場合、着信コールによってモバイル クライアントとデスクトップフォンの両方のシェアド ラインが呼び出されます。一方、クライアントが WLAN ネットワークに接続しておらず、モバイル データ接続を介した VPN 経由で接続しているか、またはまったく接続していない場合は、ユーザに対して Cisco Unified Mobility が有効になっており、ユーザのダイレクト コネクト クライアント デバイスの携帯の番号でモバイル コネクト（シングル ナンバー リーチ）が有効であるときに、会社の番号に着信コールがあると（発信元が社内か公衆網からかに関係なく）、デバイスの携帯の番号が呼び出されます。デュアルモード クライアント デバイスと同様に、クライアント デバイスが WLAN ネットワークに接続し、Unified CM に登録されている場合、会社の番号への着信コールがモバイル コネクトを介してダイレクト コネクト クライアント デバイスの携帯の番号に転送されることはありません。

いずれの場合も、ダイレクト コネクト クライアント デバイスの携帯電話番号に対して直接発信された着信コールは、プロバイダー ネットワークやデバイスの設定でモバイル ネットワーク経由でデバイスにコールが転送されないように設定されている場合を除き、モバイル ネットワークでデバイスに直接ルーティングされます。このようなコールは、ユーザの会社の電話番号に対して発信されたコールではないため、適切な動作です。これらのコールは個人的なコールであると見なされるため、会社経由でルーティングされません。

発信コール ルーティング

ダイレクト コネクト モバイル クライアント デバイスのネットワーク接続の特性により、発信コールのルーティング動作はわずかに異なります。デバイスが企業の WLAN に接続し、Unified CM に登録されている場合、発信コールは社内番号宛てか、社外の公衆網番号宛てかにかかわらず、Unified CM 内のダイヤル プラン設定に基づきエンタープライズ テレフォニー インフラストラクチャによってルーティングされます。デバイスがモバイル データ ネットワークを介して会社に接続されている場合、発信コールのルーティングは、Unified CM 内の Dial-via-office 機能によって実施されます。この場合、コール シグナリングは会社へのモバイル データ接続を通過し、音声メディアはモバイル ボイス ネットワークおよび公衆網を通過します。企業接続が使用できない場合、会社の番号からコールを発信することはできず、代わりにダイレクト コネクト クライアント デバイスの携帯の番号を利用してモバイル ボ

イス ネットワーク経由でコールを発信する必要があります。または、Cisco Unified Mobility に装備されている 2 ステージ ダイヤリング機能を利用することもできます（「モバイル ボイス アクセスとエンタープライズ機能アクセス」（P.25-48）を参照）。

ダイヤル プラン

Dial-via-office および VoWLAN コールの使用により、ダイレクト コネクト モバイル クライアントでは、内線用の短縮ダイヤルや公衆網およびサイト間の振り分け用数字を利用したダイヤリングを含む企業のダイヤリング方式を使用して、発信コールをダイヤルできます。ただし、企業接続がないために Dial-via-office 機能や VoWLAN コールを使用できない場合には、企業のダイヤリング方式を使用できず、ユーザはモバイル ボイス ネットワークおよび公衆網で必要とされる完全長の E.164 番号ダイヤリングを使用して発信コールをダイヤルする必要があります。

企業のダイヤリングでは便利な短縮ダイヤルを利用できますが、企業のダイヤリングと公衆網またはモバイル ボイス ネットワーク ダイヤリングでは異なるため、ユーザが会社に接続しているかどうかに関係なく同じ番号をダイヤルして着信側接続先に到達できるよう、必要なダイヤリング パターンを正規化することが推奨されます。ダイレクト コネクト モバイル クライアントのユーザ用に Unified CM 内でダイヤル プランとダイヤリング動作を正規化することにより、管理者は、クライアント デバイスが会社に接続し、Unified CM に登録されているかどうかをユーザが気にする必要のない、最善のエンドユーザ ダイヤリング エクスペリエンスを提供できます。

モバイル クライアントのダイヤル プランの正規化の詳細については、デュアルモードの電話機とクライアントに関する「ダイヤル プラン」（P.25-68）を参照してください。

発信者 ID

ダイレクト コネクト モバイル クライアント デバイスが（モバイル データ ネットワークまたは企業の WLAN を介して）会社に接続し、Unified CM に登録している場合、Dial-via-office または WLAN を利用して発信されたすべてのコールは、ユーザの会社の電話番号を発信者 ID とした状態でルーティングされます。これにより、遠端でコール履歴リストから発信される返信コールはユーザの会社の番号に対して発信されることになり、常に会社経由でルーティングされます。ダイレクト コネクト モバイル クライアントのユーザに対して Cisco Unified Mobility が有効になっており、ダイレクト コネクト クライアント デバイスの携帯の番号でモバイル コネクトがオンになっている場合、WLAN 接続がないと、会社の番号への返信コールも公衆網経由でダイレクト コネクト モバイル クライアント デバイスに転送されます。

通話切替機能

次に示すように、ダイレクト コネクト モバイル クライアントには、アクティブなビジネス コールの最中に、付加サービスや保留、再開、転送、および会議などの通話切替機能を呼び出すための一般的な 3 つの方法があります。

- WLAN 経由の SIP または SCCP シグナリング

  WLAN に接続され、Unified CM に登録されている場合、ユーザがコール中メニュー ソフトキーを押すと、クライアントでサポートされているシグナリング プロトコルを使用する IP デスクトップフォンと同様に、ダイレクト コネクト モバイル クライアントは通話切替機能の信号を送信できます。

- モバイル データ接続を介した SIP モバイル拡張

  モバイル データ接続を介して会社に接続している場合、ユーザがコール中メニュー ソフトキーを押すと、ダイレクト コネクト モバイル クライアントは Unified CM へのデータ接続を介した SIP モバイル拡張コールを利用して、通話切替機能の信号を送信できます。これらの通話切替機能は、Dial-via-office および会社の固定モビリティ コール（モバイル コネクトやシングル ナンバー リーチ コールなど）に対してのみ呼び出すことができます。

- フォールバック方式としての DTMF 機能アクセス コード

  企業接続を使用できない場合、ダイレクト コネクト モバイル クライアントのユーザは、Cisco Unified Mobility DTMF 機能アクセス コードを使用して手動で通話切替機能を呼び出すことができます。この通話切替機能方式を使用するには、コールが会社の固定モビリティ コール（モバイル コネクト、シングル ナンバー リーチ、または 2 ステージ ダイヤリング対象コールなど）であることが必要です。Unified Mobility 通話切替機能の詳細については、「通話切替機能」（P.25-42）を参照してください。

緊急サービス

他のモビリティ クライアント ソリューションと同様に、ダイレクト コネクト モバイル クライアントから 911、999、および 112 などの公共サービス番号への緊急コールを発信すると問題が生じます。ダイレクト コネクト モバイル クライアント デバイスは社内にある可能性も、社外にある可能性もあるので、緊急時における位置の通知について考慮する必要があります。携帯電話はすでにプロバイダー ネットワークの位置サービスを利用しています。これらの位置サービスは常に利用可能であり、通常は企業ワイヤレス ネットワークよりもはるかに正確に位置を特定できるため、緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。ダイレクト コネクト モバイル クライアント デバイスが緊急サービスおよび位置サービスにモバイル ボイス ネットワークのみを利用するよう、Unified CM は、ダイレクト コネクト クライアント デバイス設定ページの [Emergency Numbers] フィールドに設定された番号に対するすべてのコールを強制的にモバイル ボイス ネットワーク経由でルーティングします。デフォルトでは、緊急番号 911、999、および 112 が [Emergency Numbers] フィールドに設定されます。

外部コール ルーティング

ダイレクト コネクト モバイル クライアント デバイスが社外にあり、企業接続が存在しない場合は、モバイル ボイス ネットワーク経由でのみコールの発信と受信を行うことができます。このようにモバイル ボイス ネットワーク経由で直接ダイヤルされるコールは、会社に固定されていないので、Unified CM からは認識できません。そのため、これらのコールに対しては、会社の通話切替機能を呼び出したり、デスクトップフォンのピックアップを行ったりすることはできません。このような状況では、システム管理者が利用可能に設定している場合、ユーザは Unified Mobility エンタープライズ機能アクセスまたはモバイル ボイス アクセス 2 ステージ ダイヤリング機能を利用してコールを会社に固定できます。

Dial-via-office

Dial-via-office 機能を利用すると、ダイレクト コネクト モバイル クライアントには、携帯電話から Cisco Unified CM テレフォニー インフラストラクチャおよび会社の公衆網ゲートウェイを使用してコールを発信する機能が備わります。この機能は、ダイレクト コネクト モバイル クライアントと Unified CM との間のモバイル データ ネットワーク接続を介した SIP シグナリングによって実施されます。Unified CM システム管理者が Dial-via-office の使用を強制することも、管理者がユーザに対して、Dial-via-office を使用するか、モバイル ボイス ネットワーク経由でコールを直接ダイヤルするかを決定させることもできます。前述のとおり、Dial-via-office コールが強制されている場合でも、緊急番号へのコール（ダイレクト コネクト クライアント デバイス設定ページの [Emergency Numbers] フィールドで設定したとおり）は常に、モバイル ボイス ネットワークを介して直接ダイヤルされます。

Dial-via-office の操作および動作は、Cisco Unified Mobile Communicator ソリューションに関する説明とほぼ同じですが（「Dial-via-office」（P.25-90）を参照）、Cisco Unified Mobility Advantage サーバと Cisco Unified Mobile Communication クライアントが関与しない点が唯一異なります。代わりに、Dial-via-office コールのセットアップ用の通信は、ダイレクト モバイル クライアントと Unified CM の間でモバイル データ ネットワーク接続を介して直接実施されます。

Cisco Unified Mobile Communicator ソリューションと同様に、ダイレクト コネクト モバイル クライアントは Dial-via-Office Reverse Call Back（DVO-R: Dial-via-office リバース コールバック）または Dial-via-Office Forward（DVO-F; Dial-via-office 転送）操作を実行できます。

Dial-via-office コール フローおよび操作については、「Dial-via-office」（P.25-90）を参照してください。

セッション再開

Cisco Unified CM 8.5 以降、ダイレクト コネクト モバイル クライアントのユーザは、コールのセットアップ時やネットワーク障害の発生時に Dial-via-office 転送コールのリダイヤルを行うことができます。Unified CM 8.5 以降のリリースでは、ユーザが最後にダイヤルした相手の電話番号が、Redial Await Timer サービス パラメータで指定した期間キャッシュされます。デフォルトでは、相手の電話番号がキャッシュされるのは 3 分間です。コールのセットアップ時やネットワーク障害が発生した場合などに、リダイヤル ソフトキーを押すかモバイル電話機のコール履歴リストを選択すると、Redial Await Time で期限切れになるまでは、最後にダイヤルした電話番号に Dial-via-office 転送機能を使用して自動的に再接続します。

（注）　Unified CM 8.5 以降のリリースに搭載されたセッション再開機能または Dial-via-office 転送リダイヤル機能は、Dial-via-office 転送機能に対応する Cisco Unified Mobile Communicator 7.*x* クライアントおよび Cisco Unified Mobility Advantage 7.1(3) の新規および既存の展開で使用することもできます。この機能を使用するために、Unified Mobile Communicator や Unified Mobility Advantage の設定を変更する必要はありません。

モバイル トール バイパスの最適化

Dial-via-office コールの最低料金のルーティングを実現するため、Cisco Unified CM 8.5 より、管理者は、Dial-via-office 操作に使用できるように複数のエンタープライズ機能アクセス番号をシステムに設定できるようになりました。また、これらの番号は、新しいモビリティ プロファイル構成要素を使用してユーザに割り当てることができます。複数のエンタープライズ機能アクセス番号を使用できることにより、Dial-via-office 転送コールのローカル アクセス番号および Dial-via-office リバース コールのローカル側で有効な発信者 ID に対応できます。Dial-via-office 転送アクセス番号および Dial-via-office リバース発信者 ID は、地理的に適したモビリティ プロファイルの割り当てに従ったユーザの地理的な位置に基づいています。

モバイル トール バイパス最適化機能では、まず、複数のエンタープライズ機能アクセス番号を設定します。この番号はそれぞれ特定の地理的な位置に対応しています。グローバルに展開されているシステムでは、管理者は世界中の位置に対し、ユーザ数とオフィスの場所に基づいてローカル アクセス番号または DID を付与します。たとえば、ローカル番号を米国の都市の San Jose、New York、Miami、および英国の London、ドイツの Berlin、日本の Tokyo に設定できます。

次に、これらの複数のアクセス番号を、モビリティ プロファイルの設定に基づいてユーザに割り当てます。モビリティ プロファイルは、それぞれの地理的な位置で作成され、その位置のユーザに割り当てられます。たとえば、モビリティ プロファイルは、San Jose、New York、Miami、London、Berlin、Tokyo のユーザに設定されます。それぞれのプロファイルにはローカル側で有効な、その地理的な位置に特定したアクセス番号または DID が含まれています。この方法では、それぞれの位置のユーザは Dial-via-office 転送サービスに、長距離用番号や国際番号ではなく市内番号を使用してアクセスできます。それぞれの地理的な位置に市内番号を付与することで、一般に市内発信に適用される請求料率の方が安いため、コスト削減になります。

それぞれのモビリティ プロファイルは、ダイヤル プランおよび Dial-via-office によって最大 3 つまで設定されます。各プロファイルの Dial-via-office 転送の箇所で、管理者はエンタープライズ機能アクセス番号およびサービス アクセス番号を設定できます。短縮形式で設定した場合は、サービス アクセス番号はエンタープライズ機能アクセス番号の E.164 形式で提供され、サービス アクセス番号およびエンタープライズ機能アクセス番号がペアで使用されます。エンタープライズ機能アクセス番号が完全な E.164 形式で設定されている場合、サービス アクセス番号を設定する必要はありません。これらの番号のいずれかまたは両方が、システムによりダイレクト コネクト モバイル クライアントに転送された番号として、次に Dial-via-office 転送コールを完了するためのシステムへのコールにクライアントが使用する番号として、Dial-via-office 転送動作で使用されます。モビリティ プロファイルで設定できる他の

番号は、それぞれのプロファイルの Dial-via-office リバース コールバック部分の、コールバック発信者 ID です。この番号は、Dial-via-office リバース コールバック コールで公衆網にあるダイレクト コネクト モバイル クライアント デバイスへの発信コールを行うときに Unified CM システムが使用する発信者 ID として指定します。

モビリティ プロファイルには [Mobile Client Calling Option] フィールドも含まれており、システム管理者はこのフィールドを使用して、Dial-via-office コールが発信されたときに Dial-via-Office リバースを使用するか、Dial-via-Office 転送を使用するかを指定できます。これにより、モバイル クライアントが使用する Dial-via-office コール方向の管理制御が可能になり、管理者は最も安価な方法で Dial-via-office コールが発信されるようにすることができます。

モビリティ プロファイルは、ユーザが通常クライアントを使用する位置に基づいてユーザに割り当てる必要があります。ユーザが地理的な位置を移動した場合、管理者は新しい位置に基づいて、手動でユーザに別のプロファイルを割り当てる必要があります。システムでは、モビリティ プロフィルは、ユーザの位置に基づいて動的に更新されません。

モビリティ プロファイルは、モビリティ ID および Dial-via-office 機能を利用できるように設定されたモバイル デバイスだけに割り当てることができます。Cisco Mobile 8.5 for Nokia などのダイレクト コネクト モバイル クライアントおよび旧リリースの Cisco Unified Mobile Communicator クライアントは、モビリティ ID および Dial-via-office 機能が設定されたデバイスです。モビリティ プロファイルは、通常の Unified Mobility リモート接続先に設定できません。

（注） Unified CM 8.5 以降のリリースで提供されているモバイル トール バイパス最適化機能は、Cisco Unified Mobile Communicator 7.*x* クライアントおよび Cisco Unified Mobility Advantage 7.1(3) の新規および既存の展開で使用できます。この機能を使用するために、Unified Mobile Communicator や Unified Mobility Advantage の設定を変更する必要はありません。Unified Mobility Advantage サーバでは、Unified CM 8.5 以降のリリースで転送されたアクセス番号が自動的に使用されます。ただし、管理者が Dial-via-office リバースまたは Dial-via-office 転送を指定できる [Mobile Client Calling Option] フィールドは、Cisco Unified Mobile Communicator デバイスの Dial-via-office コール フローに影響を与えません。Cisco Unified Mobile Communicator クライアントの Dial-via-office の方向は、クライアント自身だけで制御されます。

追加のサービスおよび機能

Dial-via-office および VoWLAN コール処理サービスまたは呼制御サービスに加えて、ダイレクト コネクト モバイル クライアントでは、この項に説明する機能およびサービスを提供できます。

XMPP ベースの IM およびプレゼンス

ダイレクト コネクト モバイル クライアントは、Extensible Messaging and Presence Protocol（XMPP）に対応しており、オンプレミスの Cisco Unified Presence サーバまたはオフプレミスの Cisco WebEx Connect クラウド サービスへの統合を通じた企業向けの IM およびプレゼンス サービスを利用できます。いずれの場合も、ダイレクト コネクト モバイル クライアントにより、次のことが可能になります。

- ユーザを連絡先リストまたはバディ リストに追加する。
- ユーザのプレゼンスおよび応答可能性のステータスを設定および伝達する。
- バディまたは連絡先のプレゼンス ステータスを受信する。
- Instant Messaging（IM; インスタント メッセージング）またはテキスト メッセージを作成し、送信する。
- IM またはテキスト メッセージを受信する。
- IM またはテキスト メッセージを音声コールにエスカレーションする。

社内ディレクトリ アクセス

ダイレクト コネクト モバイル クライアントは、モバイル データ ネットワークまたは WLAN 経由で会社に接続している場合、LDAP を使用して社内ディレクトリにアクセスし、ディレクトリ ルックアップを行うことができます。この機能はダイレクト コネクト モバイル クライアントに必須の機能ではありませんが、携帯電話から社内ディレクトリ情報にアクセスできると、ダイレクト コネクト クライアント ユーザの生産性が向上します。

企業の MWI およびメッセージ数インジケータ

ダイレクト コネクト モバイル クライアントは、企業ボイスメール サービスにアクセスすることもできます。ダイレクト コネクト クライアントでは、未読のボイスメールがユーザの企業ボイスメール ボックスにある場合には企業の Message Waiting Indication（MWI; メッセージ待機インジケータ）と、ボイスメール ボックス内の新規または未読のメッセージ数を受信できます。MWI とメッセージ数インジケータを受信するには、ダイレクト コネクト モバイル クライアントが企業ネットワークに（モバイル ボイス ネットワークまたは WLAN 経由で）接続している必要があります。

通常の会社の電話機と同様に、ダイレクト コネクト モバイル クライアントを使用して、ボイスメール システム番号にダイヤルし、必要な資格情報を提供した後で適切なボイスメール ボックスに移動することにより、企業ボイスメール メッセージを取得できます。

モバイル コネクトのオン/オフ

Unified Mobility に統合し、モバイル コネクトを有効にしている場合、ダイレクト コネクト モバイル クライアントではモバイル コネクトのステータスを表示し、クライアント設定インターフェイスを介してモバイル コネクトのオフとオフを切り替えることができます。このため、ユーザは、モバイル データ ネットワーク経由でリモートから会社に接続している場合でも、ダイレクト コネクト モバイル クライアント デバイスの携帯の番号に対してモバイル コネクトまたはシングル ナンバー リーチ機能を有効にしたり、無効にしたりすることができます。

ダイレクト コネクト モバイル クライアント：Cisco Mobile 8.5 for Nokia

Cisco Mobile 8.5 for Nokia は、Nokia モバイル スマート フォン対応のダイレクト コネクト モバイル クライアントです。Nokia デバイスにインストールすると、クライアントはローカルの企業 WLAN ネットワークに関連付けることも、モバイル データ ネットワークを介して会社にリモートに関連付けることもできます。クライアントは Unified CM に登録され、通信できるようになります。

Cisco Mobile 8.5 ダイレクト コネクト モバイル クライアントを登録し、Dial-via-office サービスを提供するには、Unified CM で適切な Nokia S60 デバイス タイプがサポートされている必要があります。このデバイス タイプは、必要な Cisco Options Package（COP）ファイルを Unified CM にロードすると使用可能になります。COP ファイル（cmterm-nokia_s60_8.5v06-sccp.cop.sgn）は、次の場所で見つけることができます。

http://tools.cisco.com/support/downloads/pub/Redirect.x?mdfid=281001428

COP ファイルがインストールされ、ダイレクト コネクト クライアント デバイスが Unified CM 内に設定された後は、Cisco Mobile 8.5 for Nokia クライアントを Nokia デバイスにロードする必要があります。この作業は、USB、Bluetooth、または赤外線ポートを備えたコンピュータを使用して行うことができます。Cisco Mobile 8.5 Symbian Installation System（SIS）ファイルを Nokia デバイスにロードした後は、少なくとも、ローカルの企業 WLAN にアクセスして企業の WLAN インフラストラクチャおよびセキュリティ ポリシーに基づいて接続するようにデバイスを設定する必要があります。VPN を使用したリモートの企業ネットワーク接続を有効にするには、その他の設定も必要です。

Cisco Mobile 8.5 Nokia デバイスを Unified Mobility と統合して、ユーザがモバイル コネクトなどの機能を利用できるようにするには、Nokia の携帯電話番号をモビリティ ID として設定し、それを Unified CM 内で Nokia S60 デバイスに関連付けます。

Cisco Mobile 8.5 クライアントは、Symbian Series 60 Third Edition Feature Pack 1 (3.1) または Feature Pack (3.2) ファームウェアを実行する Nokia ハンドセットでサポートされます。たとえば、Nokia E55、E66、E71、E72、および E75 などのデバイスが含まれます。

Nokia 携帯電話の WLAN インターフェイスは通常、802.11b および 802.11g ネットワーク接続をサポートしています。

Cisco Mobile 8.5 クライアントは、Dial-via-office サービスを提供するだけでなく、LDAP 準拠のディレクトリを指すように設定されている場合はディレクトリ ルックアップ サービスも提供します。また、Cisco Unified Presence または Cisco WebEx Connect に統合されている場合は XMPP ベースのプレゼンスおよび IM を提供します。

システム要件とサポートされているデバイスの詳細については、次の Web サイトにある Cisco Mobile 8.5 for Nokia のリリース ノートを参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cumc/cisco_mobile/nokia/8_x/Release_Notes/Cisco_Mobile_Nokia_85_RN.html

Cisco Mobile 8.5 for Nokia のインストールと設定の詳細については、次の Web サイトで入手可能な管理ガイドを参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cumc/cisco_mobile/nokia/8_x/admin/Cisco_Mobile_for_Nokia_8.5_Admin_Guide.html

Cisco Mobile 8.5 と Nokia Call Connect の共存

WLAN 機能を介したデュアルモード ボイスをサポートするには、デバイスに Cisco Mobile 8.5 と Nokia Call Connect デュアルモード クライアントを共存インストールする必要があります。Nokia Call Connect クライアントは、Voice over WLAN コールをサポートします。両方のクライアントが、Unified CM 内の Nokia デバイスに対する Nokia S60 デバイス設定に関連付けられます。

共存で動作する場合、Nokia Call Connect デュアルモード クライアントは「デュアルモード クライアント：Nokia Call Connect」（P.25-77）で説明したとおりに動作します。Cisco Mobile 8.5 と共存する Nokia Call Connect デュアルモード クライアントの操作と展開に関しては、操作的および機能的な動作においてスタンドアロンの Nokia Call Connect デュアルモード クライアントのインストールと変わりません。ハンドオフ操作と設定に関する同一の設計上および展開上の要件を考慮する必要があります。同様に、「ワイヤレス デバイスのローミング」（P.25-14）に示されている設計上の推奨事項と要件はすべて、Cisco Mobile 8.5 と共存して動作する Nokia Call Connect に適用されます。

Cisco Mobile 8.5 および Nokia Call Connect クライアントを共存展開する際、Unified CM 管理者は Dial-via-office を強制しないでください。代わりに、Nokia S60 デバイス設定ページの [Dial Policy] パラメータを [Let User Choose] として設定してください。これにより、ユーザは、Dial-via-office を使用するときに各自の意思を最大限反映できるので、ユーザが社外にいるときや、WLAN 経由の音声品質が低いときにだけ、この機能が使用されるようにすることができます。

管理者が Cisco Mobile 8.5 に対して Dial-via-office を強制する場合には、ユーザは Cisco Mobile 8.5 クライアント内で [Allow dial via office for] を [Calls from this app] に設定して、クライアント アプリケーション内から直接発信されたコールだけが Dial-via-office の呼び出しを試みるようにする必要があります。クライアントをこのように設定することによって、ユーザは、予期せず Dial-via-office が実行されないようにできます。Cisco Mobile 8.5 クライアントがフォアグラウンドで実行されていない場合、Dial-via-office は呼び出されません。

これらの 2 つのクライアントが共存して動作するときは、次の点を考慮してください。

- WLAN 信号の強度が強い場合には、Nokia Call Connect デュアルモード クライアントを Voice over WLAN コールの発信および受信に使用します。
- 音声品質が低いか、WLAN 接続が使用できない場合には、Cisco Mobile 8.5 ダイレクト コネクト クライアントを Dial-via-office コールに使用します。

いずれの場合も、ユーザは、ダイレクト コネクト モバイル クライアント デバイスが社外にあるか、WLAN 上の音声品質が低い場合に限り、Dial-via-office を使用するようにします。

Cisco Mobile 8.5 と Cisco Unified Mobility との間の相互作用

Nokia 対応の Cisco Mobile 8.5 ダイレクト コネクト モバイル クライアントを Cisco Unified Mobility と統合することで、Cisco モバイル コネクト、通話切替 DTMF 機能（モバイル データ接続または WLAN 接続が使用できない場合）、シングル企業ボイスメール ボックス、およびデスクトップフォンのピックアップを利用できます。

Unified Mobility と統合するには、Unified CM 内で、Nokia ダイレクト コネクト クライアント デバイスの携帯電話番号を Nokia S60 デバイスに関連付けられたモビリティ ID として設定する必要があります。システム内で携帯の番号をモビリティ ID として設定した後は、モバイル コネクトを利用して、ユーザの会社の番号への着信コールがモバイル ボイス ネットワーク経由で Nokia ダイレクト コネクト クライアント デバイスに転送されるようにすることができます。モバイル コネクト機能は、Cisco Mobile 8.5 クライアント内でリモートから有効または無効にすることもできます。Nokia デバイスで Nokia Call Connect デュアルモード クライアントも実行している場合には、デバイスが社内にあり、WLAN 経由で Unified CM に登録されていると、会社の番号への着信コールはデバイスのモバイル ボイス ネットワーク インターフェイスには転送されません。Nokia デバイスが社内にある場合は、デバイスの WLAN インターフェイスだけが着信コールを受信します。これにより、会社の公衆網ゲートウェイ リソースの必要以上の消費を回避できます。

社外で Nokia デバイスからモバイル データ ネットワークに到達できる場合、Cisco Mobile 8.5 クライアントではコールの発信に Dial-via-office を使用できます。ただし、モバイル データ接続を使用できない場合でも、ユーザは、Unified Mobility 2 ステージ ダイヤリング機能のモバイル ボイス アクセスまたはエンタープライズ機能アクセスを使用してビジネス コールを発信できます。また、会社の任意の固定コール（Dial-via-office、2 ステージ ダイヤリング、またはダイレクト ダイヤリング対象の会社の番号およびモバイル コネクト）については、ユーザは Cisco Mobile 8.5 クライアントのデスクへのコールの移動機能を使用して、アクティブ コールをデスクトップフォンに移動できます。企業接続を使用できない場合には、DTMF 機能アクセス コードによって通話切替機能を呼び出すこともできます。

Nokia ダイレクト コネクト モバイル クライアント デバイスに対してモビリティ ID を設定することに加えて、リモート接続先として追加の携帯電話番号またはオフシステム電話番号を設定して、これらの番号を Unified CM 内の Nokia S60 デバイスに関連付けることができます。モビリティ ID および追加のリモート接続先を Nokia デバイスに関連付ける場合は、リモート接続先プロファイルを設定する必要はありません。既存の Nokia 携帯電話ユーザに対して Unified Mobility がすでに有効になっており、Cisco Mobile 8.5 に移行している場合、既存のリモート接続先プロファイルを削除し、設定されているリモート接続先を削除して Nokia S60 デバイスに直接追加しなおす必要があります。リモート接続先およびモビリティ ID が Unified CM システム内で固有でなければならないため、この作業が必要になります。

Cisco Unified Mobility の機能セット、および設計と展開の考慮事項の詳細については、「Cisco Unified Mobility」（P.25-37）を参照してください。

ダイレクト コネクト モバイル クライアントのハイ アベイラビリティ

ダイレクト コネクト モバイル クライアント デバイスは、その特性上ネットワーク接続に関して非常に高い可用性を備えていますが（企業の WLAN ネットワークまたはモバイル データ ネットワークが利用できない場合には、モバイル ボイス ネットワークを音声に使用できます）、企業の WLAN、VPN インフラストラクチャ、および IP テレフォニー インフラストラクチャのハイ アベイラビリティについては考慮の余地があります。

まず、企業の WLAN は、冗長な WLAN アクセスが可能になるように配置する必要があります。たとえば、AP およびその他の WLAN インフラストラクチャ コンポーネントは、ワイヤレス AP の 1 つに障害が発生しても、ダイレクト コネクト モバイル クライアントのネットワーク接続には影響がないように展開する必要があります。同様に、常にデュアルモード デバイスがネットワークに安全に接続できるように、WLAN の管理およびセキュリティ インフラストラクチャも高い冗長性を備えた配置にする必要があります。企業内 AP の集中型設定および管理が可能であり、ネットワーク アクティビティおよび AP の障害に基づいて WLAN を動的に調整できることから、コントローラベースのワイヤレス LAN インフラストラクチャが推奨されます。

次に、VPN セッション端末の喪失がモバイル クライアントのリモート企業接続に影響したり、妨げになったりしないように、Cisco IOS または ASA ヘッドエンド VPN または AnyConnect セッション端末を含む VPN インフラストラクチャ コンポーネントも高い冗長性を備えた展開にします。

Unified CM のコール処理サービスおよび登録サービスのハイ アベイラビリティについても考慮する必要があります。Unified CM のコール処理サービスを利用する企業内の他のデバイスと同様に、ダイレクト コネクト モバイル クライアントも Unified CM に登録する必要があります。Unified CM クラスタのアーキテクチャにはプライマリおよびバックアップのコール処理サービスおよびデバイス登録サービスが用意されており、冗長な特性を持っているため、1 つの Unified CM サーバ ノードで障害が発生しても、ダイレクト コネクト モバイル クライアント デバイスの登録やコール ルーティングは引き続き利用可能です。

公衆網アクセスについても同様の事項を考慮する必要があります。IP テレフォニー配置と同様、複数の公衆網ゲートウェイおよびコール ルーティング パスを配置して、公衆網への可用性の高いアクセスを確保する必要があります。このことは、ダイレクト コネクト モバイル クライアントの展開に固有の考慮事項ではありませんが、重要な考慮事項です。

ダイレクト コネクト モバイル クライアントのキャパシティ プランニング

ダイヤル コネクト モバイル クライアントにおけるキャパシティ プランニングに関する考慮事項は、登録、コール処理、公衆網アクセスなどのサービスのために IP テレフォニー インフラストラクチャおよびアプリケーションを利用する他の IP テレフォニー エンドポイントまたはデバイスと同じです。

ダイレクト コネクト モバイル クライアントを展開する場合、Unified CM における登録の負荷および Unified Mobility の制限について考慮することが重要です。1 つの Unified CM サーバでは、最大 10,000 のデバイスの設定および登録を処理できます。ダイレクト コネクト モバイル クライアント デバイスを展開する場合、サーバあたりでサポートされる最大デバイス数を考慮する必要があります。追加の負荷を処理するために、コール処理サブスクライバ ノードを追加で展開する必要がある場合があります。

また、「Cisco Unified Mobility のキャパシティ プランニング」（P.25-61）で説明したように、1 つの Unified CM クラスタ内のリモート接続先およびモビリティ ID の最大数は 15,000 です。ほとんどのダイレクト コネクト モバイル クライアントは、モバイル コネクトやデスクトップフォンのピックアップなどの機能を利用するために Unified Mobility と統合されるため、これらの各ダイレクト コネクト クライアント デバイスの携帯電話番号は Unified CM クラスタ内にモビリティ ID として設定する必要があります。これは、Unified Mobility との統合を容易にするため、場合によってはハンドオフを容易にするために必要です。したがって、これらのダイレクト コネクト クライアント デバイスを Unified Mobility と統合する場合には、Unified CM クラスタにおけるリモート接続先およびモビリティ ID の全体的な容量を考慮して、十分な容量を確保することが重要です。追加のユーザまたはデバイスがシス

テム内の Unified Mobility にすでに統合されている場合は、これらのユーザまたはデバイスによって、ダイレクト コネクト クライアント デバイスで利用可能なリモート接続先およびモビリティ ID の空き容量が制限される可能性があります。

ダイレクト コネクト モバイル クライアントを展開する場合、Unified CM システムおよび公衆網ゲートウェイの全体的なコール処理容量も考慮する必要があります。クライアント デバイスの実際の設定および登録を処理する以外に、システムでは、これらの新しいデバイスとユーザによって増加する BHCA の影響を吸収するために十分な容量も必要です。同様に、ダイレクト コネクト クライアントを処理するのに十分な公衆網ゲートウェイの容量を確保することも重要です。

上記の考慮事項は、ダイレクト コネクト クライアント デバイスに固有なものではありません。これらの考慮事項は、デバイスやユーザが Unified CM に追加されることによって Unified Communications システム全体の負荷が高まるすべての状況に当てはまります。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を使用して、Unified CM を含む Cisco Unified Communications システムの容量を計算できます。このサイジング ツールでは、システム全体の容量を計算するための入力としてモバイル クライアント電話デバイスの数を受け取り、入力された数のモバイル クライアント電話デバイスおよびそれらのデバイスがシステムの全体的なサイズに与える影響に対応できる適切なシステム サイズを、デバイスの登録、コール処理（BHCA）、およびゲートウェイの利用負荷に基づいて計算します。システムのサイジングでサポートが必要な場合は、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

シスコ代理店と従業員は、Cisco Unified Communications Sizing Tool を次の Web サイトで入手できます。

http://tools.cisco.com/cucst

ダイレクト コネクト モバイル クライアントの設計上の考慮事項

ダイレクト コネクト モバイル クライアントを展開するときは、次の設計上の推奨事項に従ってください。

- ダイレクト コネクト モバイル クライアントのユーザが緊急コールを発信し、デバイスおよびユーザの位置を特定する場合には、モバイル ボイス ネットワークを利用することを推奨します。これは、通常モバイル プロバイダー ネットワークでは、企業の WLAN ネットワークよりもはるかに信頼性のある位置情報が提供されるためです。これらのクライアント デバイスから緊急コールを発信したり位置サービスを利用したりする場合にモバイル ボイス ネットワークだけが利用されるようにするには、911、999、および 112 などの緊急番号がダイレクト コネクト クライアント デバイス設定ページの [Emergency Numbers] フィールドに設定されており、これらの番号に対するすべてのコールがモバイル ボイス ネットワーク経由で送信されることを確認します。
- 地理的な複数の位置にわたってユーザのダイレクト コネクト モバイル クライアントを展開する際に、位置に固有のシステム アクセス番号を Dial-via-office に割り当てるために、モバイル トール バイパスの最適化機能を使用することを検討してください。Dial-via-office の方向がコール コストに影響する場合には、特定の Dial-via-office 方向（フォワードまたはリバース）を強制するために、モビリティ プロファイルの [Mobile Client Calling Option] フィールドを使用することを検討してください。
- Cisco Mobile 8.5 ダイレクト コネクト クライアントと Nokia Call Connect デュアルモードの両方が同じハンドセットに展開されている場合は、次のことが推奨されます。
  - 「ワイヤレス デバイスのローミング」（P.25-14）で説明する Voice over WLAN に関するすべての推奨事項と要件に従ってください。
  - 「デュアルモードの電話機とクライアント」（P.25-64）で説明する Nokia Call Connect の設定および展開に関するすべての推奨事項と要件に従ってください。

  - デュアルモード機能が有効である場合、Unified CM 管理者は Dial-via-office を強制しないでください。代わりに、Nokia S60 デバイス設定ページの [Dial Policy] パラメータを [Let User Choose] として設定してください。
  - 管理者が Cisco Mobile 8.5 に対して Dial-via-office を強制する場合、ユーザは Cisco Mobile 8.5 クライアント内で [Allow dial via office for] を [Calls from this app] に設定して、クライアント アプリケーション内から直接発信されたコールだけが Dial-via-office の呼び出しを試みるようにする必要があります。クライアントをこのように設定することによって、ユーザは、予期せず Dial-via-office が実行されないようにできます。Cisco Mobile 8.5 クライアントがフォアグラウンドで実行されていない場合、Dial-via-office は呼び出されません。

- 共存して動作する Cisco Mobile 8.5 と Nokia Call Connect クライアントでのコールの発信に関して、次の点を考慮してください。
  - WLAN 信号の強度が強い場合には、Nokia Call Connect デュアルモード クライアントを Voice over WLAN コールの発信および受信に使用します。
  - 音声品質が低いか、WLAN 接続が使用できない場合、Cisco Mobile 8.5 ダイレクト コネクト クライアントを Dial-via-office コールに使用します。

CHAPTER 26

Cisco Unified Contact Center

この章では、Cisco Unified Communications システムで使用可能な Cisco Unified Contact Center ソリューションについて説明します。Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise、Cisco Unified Customer Voice Portal、Cisco Unified Expert Advisor などのシスコ製品に関する情報を示します。また、Cisco Unified Communications Manager やその他の Unified Communications コンポーネントを使用してこれらの Cisco Unified Contact Center 製品を配置する際の設計上の考慮事項についても取り上げます。

この章では、次のトピックについて取り上げます。

この章では最初に、メインの Cisco Unified Contact Center ポートフォリオの概要を示します。続いて、コンタクト センターのさまざまな Unified Communications 配置モデルについて取り上げます。最後に、帯域幅、遅延、Cisco Unified Communications Manager との統合、サイジングなどのトピックに関する設計上の考慮事項について説明します。

この章の目的は、各コンタクト センター製品とその各種コンポーネントの詳細を説明することではなく、各製品を Cisco Unified Communications システムと統合する際の設計上の考慮事項について説明することです。Unified Contact Center の各製品の詳細な設計ガイドラインは、Cisco Unified Contact Center Express、Cisco Unified Contact Center Enterprise、および Cisco Unified Customer Voice Portal 製品向けの Solution Reference Network Design（SRND; ソリューション リファレンス ネットワーク デザイン）の個別ガイドを参照してください。これらの製品固有の SRND は、次のサイトで入手できます。

http://www.cisco.com/go/ucsrnd

この章の新規情報

表 26-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 26-1　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco MediaSense	「Cisco MediaSense」（P.26-6）	2011 年 6 月 2 日
製品名が Cisco Unified Media Capture Platform（Unified MCP）から Cisco MediaSense に変更されました。	「Cisco MediaSense」（P.26-6）	2011 年 1 月 31 日

Cisco Contact Center アーキテクチャ

この章では、次の主要な Cisco Contact Center 製品について説明します。

- Cisco Unified Contact Center Enterprise（Unified CCE）
- Cisco Unified Customer Voice Portal（Unified CVP）
- Cisco Unified Contact Center Express（Unified CCX）
- Cisco Unified Expert Advisor（Unified Expert Advisor）

Cisco Unified Contact Center Enterprise

Cisco Unified Contact Center Enterprise（Unified CCE）は、VoIP コンタクト センター ソリューションを提供します。これにより、インバウンドおよびアウトバウンドの音声アプリケーションを、リアルタイム チャット、Web コラボレーション、電子メールなどのインターネット アプリケーションと統合できます。この統合により、顧客がどの通信チャネルを選択したかに関係なく、各エージェントが同時に複数のインタラクションに対応することを支援する統合的な機能が提供されます。各インタラクションは一意であり、個別的なサービスを必要とすることがあるため、シスコは、ほぼすべてのコンタクト属性に基づいて各インタラクションを管理するためのコンタクト センター ソリューションを提供しています。Unified CCE 配置は通常、大規模なコンタクト センターに対して使用され、何千ものエージェントをサポートできます。

Unified CCE は、次の主要なソフトウェア コンポーネントを採用しています。

- Call Router

  Call Router は、コールまたはカスタマー コンタクトのルーティング方法に関するすべての決定を行います。

- Logger

  Logger は、コンタクト センターの設定情報とデータサーバへ配信する履歴レポートデータを一時的に格納するデータベースを保持します。Call Router および Logger の組み合せは、*Central Controller* と呼ばれます。

- ペリフェラル ゲートウェイ

  Peripheral Gateway（PG; ペリフェラル ゲートウェイ）は、各種の「周辺」機器（Unified CM、Cisco Unified IP Interactive Voice Response（Unified IP IVR）、Unified CVP、マルチチャネル製品など）を接続します。Unified CM と連携するペリフェラル ゲートウェイは、*Agent PG* とも呼ばれます。

- CTI サーバおよび CTI Object Server（CTI OS）

  CTI サーバおよび CTI Object Server は、エージェント デスクトップと連携します。エージェント デスクトップは、Cisco Agent Desktop（CAD）ソリューション、Cisco CTI Desktop Toolkit、またはサードパーティ製 CRM アプリケーション向けの Customer Relationship Management（CRM; カスタマー リレーションシップ マネージメント）コネクタに基づいて設定できます。

- Administration & Data Server

  Administration & Data Server は、設定インターフェイスと、リアルタイム データ ストレージと履歴データ ストレージを提供します。

Cisco Unified CCE ソリューションは、エージェントの電話機を制御する Cisco Unified Communications Manager（Unified CM）との統合に基づいています。Unified CM を使用せず従来の ACD を使用する配置では、Unified CCE ではなく Cisco Unified Intelligent Contact Management Enterprise（Unified ICME）を使用します。

キューイングおよびセルフサービスの機能は、Cisco Unified IP Interactive Voice Response（Unified IP IVR）または Cisco Unified Customer Voice Portal（Unified CVP）によって提供され、Unified CCE Call Router によって制御されます。

ほとんどの Unified CCE サーバは冗長構成にする必要があります。冗長インスタンスは、サイド A インスタンスおよびサイド B インスタンスと呼ばれます。たとえば、Call Router A および Call Router B は、2 つの異なるサーバ上で稼動する Call Router コンポーネントの冗長インスタンスです。

Cisco Unified Customer Voice Portal

Cisco Unified Customer Voice Portal（Unified CVP）は、Voice over IP（VoIP）ネットワークでの通信事業者クラスの IVR サービスを提供します。CRM データベース統合と、Automated Speech Recognition（ASR; 自動音声認識）と Text-to-Speech（TTS; テキストツースピーチ）の統合により、Unified CVP は、基本的な入力要求と情報収集のアプリケーションや高度なセルフサービス アプリケーションを実行できます。また、Unified CVP は、音声ゲートウェイと IP エンドポイント間でコールをルーティングおよび転送することにより、IP ベースのコール スイッチング サービスを提供します。

Unified CVP は、Voice Extension Markup Language（VXML）をベースにしています。これは HTML に似た業界標準のマークアップ言語であり、Web 開発とコンテンツ配信の力を利用する IVR サービスを開発する目的で使用されます。

Unified CVP は、スタンドアロンで配置することも、セルフサービスおよびキューイングの機能を利用するために Unified CCE と統合することもできます。Unified CVP では、音声コールとビデオ コールの両方をサポートしています。

Unified CVP ソリューションは、次の主要なコンポーネントを採用しています。

- Unified CVP コール サーバ

  Unified CVP コール サーバは、SIP および H.323 サービスを介して SIP および H.323 の機能を制御できます。また、Unified CVP コール サーバは、Intelligent Contact Management（ICM）サービスを介して Unified CCE Call Router と統合できます。IVR サービスを使用すると、Unified CVP コール サーバは、VXML Micro アプリケーションを実行したり、VoiceXML ページを作成したりできます。

- Unified CVP VXML Server

  このコンポーネントは、VoiceXML ゲートウェイに組み込まれた音声ブラウザと VoiceXML ページをやりとりすることによって、複雑な IVR アプリケーションを実行します。Unified CVP VXML Server アプリケーションは、Cisco Unified Call Studio を使用して記述され、実行のために Unified CVP VXML Server に配置されます。Unified CVP コール サーバまたは Unified CVP VXML Server を経由する RTP トラフィックはないことに注意してください。

- Cisco Voice Gateway

  Cisco Voice Gateway は、コールが Unified CVP システムに出入りするポイントです。Cisco Voice Gateway には、公衆網への TDM インターフェイスを含めることができます。あるいは、公衆網へのインターフェイスが IP 音声トランクである場合は、Cisco Unified Border Element を使用することもできます。

- Cisco VoiceXML Gateway

  VoiceXML Gateway は、Cisco IOS Voice Browser のホストとなります。このコンポーネントは、Unified CVP Server IVR Service または Unified CVP VXML Server からの VoiceXML ページを解釈します。VoiceXML Gateway では、.wav ファイルをベースにしたプロンプトを発信者に再生できます。また、DTMF 入力または音声を介して発信者からの入力を受け入れることができます（自動音声認識と統合されている場合）。続いて VoiceXML Gateway は、制御側アプリケーションに結果を返し、次の指示を待機します。

  Cisco VoiceXML Gateway は、Cisco 音声ゲートウェイと同じルータ上に配置できます。このモデルは、小規模な拠点オフィスにも配置する場合に適しています。しかし、VoiceXML Gateway を個別のルータ プラットフォーム上で実行することもできます。このモデルは、複数の音声ゲートウェイが含まれる大規模な集中型配置での使用に適しています。

詳細については、次の URL にある『*Cisco Unified Customer Voice Portal SRND*』の最新版を参照してください。

http://www.cisco.com/go/ucsrnd

Cisco Unified Contact Center Express

Cisco Unified Contact Center Express（Unified CCX）は、400 までのエージェントに対して、使いやすく可用性の高い高度なカスタマー インタラクションを提供する必要のある、部門、企業の支店、または中小規模の会社のニーズに対応するものです。Unified CCX は、複数のサイトにわたる統合セルフサービス アプリケーションを使用して可用性の高い仮想コンタクト センターをサポートすることにより、カスタマー コンタクト インタラクションの効率、可用性、およびセキュリティを高めるような設計になっています。

Unified CCX は、JTAPI を使用して Unified CM と統合できます。また、SIP を使用して Unified CME と統合できます。

Unified CCX のすべてのコンポーネント（Unified CCX エンジン、Unified CCX データベース、CAD Server、Unified CCX Outbound Dialer、および Express E-mail Manager を含む）が、単一のサーバ上にインストールされます。Unified CCX を Unified CM に統合する場合、別の Unified CCX サーバを追加して、システムを冗長構成にすることができます。

Unified CCX には、E メール、発信ダイヤラ、およびエージェント サイレント モニタリングと録音の機能が組み込まれています。Unified CCX は、Cisco TelePresence などのビデオ エンドポイントと統合して、Automated Speech Recognition（ASR; 自動音声認識）と Text-to-Speech（TTS）、HTTP、VXML などの高度な機能をサポートできます。また、コンタクト センターのパフォーマンスと品質を最適化するために、Cisco Unified Workforce Optimization などの製品もサポートしています。

Cisco Unified IP IVR は、Unified CCX と同じソフトウェア アーキテクチャを共有しています。Cisco Unified IP IVR は、Unified CCE ソリューションに入力要求、情報収集、およびキューイングの機能を提供します。また、Cisco Unified IP IVR をスタンドアロンのセルフサービス アプリケーションとして使用することもできます。

Cisco Unified Expert Advisor

Cisco Unified Expert Advisor は、プレゼンスが有効になっているエンタープライズ ナレッジ ワーカーが、正式なコンタクト センターでよくある厳格なツールやビジネス ルールを使用しなくてもカスタマーの着信コールを処理できるようにすることで、カスタマー ケアの範囲を拡張しています。Cisco Unified Personal Communicator や Microsoft Office Communicator などのエンタープライズ プレゼンス クライアントを使用してコールの受け入れや事前コール データの受信ができるエンタープライズ ナレッジ ワーカーやエキスパートは、Cisco Unified Expert Advisor を使用すると、コールのインテリジェント ルーティングを行うことができます。

Cisco Unified Expert Advisor は、Unified CCE ソリューションのアドオンとして配置することも、Unified CCE エージェントを使用しないスタンドアロン アプリケーションとして配置することもできます。

ナレッジ ワーカーは、Unified CM から到達可能なあらゆる電話機（IP Phone や携帯電話を含む）を使用できます。

管理

Cisco Contact Center 製品には、管理の機能が組み込まれています。たとえば、Unified CCE は、Unified CCE とともにインストールされる Configuration Manager ツールを使用して管理できます。また、Unified CVP は、Unified CVP Operations Console（Operations, Administration, Maintenance, and Provisioning（OAMP）とも呼ばれる）を使用して管理できます。

さらに、エージェントや機器の管理などの基本的な管理機能を実行するための操作および手順を簡素化するために、Cisco Unified Contact Center Management Portal（Unified CCMP）を配置できます。Unified CCMP は、コンタクト センターのシステム管理者、ビジネス ユーザ、およびスーパーバイザ向けに設計されたブラウザベースの管理アプリケーションです。Cisco Unified Contact Center Enterprise（Unified CCE）、Unified Intelligent Contact Management（Unified ICM）、Unified Communications Manager（Unified CM）、および Unified Customer Voice Portal（Unified CVP）機器を重ね合わせた緻密なマルチテナントのプロビジョニング プラットフォームです。

レポーティング

Cisco Unified Intelligence Center（Unified IC）は、Cisco Contact Center ソリューション用の主要なレポーティング ツールです。Unified IC は、Unified CCE、Unified CCX、Unified CVP、および Unified Expert Advisor でサポートされています。このプラットフォームは Web ベースのアプリケーションであり、多数の Web 2.0 機能、高いスケーラビリティ、優れたパフォーマンス、および高度な各機能（他の Cisco Unified Communications 製品やサードパーティ製データ ソースからのデータを統合する機能など）を提供します。

Cisco Unified Intelligence Center は、データベース（Unified CCE Administration & Data Server データベースや Unified CVP Reporting Informix データベースなど）からソース データを取得します。次にレポートが生成されて、レポーティング クライアントに提供されます。

マルチチャネル サポート

Cisco Unified Enterprise ソリューションでは、マルチチャネル サポートのための Web インタラクションおよび電子メール インタラクションをサポートしています。Cisco Unified Web Interaction Manager（Unified WIM）テクノロジにより、ほとんどすべての Web ブラウザから通信を確立できます。Cisco Unified E-Mail Interaction Manager（Unified EIM）は、着信電子メール ルーティング、自動電子メール応答またはエージェント介入による電子メール応答、リアルタイム レポーティングと履歴レポーティングを提供し、エージェント、スーパーバイザ、管理者、ナレッジ ベース管理者向けのロールベースの階層権限を提供します。

これらの製品の設計情報については、次の URL で入手可能な『*Cisco Unified Web and E-Mail Interaction Manager Solution Reference Network Design Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps7236/products_implementation_design_guides_list.html

録音とサイレント モニタリング

Cisco Unified Contact Center ソリューションでは、次の各オプションに基づいて、録音とサイレント モニタリングの機能が提供されます。

- Cisco スイッチの SPAN 機能

  この機能により、ネットワーク トラフィックは、Cisco コンタクト センター サーバが接続されている宛先ポートに複製されます。

- 電話機で音声ストリームを接続先の PC にスパンできること

  この場合、エージェント デスクトップは音声パケットを受信し、録音サーバまたはサイレント モニタリングのためにスーパーバイザー デスクトップに送信します。

- Cisco IP Phone の Built-in Bridge（BIB; ビルトイン ブリッジ）による Unified CM およびメディア複製

  このオプションを使用した場合は、録音フローのセットアップ中に Unified CM が呼び出され、それらのフローに対するコール アドミッション制御を実行できるようになります。

Cisco MediaSense

Cisco MediaSense は、Open Recording Architecture（ORA）オープン インターフェイスが実装された IP ベースのメディア（音声およびビデオ）録音および再生システムです。Cisco MediaSense は、Cisco Unified Communications アーキテクチャに統合され、コンタクト センター配置とコンタクト センター以外の配置の両方に対して録音ソリューションを提供します。録音は、メディア分岐により行われます。メディア分岐では、Cisco IP Phone の Built-In Bridge（BIB; ビルトイン ブリッジ）を使用して、Cisco MediaSense Recording Server にメディアを複製します。

Cisco MediaSense は、冗長で可用性の高いアーキテクチャをサポートします。Cisco MediaSense を、アクティブ/アクティブ モードの 2 台の Recording Server を使用して、非冗長単一サーバ、または可用性の高い冗長なシステムとして配置できます。追加のサーバを追加して、ストレージ容量を拡張できます。

Cisco MediaSense 録音システムの詳細については、次の Web サイトで入手可能な『*Solution Reference Network Design for Cisco MediaSense*』を参照してください。

http://www.cisco.com/en/US/products/ps11389/products_implementation_design_guides_list.html

コンタクト センター配置モデル

この項では、Cisco Unified Contact Center ソリューションの配置に使用されるさまざまな設計モデルについて説明します。これらの配置モデルの詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

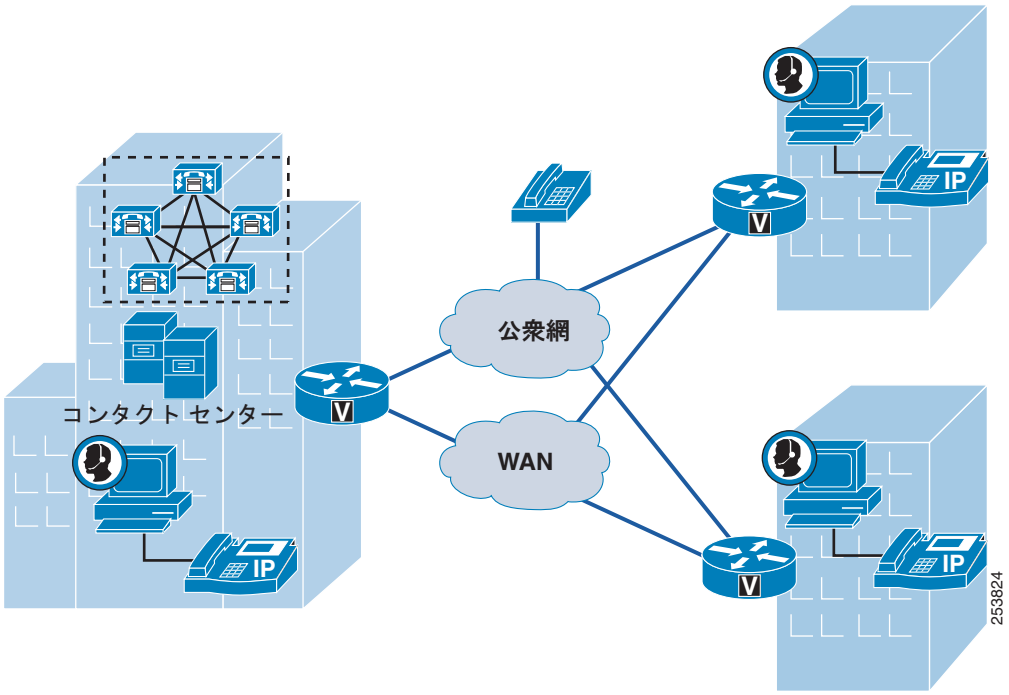
単一サイト コンタクト センター

この配置では、コール処理サーバ、音声ゲートウェイ、コンタクト センター サーバなどのすべてのコンポーネントが同じサイトに存在します。エージェントとスーパーバイザも、そのサイトに配置されます。単一サイト配置モデルの主要なメリットは、WAN 接続が不要なので、低帯域幅のコーデック（G.729、トランスコーダ、compressed Real-Time Transport Protocol（cRTP; RTP ヘッダー圧縮）、コール アドミッション制御など）を使用する必要がないことです。

集中型コール処理を使用するマルチサイト コンタクト センター

集中型コール処理を使用するマルチサイト配置は、単一のコール処理クラスタで構成されます。このクラスタは、多数のリモート サイトにサービスを提供し、IP WAN を使用します。また、Cisco Contact Center アプリケーション（Unified CCE、Unified CCX、Unified CVP、および Unified Expert Advisor）は通常、管理の全体的なコストを削減するために集中化されます。図 26-1 はこのタイプの展開を示しています。

図 26-1　集中型コール処理を使用するマルチサイト コンタクト センター



このタイプの配置では、エージェントまたは音声ゲートウェイがリモート サイトに存在しているため、サイト間の帯域幅の要件を考慮することが重要です。また、コール アドミッション制御や Quality of Service（QoS）などを慎重に設定することも重要です。Unified Communications ソリューションの全般的な設計上の考慮事項の詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

Unified Communications システムでのコンタクト センター配置には、通常、さらに次のような帯域幅の要件があります。

- エージェントが処理するトラフィック量のほうが、標準的なユーザが処理するトラフィック量よりも多いこと、その結果、音声およびシグナリング トラフィックもエージェントのほうが多いこと。
- エージェントとスーパーバイザが、画面ポップアップ、レポート、統計などの機能が搭載されたデスクトップを使用していること。この場合、エージェントまたはスーパーバイザのデスクトップとコンタクト センター サーバの間のデータ トラフィックが発生します。また、たとえばエージェントまたはスーパーバイザがリモートにあり、中央にあるサーバからデータをプルする場合は、帯域幅の計算でレポーティング情報を考慮する必要があります。詳細およびガイダンスについては、http://www.cisco.com/go/ucsrnd で入手可能な個別の Cisco Contact Center 製品の設計ガイドを参照してください。
- IVR ソリューションのタイプによっては、音声ゲートウェイと IVR システムの間にトラフィックが発生することがあります。たとえば、音声ゲートウェイが分散されており、Unified IP IVR を使用するリモート サイトに配置された音声ゲートウェイにコールが到着した場合、音声ゲートウェイと Unified IP IVR の間に WAN 経由の音声トラフィックが発生します。Unified CVP を使用すると、コールをリモート サイトでキューイングできます。この場合、VXML ゲートウェイがコール トリートメントとキューイングを提供し、それにより WAN 経由の IVR の音声トラフィックを回避して、全体的な WAN 帯域幅要件を低減します。

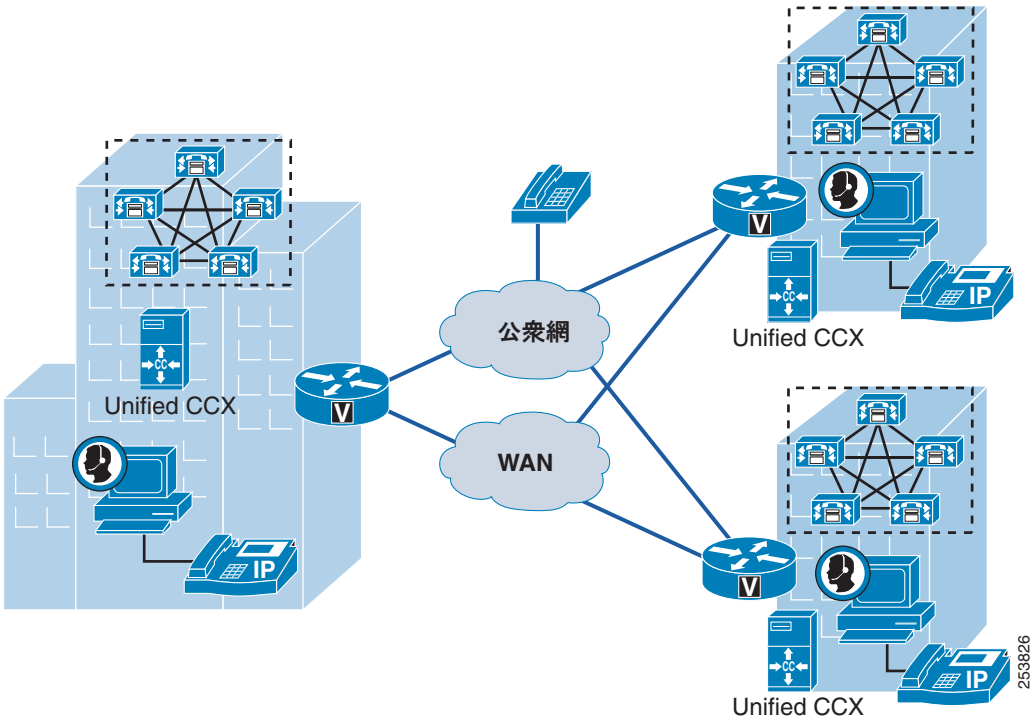
リモート エージェント（たとえば、自宅勤務のエージェントなど）も、Cisco Unified Contact Center でサポートされます。主に 2 つのソリューションがあります。1 つめのソリューションでは、エージェントは、ブロードバンド インターネット接続により中央サイトに接続された IP Phone を使用する必要があります。このソリューションでは、電話機は Cisco Unified Contact Center アプリケーションにより CTI 制御されます。2 つめのソリューションは、Cisco Unified Mobile Agent に基づいています。これにより、エージェントは、携帯電話などの任意の公衆網電話機を使用してコール センターに参加できます。

分散型コール処理を使用するマルチサイト コンタクト センター

分散型コール処理を使用するマルチサイト配置は、複数のサイトで構成されます。それぞれのサイトに、IP WAN に接続された独自のコール処理クラスタがあります。この項では、各 Unified CM クラスタにエージェントが登録されていることを前提としています。

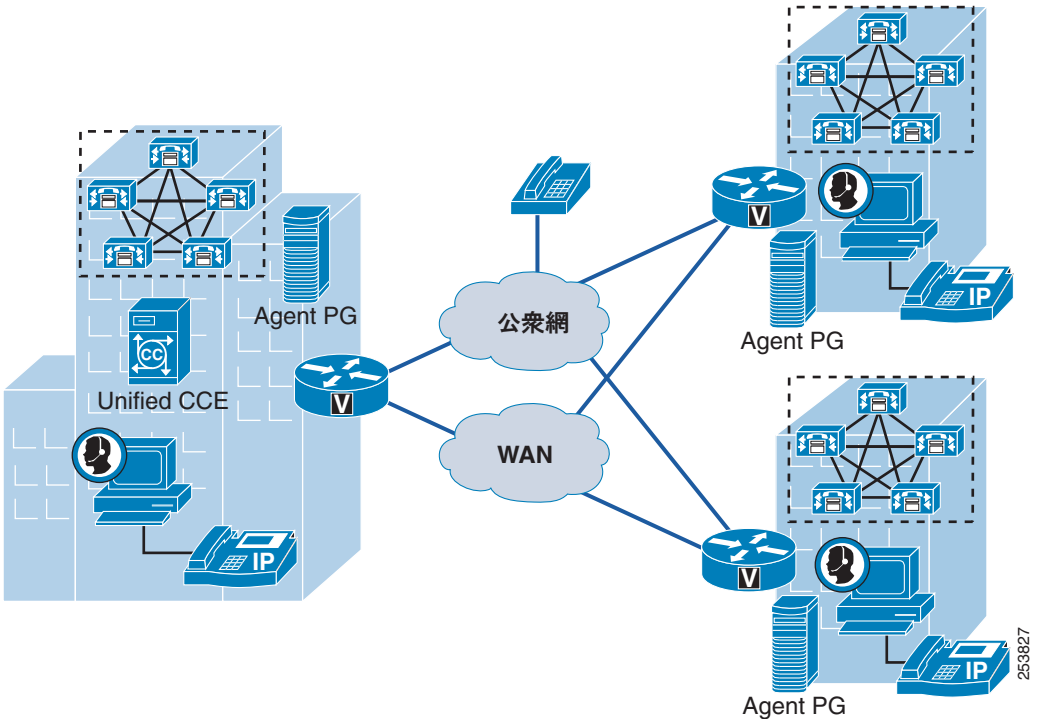
1 つの Unified CCX 配置を複数の Unified CM クラスタ間で共有することはできません。図 26-2 に示すように、各 Unified CM クラスタにそれぞれの Unified CCX 配置が必要です。

図 26-2　　分散型コール処理を使用するマルチサイト Unified CCX 配置



Unified CCE の要件は、Unified CCX の要件とは異なります。1 つの Unified CCE システムは、複数の地理的なロケーションに分散された複数の Unified CM クラスタにまたがることができます。Unified CCE Agent PG は、それぞれの Unified CM クラスタ ロケーションにインストールする必要があります。Unified CCE Central Controller（Call Router + Logger）から物理的にリモートにすることもできます。図 26-3 に、このタイプの配置を示し、Agent PG の位置を示します。

図 26-3　分散型コール処理を使用するマルチサイト Unified CCE 配置



複数のコンタクト センター配置が必要な場合は、Unified ICM を介してこれらの配置を接続します。このためには、親子配置モデルを使用して、単一の仮想コンタクト センターを構成します。親子モデルを使用すると、すべてのコンタクト センター配置にわたってエンタープライズ キューイングとエンタープライズ レポーティングを実行できるなど、複数のメリットがあります。また、サイトが完全な冗長構成となるため、スケーラビリティが向上します。親子モデルの詳細については、次の各マニュアルを参照してください。

- 次の URL で入手可能な『*Cisco Unified Contact Center Enterprise SRND*』
  http://www.cisco.com/go/ucsrnd
- 次の URL で入手可能な『*Cisco Contact Center Gateway Deployment Guide for Cisco Unified ICME/CCE/CCX*』
  http://www.cisco.com/en/US/products/sw/custcosw/ps1001/prod_installation_guides_list.html

分散型コール処理を使用するマルチサイト配置でも、集中型コール処理を使用するマルチサイト モデルの場合と同様に、QoS、コール アドミッション制御、コーデックなどを慎重に設定する必要があります。

IP WAN を介したクラスタリング

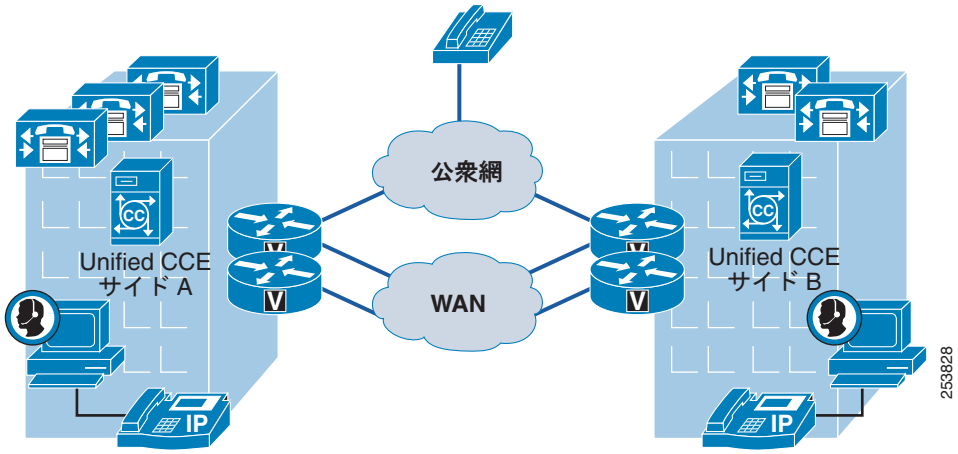
この配置モデルでは、単一の Unified CM クラスタが、QoS 機能が有効になっている IP WAN により接続された複数のサイトにわたって配置されます。このモデルを使用すると、Cisco Unified Contact Center ソリューションを配置できます。実際には、Cisco Unified Contact Center コンポーネント自体を WAN 経由でクラスタ化することもできます。

たとえば、Unified CCE を使用すると、サイト A サーバを Unified CCE のサイド B サーバからリモートにし、IP WAN 接続によってサイド B サーバから分離できます（Unified CCE のハイ アベイラビリティの詳細については、「コンタクト センターのハイ アベイラビリティ」（P.26-12）を参照してください）。このタイプの配置には、次の設計上の考慮事項があります。

- 2 つのサイト間の IP WAN は、単一障害点のないハイ アベイラビリティ構成にする必要があります。たとえば、IP WAN リンク、ルータ、およびスイッチは冗長構成にする必要があります。WAN リンクを冗長構成にするには、複数の WAN リンクを使用するか、復元性が高く冗長性が組み込まれている SONET リングを使用します。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。
- Agent Peripheral Gateway（Agent PG）は、接続先の CTI Manager サーバと同じ場所に設置する必要があります。Unified CCE を配置する際は、大量のリダイレクト トラフィックと転送トラフィック、および追加の CTI トラフィックがあるため、Unified CM サーバ間の Intra-Cluster Communication Signaling（ICCS）帯域幅の要件が高くなります。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。
- 1 つのサイトに Unified CCE プライマリ サーバと Unified CM プライマリ サーバを配置して、別のサイトに Unified CCE セカンダリ サーバと Unified CM セカンダリ サーバを配置した場合、2 つのサイト間の最大遅延は、Unified CM の遅延要件（Round Trip Time [RTT; ラウンドトリップ時間]）が 80 ms）によって決まります。ただし、Unified CCE サーバが Unified CM サーバとは別のロケーションに配置されている場合は、Unified CCE 冗長サーバ間の遅延がさらに大きくなる可能性があります。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。

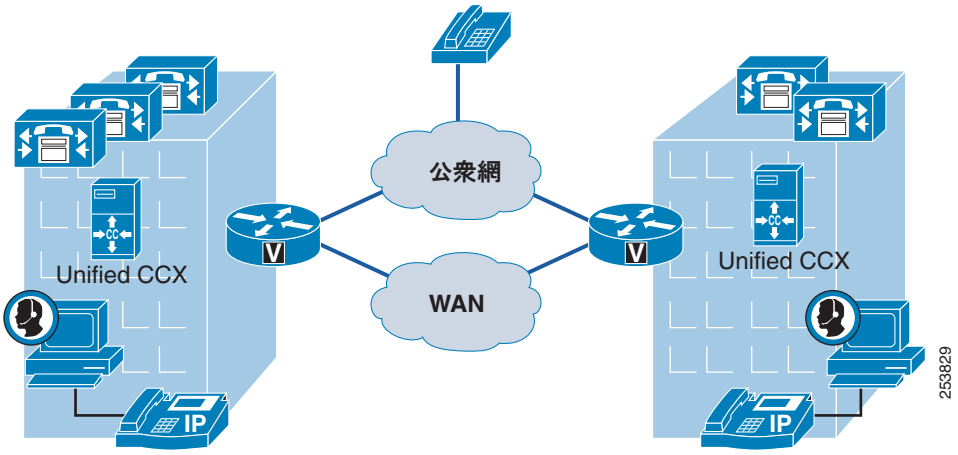
図 26-4 は、WAN 経由のクラスタリングを使用する Unified CCE の配置を示しています。

図 26-4　　WAN 経由のクラスタリングを使用する Unified CCE 配置



Unified CCX ソリューションおよび Unified IP IVR ソリューションを使用すると、Unified CCX プライマリ サーバまたは Unified IP IVR プライマリ サーバをバックアップ サーバからリモートにすることもできます。Unified CCX 配置の要件は、Unified CCE 配置の要件とは異なります。たとえば、Unified CCX では冗長な WAN リンクは必要ありません。また、Unified CCX のプライマリ サーバとバックアップ サーバの間の最大遅延は、80 ms RTT です。図 26-5 はこのタイプの展開を示しています。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCX SRND』を参照してください。

図 26-5　WAN 経由のクラスタリングを使用する Unified CCX 配置



Unified Expert Advisor では、Unified Communications コンポーネント（Unified CM や Unified CCE など）が WAN 経由でクラスタ化されている配置をサポートしますが、Unified Expert Advisor のプライマリ ランタイム サーバとバックアップ ランタイム サーバは同じサイトに配置する必要があります。

コンタクト センターを配置する際の設計上の考慮事項

この項では、コンタクト センターを配置する際の次の主要な設計上の考慮事項について簡単に説明します。

- 「コンタクト センターのハイ アベイラビリティ」（P.26-12）
- 「帯域幅、遅延、および QoS に関する考慮事項」（P.26-13）
- 「コール アドミッション制御」（P.26-14）
- 「Unified CM との統合」（P.26-15）
- 「コンタクト センターのその他の設計上の考慮事項」（P.26-16）

コンタクト センターのハイ アベイラビリティ

すべての Cisco Unified Contact Center 製品は、ハイ アベイラビリティを提供します。たとえば、Unified CCX または Unified IP IVR を Unified CM と統合する場合、別の Unified CCX または Unified IP IVR サーバを追加すると、ハイ アベイラビリティが実現されます。1 台のサーバがアクティブ サーバとなり、すべてのコール処理を取り扱います。もう 1 台のサーバはスタンバイ モードとなり、プライマリ サーバに障害が発生したときだけアクティブになります。また、Unified CVP は、複数の Unified CVP サーバ、音声ゲートウェイ、VXML ゲートウェイ、SIP プロキシなどを使用するハイ アベイラビリティ配置をサポートしています。

Unified CCE では、ほとんどのサーバは冗長構成にする必要があります。冗長インスタンスは、サイド A インスタンスおよびサイド B インスタンスと呼ばれます。たとえば、Call Router A および Call Router B は、2 つの異なるサーバ上で稼動する Call Router モジュール（プロセス）の冗長インスタンスです。この冗長構成は、*デュプレックス モード*とも呼ばれます。Call Router は 2 台のサーバで同期して実行されます。つまり、すべてのコールは、二重サーバの両サイドで処理されています。他のコンポーネント（ペリフェラル ゲートウェイなど）は、ホットスタンバイ モードで稼動します。つまり、常にペリフェラル ゲートウェイのうち 1 つだけがアクティブな状態となります。

Unified Contact Center コンポーネントそのものを冗長構成にするだけでなく、Unified Contact Center コンポーネントと Unified CM との統合を冗長構成にすることもできます。たとえば、Unified CCX サーバまたは Unified IP IVR サーバそれぞれをプライマリ CTI Manager に接続し、さらにプライマリ CTI Manager の障害発生時に備えてバックアップ CTI Manager にも接続できます。Unified CCE を使用して、PG サイド A をプライマリ CTI Manager に接続し、冗長な PG サイド B をセカンダリ CTI Manager に接続することで、1 つの CTI Manager に障害が発生した場合のハイ アベイラビリティが実現されます。

詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

帯域幅、遅延、および QoS に関する考慮事項

この項では、マルチサイト コンタクト センター配置における WAN 帯域幅のプロビジョニング方法を、さまざまなタイプの呼制御トラフィックおよびリアルタイム音声トラフィックを考慮に入れて説明します。適切に帯域幅プロビジョニングおよび QoS を実装することは、コンタクト センター配置の成否を決める重要な要素であるため、遅延および QoS パラメータについて理解しておくことが重要です。

帯域幅のプロビジョニング

コンタクト センター ソリューションは、次の主要なタイプのトラフィックに対応できる十分な WAN 帯域幅を必要とします。

- 着信ゲートウェイと IVR システムの間の音声トラフィック。Unified IP IVR を使用する場合、Unified IP IVR サーバが中央に配置され、公衆網ゲートウェイがリモートに配置されていると、WAN 経由の音声トラフィックが発生します。Unified CVP を使用する場合、エッジでコールをキューイングできます。このため、音声トラフィックをリモート サイトに対してローカルに保ち、WAN リンクを介する音声トラフィックを回避できます。
- 着信ゲートウェイとエージェントの間の音声トラフィック。
- 音声シグナリング トラフィック。これは通常、着信ゲートウェイと Unified CM の間、およびエージェント電話機と Unified CM の間のシグナリング トラフィックに対応します。
- Unified CVP が配置されている場合の VXML ゲートウェイ トラフィック。このトラフィックには、メディア サーバからのメディア ファイル取得や、VXML サーバとの間で交換される VXML ドキュメントが含まれます。
- エージェントまたはスーパーバイザのデスクトップと Unified Contact Center サーバの間のデータ トラフィック（CAD または CTI-OS トラフィック）。
- レポーティング ユーザと Unified Contact Center Reporting サーバの間のレポーティング トラフィック。
- Unified Contact Center サーバ間のトラフィック（サーバどうしがリモートに配置されている場合）。たとえば、このタイプのトラフィックは、IP WAN 経由またはマルチサイトでのクラスタリングや、Unified CCE Central Controller からリモートの PG を使用して分散コール処理を行う場合に発生します。

- 大量のリダイレクト トラフィックと転送トラフィック、および追加の CTI トラフィックによって Unified CM サブスクライバ間に発生する、追加の Intra-Cluster Communication Signaling（ICCS）トラフィック。
- 録音とサイレント モニタリングによる音声トラフィック。ソリューションによっては、エージェントとの会話をサイレントにモニタリングまたは録音する目的で、1 つまたは 2 つの RTP ストリームを送信できます。

帯域幅の計算とガイドラインについては、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

遅延

エージェントおよびスーパーバイザは、コール処理サーバおよびコンタクト センター サーバからリモートな場所に配置できます。技術的には、CTI OS サーバと CTI OS クライアント間の遅延は、CAD サーバと CAD/CSD デスクトップ間の遅延と同じく、タイムアウト値が大きいために、非常に長くなる可能性があります。遅延時間が長いと、ユーザ エクスペリエンスに影響し、混乱が発生したり、ユーザに許容されない状態となることがあります。たとえば、電話が鳴り出していても、デスクトップが更新されるのはあとになってからということがあります。

コンタクト センターのコンポーネントとコール処理サーバの間、およびコンタクト センターのコンポーネント間の遅延の要件は、コンタクト センターのソリューションによって異なります。たとえば、Unified CCX 冗長サーバは互いにリモートの場所に配置でき、最大遅延は 80 ms RTT です。Unified CCE を使用する場合、Unified CCE サーバと Unified CM の間、または Unified CCE 各サーバ間の最大遅延は、80 ms RTT より大きくなります。

詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

QoS

他の Unified Communications コンポーネントを使用する配置と同様に、コンタクト センター配置でも、時間に依存するトラフィックや重要なトラフィックを優先させるために、Quality of Service（QoS）の設定が必要となります。コンタクト センター環境における音声および音声シグナリング用の QoS マーキングは、他の Unified Communications 配置の場合と同じです。コンタクト センターに固有のトラフィックは、特定の QoS マーキングを使用してマークする必要があります。たとえば、Unified CCE プライベート ネットワークのトラフィックには、AF31 としてマークする必要のあるものや、AF11 としてマークする必要のあるものがあります。QoS マーキングの推奨値および QoS 設計ガイドラインについては、Unified Contact Center ソリューションごとに、http://www.cisco.com/go/ucsrnd で入手可能な個別の『Cisco Unified Contact Center SRNDs』を参照してください。

コール アドミッション制御

他の Unified Communications コンポーネントを使用する配置と同様に、コンタクト センター配置でも、コール アドミッション制御を慎重にプロビジョニングする必要があります。「コール アドミッション制御」（P.11-1）の章に記載されているメカニズムが、コンタクト センター環境にも適用されます。

コール アドミッション制御の計算では、サイレント モニタリングと録音に関連する音声トラフィックが考慮されないことがあります。たとえば、Unified CM によるサイレント モニタリングと録音で発生する音声トラフィック（電話機で分岐（転送）される音声トラフィック）は、コール アドミッション制御の計算で適切に考慮されますが、デスクトップベース（エージェント IP Phone の背面に接続されているデスクトップ）のサイレント モニタリングで発生する音声トラフィックは考慮されません。

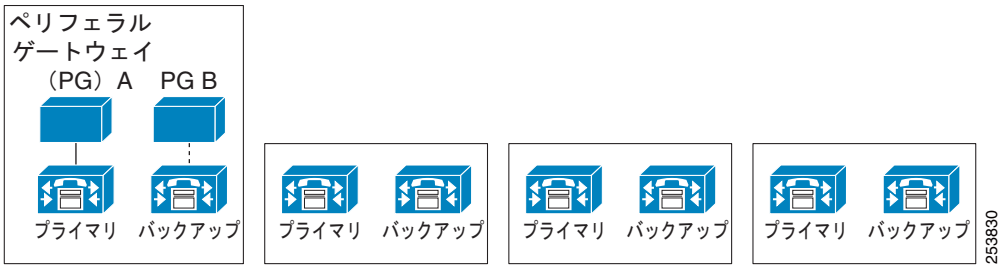
Mobile Agent および Unified CVP のコール アドミッション制御には、特別の考慮事項が適用されます。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

Unified CM との統合

Cisco Unified Contact Center コンポーネントを Unified CM と統合する際は、次の設計上の考慮事項に従ってください。

- 管理およびアップグレードの目的で、コンタクト センター配置とコンタクト センター以外の配置に対しては、別々の Unified CM クラスタを使用することを推奨します。別々のクラスタを使用できない場合は、コンタクト センターのアプリケーションとコンタクト センター以外のアプリケーションに別々の Unified CM サブスクライバ サーバを使用することを推奨します。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。
- コンタクト センター配置で Unified CM サーバに対して 2:1 冗長スキームを使用することは推奨しません。高い復元性と高速なアップグレードを実現するために、1:1 の冗長構成を使用してください。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。
- Unified CM と Unified CCX、Unified IP IVR、または Unified CCE の間の統合は、JTAPI を介して行います。Unified CCX サーバは、プライマリ CTI Manager に接続します。また、セカンダリ CTI Manager へのバックアップ接続もあります。Unified CCE を使用する場合、Agent PG は 1 つだけの CTI Manager に接続します。冗長な Agent PG は、バックアップ CTI Manager だけに接続します。プライマリ CTI Manager に障害が発生すると、プライマリ Agent PG にも障害が発生し、フェールオーバーがトリガーされます。
- Unified CCE PG を使用して CTI Manager を配置するには、いくつかの方法があります。たとえば、4 つの Unified CM サブスクライバ ペアを必要とする Unified CCE 配置においては、4 つの Agent PG を配置し、それぞれの Agent PG を、同様に CTI Manager サービスを実行している別々の Unified CM サブスクライバ ペアに接続できます。あるいは、単一の PG を、CTI Manager サービスを実行している Unified CM サブスクライバ ペアの 1 つだけに接続することもできます。この Unified CM ペアを介して、PG は 4 つすべての Unified CM サブスクライバ ペアのエージェント電話機を制御またはモニタできます。図 26-6 は、この設定を示しています。集中型配置においては、このような設定が一般的です。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCE SRND』を参照してください。
- 複数の Unified CCX を単一の Unified CM クラスタと統合することは可能です。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Unified CCX SRND』を参照してください。

図 26-6　　1 つの Agent PG と 4 つの Unified CM サブスクライバ ペアを使用する配置



コンタクト センターのその他の設計上の考慮事項

示された状況においては、次の設計上の考慮事項が追加で適用されます。

- Unified CVP ではエッジでのキューイングが可能であるため、Unified IP IVR ではなく Unified CVP を配置すれば、マルチサイト配置の帯域幅の要件を小さくできます。
- Cisco Unified Contact Center 製品およびコンポーネントのほとんどは、VMware をベースにした仮想化環境にインストールできます。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な個別の Cisco Unified Contact Center の SRND を参照してください。
- シナリオによっては、Media Termination Point（MTP; メディア ターミネーション ポイント）リソースが必要となることもあります。たとえば、Mobile Agent を使用する場合、RFC 2833 がネゴシエートされるときに、関連付けられた CTI ポートに対して MTP が必要となります。また、Unified CVP を使用するシナリオでも、MTP が必要となることがあります。詳細については、http://www.cisco.com/go/ucsrnd で入手可能な個別の Cisco Unified Contact Center の SRND を参照してください。
- Unified CM では、一部のサードパーティ製コンタクト センター製品もサポートされています。Unified CM との統合は JTAPI に基づいて行うことができます。また、コール トリートメントとキューイングおよび CTI ルート ポイントに対して CTI ポートを使用できます。Unified CM のサイズを適切に設定するには、コール フローとそれが Unified CM に与える影響をよく理解することが重要です。また、冗長構成の実装方法と、それが Unified CM または CTI のスケーラビリティに影響するかどうかも理解しておくことが重要です。

コンタクト センターのキャパシティ プランニング

すべての配置は、Cisco Unified Communications Sizing Tool（Unified CST）を使用してサイジングする必要があります。このツールは、コンタクト センター製品（Unified CCE、Unified IP IVR、Unified CVP、Unified CCX、Expert Advisor など）のサイジングを実行します。このツールによって、配置に必要なコンタクト センター リソース（エージェント数、IVR ポート数、ゲートウェイ ポート数など）が決定されます。コンタクト センター コンポーネントそのもののサイジングだけでなく、Unified CM や音声ゲートウェイを含む Unified Communications の残りの要素のサイズも決定されます。このツールは、シスコの従業員およびパートナーだけが（適切なログイン認証を使用して）、http://tools.cisco.com/cucst から入手できます。

一般に、コンタクト センターのサイジングには、コンタクト センターへの着信コールの Busy Hour Call Attempts（BHCA; 最繁時呼数）が大きく影響します。また、[Service Level Goal] や [Target Answer Time] などの他のパラメータも影響を与えます。たとえば、コールの 90% を 30 秒以内に応答処理する必要のある配置では、コールの 80% を 2 分以内に応答処理する必要のある配置よりも多くのコンタクト センター リソースが必要となります。この他に、CAD または CTI OS を使用するかどうかもサイジングに影響を与えるパラメータです。これによって、Agent PG のスケーラビリティに違いが出る可能性があります。サイジングに Unified CST を使用し、http://www.cisco.com/go/ucsrnd で入手可能な個別の Cisco Unified Contact Center の SRND で詳細情報を参照してください。

また、コンタクト センターの設計も、Unified CM サイジングに影響を与えます。コンタクト センター ソリューション内に配置される Unified CM のサイジングには、次の考慮事項が適用されます。

- 単一の Unified CM クラスタ内の Unified CCE エージェントの最大数は、IVR ソリューションによって異なります。Unified IP IVR を使用する場合、コール トリートメントとキューイング中に CTI ルート ポイントおよび CTI ポートが使用されます。これにより、Unified CM リソースが消費されます。Unified CVP を使用する場合、コール トリートメントとキューイングは通常、VXML ゲートウェイ、Unified CVP VXML サーバ、および Unified CVP コール サーバによって処理されます。これによる Unified CM への影響はありません。したがって、Unified IP IVR よりも Unified CVP を使用したほうが、単一の Unified CM クラスタでサポートできるエージェント数が多くなります。

- Unified CCE Mobile Agent 機能は CTI ポートに依存しているため、Unified CM サブスクライバからの追加のリソースが必要となります。したがって、Mobile Agent を配置した場合は、Unified CM のスケーラビリティが低下します。
- Unified CCE を配置する場合、2 つのタイプの発信ダイヤラが使用可能です。SCCP ダイヤラを使用する場合、ダイヤラ ポートが Unified CM に登録されます。発信コールがアクティブなカスタマーに到達しない場合でも、各発信コールには Unified CM が関連します。SIP ダイヤラを使用する場合、各発信コールは SIP ダイヤラ ポートから直接、発信音声ゲートウェイに送信されます。SIP ダイヤラを使用する場合は、コールはエージェントに転送されて初めて、Unified CM に到達します。したがって、SIP ダイヤラを使用すると、Unified CM のキャパシティははるかに大きくなります。
- Unified CM のサイジングを行う際には、追加の CTI アプリケーションを考慮に入れることも重要です。たとえば、一部の PC クライアントは、CTI を介してリモートから電話機を制御できます。また、一部のコール録音アプリケーションは、CTI Manager を使用して直接 Unified CM と統合できます。さらに、エージェント電話機をモニタできるものもあります。これには、Unified CM からの追加のリソースが必要となることがあります。詳細については、「コンピュータ テレフォニー インテグレーション（CTI）」（P.8-37）と、http://www.cisco.com/go/ucsrnd で入手可能な Cisco Unified Contact Center の SRND を参照してください。
- Unified CM からのリソースを消費するサイレント モニタリングと録音ソリューションもあれば（Unified CM をベースにしたサイレント モニタリングや録音機能など）、消費しないソリューションもあります（SPAN またはデスクトップ サイレント モニタリングと録音など）。
- 繰り返しますが、サイジングは複雑であるため、すべての配置は Cisco Unified Communications Sizing Tool を使用してサイジングする必要があります。このツールは、シスコの従業員とパートナーだけが（適切なログイン認証を使用して）、http://tools.cisco.com/cucst から入手できます。

詳細については、http://www.cisco.com/go/ucsrnd で入手可能な『Cisco Unified Contact Center SRNDs』を参照してください。

ネットワーク管理ツール

Unified CCE は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して管理します。Unified CCE デバイスは、SNMP v1、v2c、および v3 をサポートする組み込み型の SNMP エージェント インフラストラクチャを持ち、CISCO-CONTACT-CENTER-APPS-MIB により定義された計測手段を公開します。この MIB により、標準の SNMP 管理ステーションでモニタ可能な構成、検出、および状態の計測手段が提供されます。さらに、Unified CCE は、管理者にシステムの障害があれば警告する豊富な SNMP 通知セットを提供します。また、Unified CCE は、より詳細なイベント セットを必要とする管理者に対して、（RFC 3164 に準拠する）標準的な syslog イベント フィードも提供します。

Unified CCE SNMP エージェント インフラストラクチャおよび syslog フィードの設定の詳細については、次のサイトで入手可能な『*SNMP Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』を参照してください。

http://www.cisco.com/en/US/products/sw/custcosw/ps1001/products_installation_and_configuration_guides_list.html

Unified CVP の状態モニタリングは、任意の SNMP 標準モニタリング ツールを使用して実行できます。これにより、ソリューション ネットワークの状態の詳細が表形式で視覚的に示されます。すべての Unified CVP 製品コンポーネントおよびほとんどの Unified CVP ソリューション コンポーネントは、標準的な SNMP 管理ステーションまたはモニタリング ツールに配信できる SNMP トラップおよび統計も発行します。

Unified CCX は、SNMP および syslog インターフェイスを使用して管理することもできます。

PART 5

Unified Communications 運用とサービス アビリティ

CHAPTER 27

Cisco Unified Communications の運用とサービスアビリティの概要

ネットワーク、コール ルーティング、呼制御インフラストラクチャ、およびアプリケーションとサービスが Cisco Unified Communications システム用に配置されたあとに、ネットワークとアプリケーションの管理コンポーネントをそのインフラストラクチャの最上位で追加または階層化できます。既存の Cisco Unified Communications インフラストラクチャに配置できる運用とサービスアビリティのアプリケーションとサービスは、数多く存在します。これらのアプリケーションとサービスは、次の 4 つの基本領域に分類できます。

- ユーザとデバイスのプロビジョニング サービス：ユーザとデバイスの集中型プロビジョニングおよび設定をユニファイド コミュニケーション アプリケーションとサービスで可能にします。
- 音声品質のモニタリングおよびアラート：システム内で発生するさまざまなコール フローを継続的にモニタして、音声品質が許容できるかどうかを判別し、音声品質が許容できない場合は、管理者に警告します。
- 運用と障害のモニタリング：アプリケーションとサービスのすべての処理を集中的にモニタして、ネットワークおよびアプリケーションの障害に関して管理者に警告します。
- ネットワークとアプリケーションのプローブ：配置全体のさまざまなロケーションでネットワークとアプリケーションのトラフィック情報をプローブおよび収集し、管理者が中央ロケーションでこの情報にアクセスし、取得できるようにします。

本 SRND のこのパートでは、上記で説明しているアプリケーションとサービスについて説明します。さまざまなネットワーク管理アプリケーションとサービスの概要を示したあと、アーキテクチャ、ハイアベイラビリティ、キャパシティ プランニング、および設計上の考慮事項について説明します。ここでは、アプリケーションおよびサービスの設計関連の側面を中心に説明します。製品固有のサポートおよび設定情報については、関連する製品マニュアルを参照してください。

本 SRND のこのパートには、次の章が含まれています。

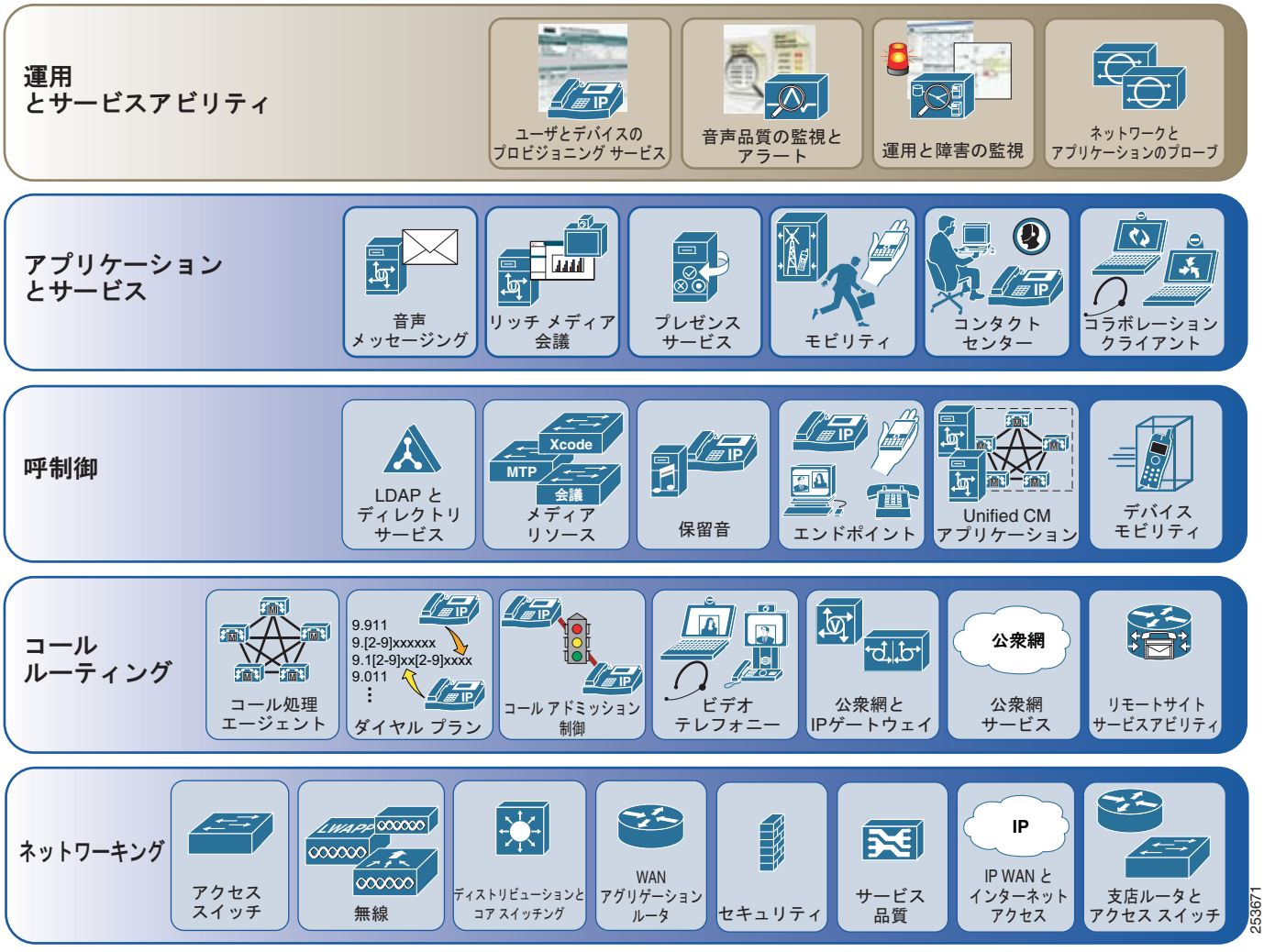
- 「ネットワーク管理」（P.28-1）

  この章では、ユニファイド コミュニケーション ネットワークとアプリケーションの管理サービスについて説明します。これらのサービスは、ほとんどのユニファイド コミュニケーション配置で一般的に普及しているサービス セットです。これらの管理サービスにより、管理者はユーザとデバイスをプロビジョニングおよび設定し、ネットワークとアプリケーションの動作および音声品質をモニタし、問題が発生したときにアラートとアラームを受信できます。また、この章では、配置モデルに対するこれらの管理アプリケーションとサービスの影響についても説明し、ネットワークとアプリケーションの管理サービスおよびアプリケーションに関する設計と配置のベスト プラクティスを示します。

アーキテクチャ

他のネットワークおよびアプリケーション テクノロジー システムの場合と同様、運用とサービスアビリティのアプリケーションおよびサービスは、基盤となるネットワーク インフラストラクチャ、システム インフラストラクチャ、およびアプリケーション インフラストラクチャの最上位で階層化して、これらのインフラストラクチャをモニタおよび制御できるようにする必要があります。図 27-1 は、Cisco Unified Communications システム アーキテクチャ全体におけるユニファイド コミュニケーションの運用とサービスアビリティの論理的ロケーションを示しています。

図 27-1　Cisco Unified Communications の運用とサービスアビリティのアーキテクチャ



ユニファイド コミュニケーションの運用とサービスアビリティ サービス（ユーザとデバイスのプロビジョニング、音声品質のモニタリングおよびアラート、運用と障害のモニタリング、ネットワークとアプリケーションのプローブなど）はすべて、運用とサービスアビリティのさまざまなアプリケーションおよびプローブにネットワーク接続するために、基盤のネットワーク インフラストラクチャを使用します。ユニファイド コミュニケーションのコール ルーティングと呼制御のインフラストラクチャ、またはユニファイド コミュニケーションのアプリケーションとサービスとの直接の依存関係はありませんが、これらのインフラストラクチャおよびアプリケーションは、さまざまな運用サービスや管理サービスが実際に管理および制御する対象となります。たとえば、ユーザとデバイスのプロビジョニング

サービスと、モニタリングおよびアラートの各種サービスでは、さまざまなユニファイド コミュニケーションのアプリケーションとサービス ノードに接続するためにネットワーク インフラストラクチャを利用して、さまざまなコンポーネントおよび動作を設定およびモニタします。また、これらのサービスでは、コンポーネント（コール処理エージェント、公衆網ゲートウェイと IP ゲートウェイ、メディア リソース、エンドポイントなど）および（音声メッセージング、リッチ メディア会議、およびコラボレーション クライアント用の）各種ユニファイド コミュニケーション アプリケーションに関して、直接対話したり、場合によっては設定の変更やアラートの受信を行います。これらのインフラストラクチャ レイヤおよび基本的なユニファイド コミュニケーションのサービスとアプリケーションに依存する以外に、運用とサービスアビリティに関連するそれぞれのサービスは、多くの場合、完全に機能するために相互依存もしています。

ハイ アベイラビリティ

ネットワーク、コール ルーティング、呼制御の各インフラストラクチャ、および重要なユニファイド コミュニケーションのアプリケーションとサービスの場合と同様、ユニファイド コミュニケーションの運用とサービスアビリティ サービスは、ネットワークやアプリケーションに障害が発生した場合でも必要なプロビジョニング、モニタリング、およびアラートが引き続き実行されるように、ハイ アベイラビリティを実現する必要があります。発生する可能性のあるさまざまなタイプの障害、およびこれらの障害に関する設計上の考慮事項を理解することが重要となります。ユニファイド コミュニケーションの運用とサービスアビリティ コンポーネントは、他のコンポーネントやサービスに依存していることから、場合によっては、運用と管理の単一アプリケーションまたはサービスの障害が、複数のサービスに影響を及ぼすことがあります。たとえば、ネットワーク管理配置のさまざまなアプリケーション サービス コンポーネントが適切に機能できる一方で、ネットワーク接続の切断または障害が発生すると、冗長ネットワーク プローブが別の接続パスとともに配置されていない限り、ネットワーク プローブはネットワークの正常性または音声品質をモニタできなくなります。

ユーザとデバイスのプロビジョニングなどの運用とサービスアビリティ機能の場合、ハイ アベイラビリティに関する考慮事項には、ネットワーク接続またはアプリケーション サーバの障害による一時的な機能の喪失によって、管理者がユーザとデバイスをプロビジョニングできなくなったり、ユーザ アカウントまたはデバイス設定を変更できなくなることが含まれます。また、これらのタイプの運用のフェールオーバーに関する考慮事項には、特定の障害が発生した場合に、管理者が一部の設定変更を引き続き実行できるように、冗長な運用または管理のアプリケーションによって一部の機能を処理できるようにするというシナリオが含まれます。

音声品質をモニタしたり、障害をモニタするためのサービスを提供する運用とサービスアビリティのアプリケーションについても、冗長化することを考慮する必要があります。ネットワークの接続が妨げられたり、サーバやアプリケーションに障害が発生した場合は、モニタや警告に関する機能が縮退したり、場合によっては、これらの機能が完全に失われます。これは、音声品質のモニタリングにおいては、コールフローやデバイスに関する音声品質の測定ができなくなる場合があることを意味します。運用と障害モニタリング サービスにおいては、設定変更された内容を追跡するためのデータや、障害の発生を示すのアラートやインジケータが損失してしまう可能性も考慮して冗長化を行う必要があります。

キャパシティ プランニング

ネットワーク、コール ルーティング、および呼制御の各インフラストラクチャ、およびユニファイド コミュニケーションのアプリケーションとサービスは、個々のコンポーネントおよびシステム全体のキャパシティとスケーラビリティを理解して設計および配置する必要があります。同様に、運用とサービスアビリティのコンポーネントとサービスの配置についても、キャパシティとスケーラビリティの考慮事項に注意して設計する必要があります。運用とサービスアビリティの各種アプリケーションとコンポーネントを配置する場合は、アプリケーション自体のスケーラビリティの考慮が重要となるだけでな

く、基盤となるインフラストラクチャのスケーラビリティについても考慮する必要があります。ネットワーク インフラストラクチャは、使用可能な帯域幅を持ち、運用によって発生する追加のトラフィック負荷を処理できる必要があります。同様に、コール ルーティングと呼制御インフラストラクチャでは、使用中のさまざまな運用とサービスアビリティ コンポーネントによって実施される、必要な入力と出力を処理できる必要があります。たとえば、音声品質のモニタリングやアラート、運用と障害のモニタリングなどの運用アプリケーションとサービスでは、所定の時間にモニタできるデバイスやコール フローの数に関して、これらの個々のアプリケーションやサービスに対するキャパシティの暗黙的要件がありますが、モニタとアラートの実行に必要となる、追加のネットワーク トラフィックおよび接続を処理するための、基盤となるインフラストラクチャおよびモニタ対象アプリケーションのスケーラビリティも、同様に重要となります。モニタおよびアラートのアプリケーションやサービス自体が多数のネットワーク デバイスやコール フローをサポートできる場合でも、基盤となるネットワークやデバイスが、接続のプローブ、またはモニタリングおよびアラート サービスによって生成されたアラーム メッセージング負荷を処理できるキャパシティを持っていない場合があります。

ユーザまたはデバイスのプロビジョニング機能を提供する運用アプリケーションまたはサービスの場合、キャパシティ プランニングの考慮事項には、プロビジョニング アプリケーションが要求された負荷を処理できること、およびユーザまたはデバイスのプロビジョニング処理が、特定の基盤ユニファイド コミュニケーションのアプリケーションとサービスでサポートされているデバイスまたはユーザの数を超えないことを保証するだけでなく、プロビジョニングまたは設定変更のトランザクションが、基盤ネットワークのキャパシティ、または特定のアプリケーションでトランザクションを処理できる割合のいずれも超えないことを保証することが含まれます。基盤となるネットワーク インフラストラクチャ、およびコール ルーティングと呼制御のインフラストラクチャが追加の負荷を処理できると想定すると、ほとんどの場合、運用プロビジョニング アプリケーション サーバを増やしたり、基になるユニファイド コミュニケーションのアプリケーション インスタンスやサービス インスタンスを増やすことで、キャパシティを追加できます。

CHAPTER 28

ネットワーク管理

ネットワーク管理は、さまざまなツール、アプリケーション、および製品によって構成され、ネットワーク システム管理者による新規および既存ネットワーク配置のプロビジョニング、運営、モニタリング、および保守を支援します。ネットワーク管理者は、ネットワーク デバイスを配置および設定する場合、また、ネットワーク インフラストラクチャやルータ、サーバ、スイッチなどのコンポーネントの正常性を運用、モニタリング、および報告する場合に、さまざまな課題に直面します。ネットワーク管理は、システム管理者による各ネットワーク デバイスとネットワーク アクティビティのモニタを支援し、問題をタイムリーに特定および調査することで、性能と生産性を高めるのに役立ちます。

リッチ メディアとデータのコンバージェンスにより、統合管理の必要性は以前よりもさらに強まっています。Cisco Unified Communications Management Suite は、Cisco Unified Communications システムのテスト、配置、およびモニタを支援する統合ツール セットを提供します。ネットワーク管理者は、さまざまな管理段階を実装して、音声、ビデオ、コンタクト センター、リッチ メディア アプリケーションなどの Cisco Unified Communications アプリケーションの性能と可用性を戦略的に管理します。ネットワーク管理は一般的に、計画（Plan）、設計（Design）、実装（Implement）、および運用（Operate）（PDIO）の各段階からなります。表 28-1 に、PDIO 段階と各段階に含まれる主なタスクを示します。

表 28-1　　ネットワーク管理の段階およびタスク

計画および設計	実装	運用
Cisco Unified Communications 機能のネットワーク インフラストラクチャを見積もります。たとえば、全体的なコール品質を予測します。 Cisco Unified Communications をサポートするようにネットワークを準備します。 ネットワーク管理のベスト プラクティスを分析します。	Cisco Unified Communications を配置およびプロビジョニングします。たとえば、ダイヤル プラン、パーティション、ユーザ機能などを設定します。 既存インフラストラクチャの機能で Cisco Unified Communications をサポートできるようにします。たとえば、音声ポート、ルータのゲートウェイ機能などを設定します。	ユーザ、サービス、IP Phone などの変更を管理します。 運用、キャパシティ プランニング、エグゼクティブ サマリーなどのレポートを生成します。 ユーザ エクスペリエンスを監視および報告します。たとえば、音声品質をモニタするセンサーを使用します。 ネットワーク障害、デバイス障害、コール ルーティング問題などの問題をモニタおよび診断します。

この章では、Cisco Unified Communications Management の実装段階と運用段階に適用される次の管理ツールおよび製品の設計ガイドラインについて説明します。

- 実装および運用
  - Cisco Unified Provisioning Manager（Unified PM）は、IP コミュニケーション サービスの初期配置と運用開始のプロビジョニングを管理します。詳細については、http://www.cisco.com/en/US/products/ps7125/tsd_products_support_series_home.html で入手可能な関連製品のマニュアルを参照してください。
- 運用
  - Cisco Unified Operations Manager（Unified OM）は、Cisco Unified Communications システム全体の予防的および反応的な診断を備えた包括的なモニタリング機能を提供します。詳細については、http://www.cisco.com/en/US/products/ps6535/tsd_products_support_series_home.html で入手可能な関連製品のマニュアルを参照してください。
  - Cisco Unified Service Monitor（Unified SM）は、Cisco Unified Communications システムの音声品質をモニタおよび評価する信頼性の高い手段を提供します。詳細については、http://www.cisco.com/en/US/products/ps6536/tsd_products_support_series_home.html で入手可能な関連製品のマニュアルを参照してください。
  - Cisco Unified Service Statistics Manager（Unified SSM）は、Cisco Unified Communications の配置に関する高度な統計分析およびレポート機能を提供します。詳細については、http://www.cisco.com/en/US/products/ps7285/tsd_products_support_series_home.html で入手可能な関連製品のマニュアルを参照してください。

Cisco Unified Communications Manager（Unified CM）でサポートされているソフトウェア バージョンの詳細については、次の URL で入手可能な『*Cisco Unified Communications Manager Software Compatibility Matrix*』を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/compat/ccmcompmatr.html

この章の新規情報

表 28-2 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 28-2　新規情報、またはこのマニュアルの以前のリリースからの変更情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
トランク使用率	「トランク使用率」（P.28-11）	2011 年 6 月 2 日
Cisco Unified Analysis Manager	「Cisco Unified Analysis Manager」（P.28-21）	2010 年 4 月 2 日
Cisco Unified Reporting	「Cisco Unified Reporting」（P.28-22）	2010 年 4 月 2 日
Cisco Unified Operations Manager による、仮想化された Unified Communications システムのモニタリング	「Cisco Unified Operations Manager」（P.28-3）	2010 年 4 月 2 日

Cisco Unified Network Management アプリケーションのネットワーク インフラストラクチャ要件

適切に設計されたネットワークは、Cisco Unified Communications ネットワークを運用および管理するための基礎となります。次の厳しい要件に従うように Cisco Unified Communications ネットワークを設計することを強く推奨します。

- 平均の IP パケット損失 <= 1%
- 平均の遅延変動（ジッタ）<= 30 ms
- 平均の片方向パケット遅延 <= 150 ms

ネットワーク内の Domain Name Service（DNS; ドメイン ネーム サービス）でデバイスの IP アドレスに対してリバース ルックアップを実行して、デバイスのホスト名を取得できるようにする必要があります。DNS を使用しない場合は、IP アドレスからホスト名への解決にホスト ファイルを使用することもできます。

Network Time Protocol（NTP; ネットワーク タイム プロトコル）を実装して、ネットワーク デバイスのクロックをネットワーク タイム サーバまたはネットワーク対応クロックに同期できるようにする必要があります。NTP によって、ネットワーク中のデバイスのすべてのログ、トラップ、ポーリング、およびレポートのタイムスタンプが正確であることが保証されるため、NTP はネットワークの運用および管理に不可欠なネットワーク サービスです。

ネットワーク内の Cisco Discovery Protocol（CDP; シスコ検出プロトコル）で適切なモニタリングを確実にできるようにする必要があります。Unified OM の自動デバイス検出は、CDP テーブルに基づきます。CDP の代わりに Ping スイープを使用することもできますが、Ping スイープを使用して検出された IP Phone は「管理対象外」として報告されます。また、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）もネットワーク デバイス上で有効にして、Cisco Unified OM が設定済みのポーリング間隔でネットワーク デバイスの情報を取得したり、管理対象デバイスによって送信されたトラップ通知で警告および障害を受信したりできるようにする必要があります。

Cisco 1040 Sensor を使用する場合には、ネットワーク内で Trivial File Transfer Protocol（TFTP; トリビアル ファイル転送プロトコル）を有効にする必要があります。TFTP を使用することで Cisco 1040 sensor は設定ファイルをダウンロードできます。

Cisco Unified Communications ネットワークの詳細については、「ネットワーク インフラストラクチャ」（P.3-1）の章を参照してください。

Cisco Unified Operations Manager

Cisco Unified Operations Manager（Unified OM）は、Cisco Unified Communications インフラストラクチャ全体の統合ビューを提供して、Cisco Unified Communications ネットワークの各要素について現在の運用ステータスを示します。また、Unified OM は、問題を迅速に切り分けおよび解決するための診断機能も提供します。Cisco ゲートウェイ、ルータ、およびスイッチに加えて、Unified OM は、次のようなさまざまな Cisco Unified Communications 要素の運用ステータスも継続的にモニタします。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unified Communications Manager Express（Unified CME）
- Cisco Unified Communications Manager Session Management Edition
- Cisco Unity および Unity Connection
- Cisco Unity Express

- Cisco Unified Contact Center Enterprise（Unified CCE）、Unified Contact Center Express（Unified CCX）、および Unified Customer Voice Portal（Unified CVP）

（注）　Cisco Operations Manager のサービス レベル ビューでは、複数の Cisco Unified System Contact Center Enterprise（SCCE）の配置はサポートしていません。

- Cisco Unified Presence
- Cisco Emergency Responder
- Cisco Unified MeetingPlace および Unified MeetingPlace Express
- Cisco Unified IP Phone

（注）　Unified OM は、仮想化された環境での Unified Communications アプリケーションの実行をサポートしていますが、VMware のモニタリングは提供していません。

Unified OM でサポートされている製品およびバージョンの詳細については、次の URL で入手可能な Cisco Unified Operations Manager データ シートを参照してください。

http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html

Unified OM が Unified Communications の要素をモニタするために使用するプロトコルは、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）です。SNMP は、トランスポート レイヤ プロトコルとして UDP を使用するアプリケーション レイヤ プロトコルです。SNMP で管理されるネットワークには、次の 3 つのキーとなる要素があります。

- 管理対象デバイス：SNMP エージェントを持つネットワーク デバイス（Unified CM、ルータ、スイッチなど）。
- エージェント：管理対象デバイスに存在するネットワーク管理ソフトウェア モジュール。このエージェントは、デバイスのローカル管理情報を SNMP メッセージに変換します。
- マネージャ：管理ステーション上で実行され、ネットワーク内の別のエージェントに接続して管理情報を取得するソフトウェア（Unified OM など）。

SNMP の実装では、SNMP v1、SNMP v2c、および SNMP v3 の 3 つのバージョンがサポートされています。SNMP v3 は、認証、暗号化、およびメッセージの完全性をサポートしています。管理トラフィックにセキュリティが必要な場合は、SNMP v3 を使用できます。Unified OM は、SNNP の 3 つのバージョンすべてをサポートしています。エージェントとマネージャが正常に通信するには、各デバイスに SNMP v1 および v2c のリード/ライト（read/write）コミュニティ ストリングまたは SNMP v3 のクレデンシャルを設定する必要があります。Unified OM に必要なのは、ネットワーク デバイス情報を収集するための SNMP 読み取りアクセスだけです。

SNMP の詳細については、次の URL で入手可能な『*User Guide for Cisco Unified Operations Manager*』を参照してください。

http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html

Cisco Unified Operations Manager の設計に関する考慮事項

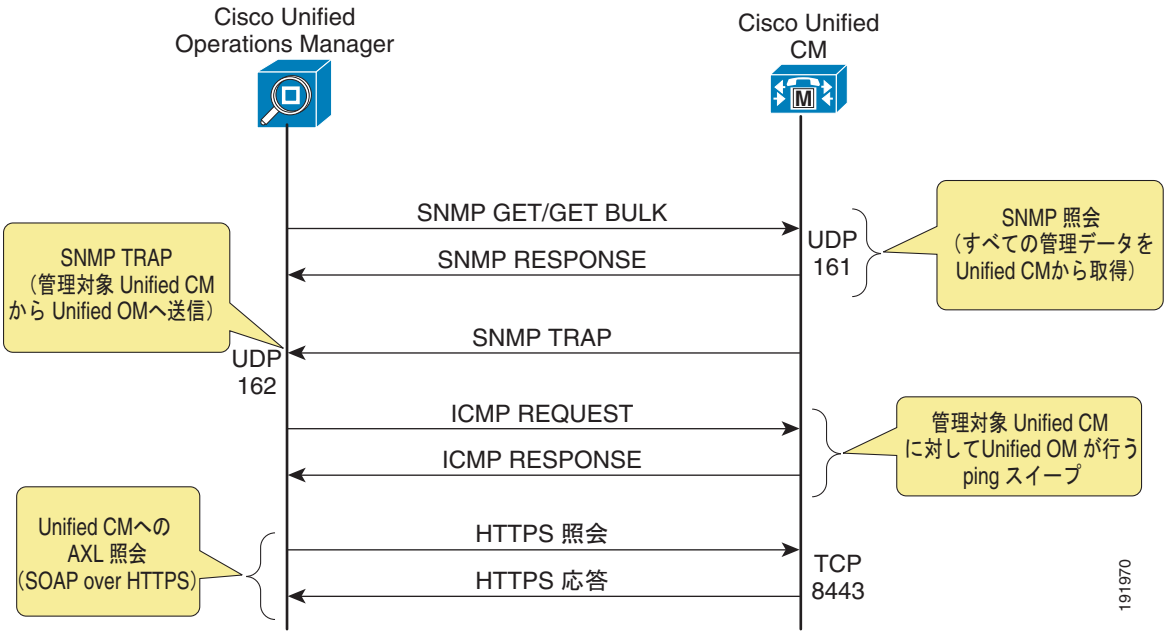
Unified OM はネットワーク内の他のデバイスとの間に次のようなインターフェイスを持ちます。

- Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）を使用して、すべての Cisco Unified Communications サーバ、ゲートウェイ、およびスイッチを管理します。

- Administrative XML Layer（AXL）を使用して、Unified CM を管理します。AXL は、Simple Object Access Protocol（SOAP）over HTTPS Web サービスとして実装されます。
- HTTP を使用して IP Phone に接続し、シリアル番号とスイッチ情報を収集します。IP Phone で HTTP が有効になっている必要があります。
- 拡張イベント処理と Cisco Unified CM のリモート syslog を統合し、Cisco Real-Time Monitoring Tool（RTMT）インターフェイスを利用して、事前に収集された Unified CM クラスタ全体のデータにアクセスします。
- Skinny Client Control Protocol（SCCP）および Session Initiation Protocol（SIP; セッション開始プロトコル）を使用して、統合テストのために Cisco Unified IP Phone と通信します。
- Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）または Ping スイープを使用して、Cisco IOS ルータやスイッチ、および他の音声デバイスや非音声デバイスとインターフェイスします。
- Windows Management Instrumentation（WMI）を使用して Cisco Unity サーバに接続します。

図 28-1 に、Unified OM がどのように Unified CM との複数のインターフェイスを利用して、パフォーマンス カウンタおよびアラームを収集するかを表したシステムレベルの概観図を示します。

図 28-1　Unified OM と Unified CM のシステムレベルの統合



フェールオーバーおよび冗長性

Unified OM では、オプションとして、次のフェールオーバーと冗長性の設定を選択できます。

- ウォーム スタンバイ：すべての Unified OM サーバがアクティブになり、ポーリングを実行します。
- コールド スタンバイ：1 つの Unified OM サーバだけがアクティブになり、ポーリングを実行します。

ウォーム スタンバイ モードでは、ネットワーク内に 1 つのバックアップ Unified OM サーバを配置できます。すべての Unified OM サーバがアクティブにポーリングを実行したり、ネットワーク デバイスから情報を収集したりします。アクティブな Unified OM サーバの 1 つに、デフォルトのポーリング間隔を設定することを推奨します。このサーバはプライマリ Unified OM サーバと呼ばれます。他のすべてのアクティブな Unified OM サーバ、つまりセカンダリ Unified OM サーバには、より長いポーリング間隔（15 分など）を設定する必要があります。これにより、管理データに必要な帯域幅を減らすことや、管理対象デバイスが複数の Unified OM サーバからの SNMP 照会に頻繁に応答しないようにできます。プライマリ Unified OM サーバで障害が発生した場合には、セカンダリ Unified OM サーバのポーリング間隔を短くして、通常の運用およびデータの収集を再開できます。

コールド スタンバイ モードでは、ネットワーク内に 2 つ以上の Unified OM サーバを配置できます。1 つの Unified OM サーバだけがアクティブにポーリングを実行したり、ネットワーク デバイスから情報を収集したりします。アクティブな Unified OM サーバにデフォルトのポーリング間隔を設定することを推奨します。このサーバは、プライマリ Unified OM サーバと呼ばれます。他のすべてのセカンダリ Unified OM サーバも設定しますが、これらのサーバではポーリングを無効にします。プライマリ Unified OM サーバで障害が発生した場合には、セカンダリ Unified OM サーバのポーリングを有効にして、通常の運用およびデータの収集を再開できます。

どちらのモードも、プライマリ サーバの設定とともにセカンダリ サーバを定期的にバックアップする必要があります。これにより、すべてのサーバで設定との同期が維持され、プライマリ Unified OM サーバで障害が発生した場合のダウンタイムが減少します。

2 枚のイーサネット Network Interface Card（NIC; ネットワーク インターフェイス カード）を備えたサーバ プラットフォームは、Unified OM でのネットワークの耐障害性に対応する NIC チーミングをサポートできます。この機能は、サーバを 2 枚の NIC、つまり 2 本のケーブルでイーサネットに接続できるようにするものです。NIC チーミングは、障害の発生したポートから正常なポートに作業負荷を転送することによって、ネットワークのダウンタイムを防止します。NIC チーミングは、ロード バランシングまたはインターフェイス速度向上用には使用できません。

複数のサーバと冗長な設計の考慮事項の詳細については、次の URL で入手可能な『*Unified Communications Operations Manager/Service Monitor Multiple Server and Redundant Design Considerations*』を参照してください。

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps6535/white_paper_c07-469725.html

ポートおよびプロトコル

表 28-3 に、Cisco Unified Operations Manager のさまざまなプロトコル インターフェイスで使用されるポートを示します。これらのポートを社内ファイアウォール（該当する場合）で開いて、Unified OM とネットワーク内の他のデバイス間の通信を可能にすることを推奨します。

表 28-3　Unified OM のポート使用

プロトコル	ポート	サービス
UDP	161	SNMP ポーリング
UDP	162	SNMP トラップ
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP サーバ
UDP	514	Syslog

表 28-3　Unified OM のポート使用（続き）

プロトコル	ポート	サービス
TCP	8080	Unified CM のステータス確認 Web サービス
TCP	8443	Unified CM と Unified OM 間の SSL ポート

Unified OM または管理対象デバイスから発信されるすべての管理トラフィック（SNMP）には、デフォルト マーキングの DSCP 0x00（PHB 0）が付けられます。ネットワーク管理システムの目標は、ネットワーク内のすべての問題または誤動作に対応することです。正確かつ信頼性の高いモニタリングを保証するために、ネットワーク管理データを優先順位付けする必要があります。QoS メカニズムを実装すると、パケット遅延、パケット損失、およびジッタが確実に減少します。ネットワーク管理トラフィックに IP Precedence 2、つまり DSCP 0x16（PHB CS2）を付けて、最小帯域幅保証を提供することを推奨します。Windows オペレーティング システムでは、DSCP 値を設定する必要があります。

管理対象デバイスがファイアウォールの背後にある場合、管理トラフィックを許可するようにファイアウォールを設定する必要があります。Network Address Translation（NAT; ネットワーク アドレス変換）を使用するネットワークでは、Unified OM のサポートは限定されています。Unified OM には、Unified OM サーバから NAT の背後にあるデバイスの NAT IP アドレスへの IP 接続および SNMP 接続が必要です。Unified OM 8.5 では静的な NAT がサポートされます。

帯域幅の要件

Unified OM は設定された間隔ごとに、管理対象デバイスに対してポーリングを実行して、運用ステータス情報を取得します。この情報には、重要な管理データが大量に含まれている可能性があります。特に低速 WAN 上に多数の管理対象デバイスがある場合は、帯域幅を管理データ用にプロビジョニングする必要があります。トラフィック量は、管理対象デバイスのタイプによってそれぞれ異なります。たとえば、Cisco 音声ゲートウェイのモニタリングと比較すると、Unified CM をモニタする方がより多くの管理メッセージが確認されることがあります。また、管理トラフィックの量は、管理対象デバイスが完全モニタリング状態にあるのか部分モニタリング状態にあるのか、および統合テストが実行されているのかどうかによって変わります。Unifed OM 8.*x* では、次の URL で入手可能な Bandwidth Estimator を使用できます。

http://www.cisco.com/web/applicat/ombwcalc/OMBWCalc.html

Cisco Unified Operations Manager サーバのパフォーマンス

Unified OM は単一サーバ モードでサポートされています。ただし、大規模ネットワークを管理するために複数の Unified OM サーバを配置できます。管理情報をより上位の「Manager of Managers」に送信するように、それぞれの Unified OM を設定できます。Unified OM のハードウェア要件およびキャパシティ情報については、次の URL で入手可能な『*Cisco Unified Operations Manager Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/ps6535/products_data_sheets_list.html

Cisco Unified Service Monitor

Cisco Unified Service Monitor（Unified SM）は、Cisco Unified Communications ネットワークでのコールの音声品質をモニタします。また、Unified CM、Cisco 1040 Sensor、および Network Analysis Module（NAM; ネットワーク解析モジュール）を利用して、ネットワーク内の疑似コールではなく、実際のコールに関する音声品質統計情報をモニタおよび収集します。続いて、収集した音声品質統計情

報を、定義済みの Mean Opinion Score（MOS; 平均オピニオン評点）しきい値と比較します。音声品質がしきい値を下回っている場合、Unified SM は、潜在的な問題が識別されたことを示す SNMP トラップ メッセージを Unified OM に送信します。また、Unified SM は、Cisco Unified Service Statistics Manager（Unified SSM）でコール データ分析を実行してレポートを生成できるように、音声品質情報を Unified SSM に送信します。

（注）　グローバルなコール品質しきい値のセットは、サポートされているコーデック タイプごとに 1 つずつ、Unified SM で定義できます。実装されている Cisco 1040 Sensor またはモニタされている Unified CM クラスタに基づいて、さまざまなしきい値をグループ化できます。Unified SM は Unified OM にバンドルされており、Unified OM と Unified SM の両方をインストールするように選択できます。

音声品質の測定

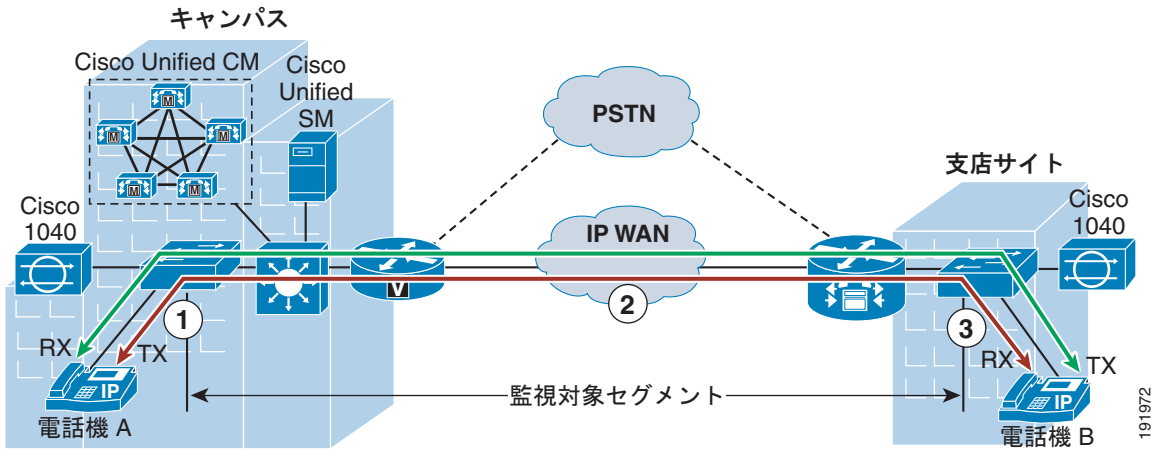
音声品質とは、IP Phone コールの音声および会話の品質を測る質的および量的な基準です。音声品質の測定は、音声会話の明確度および明瞭度を表して、評価します。Unified SM は、Cisco 1040 Sensor、Network Analysis Module（NAM; ネットワーク解析モジュール）、および Unified CM を使用して、音声品質情報をモニタおよび報告します。

Cisco 1040 Sensor の音声品質のモニタリング

Cisco 1040 Sensor は、平均的なユーザが VoIP コールで経験する主観的品質評価を予測するハードウェア デバイスです。RTP ストリームの IP ヘッダーに含まれる、パケット損失、遅延、ジッタ、隠蔽率などのさまざまな品質低下メトリクスを測定することによって機能します。この計算された品質評価は MOS 値に変換されます。MOS 値は、60 秒ごとに Unified SM に送信される Syslog メッセージに格納されます。したがって、Cisco 1040 Sensor は、ほぼリアルタイム ベースで音声品質をモニタします。

Cisco 1040 Sensor には 2 つのファスト イーサネット インターフェイスがあります。1 つはセンサー自体を管理するために使用され、もう 1 つは実際の RTP ストリームをモニタするために、Cisco Catalyst スイッチの Switch Port Analyzer（SPAN; スイッチ ポート アナライザ）ポートに接続されます。WAN 全体のコールの音声品質をモニタするには、図 28-2 に示すように、WAN クラウドの両側に Cisco 1040 Sensor のペアを配置する必要があります。

図 28-2　Cisco 1040 Sensor を使用した音声品質のモニタリング



電話機ごとに送信と受信の 2 つのコール レッグがあります。各コール レッグはコール パスに沿って 3 つのセグメントに分けられます。たとえば、図 28-2 の電話機 A の送信コール レッグの場合、セグメント 1 は電話機 A とキャンパス アクセス スイッチ間、セグメント 2 は 2 つのアクセス スイッチ間、セグメント 3 は支店サイトのアクセス スイッチと電話機 B 間になります。セグメント 1 および 3 はローカル エリア ネットワーク内にあり、このことは音声品質に対する伝送障害が最も少ないことを示します。つまり、これら 2 つのセグメントでは音声品質の低下は発生しないと考えてもほぼ間違いないため、これらの RTP ストリームをモニタする必要はありません。

セグメント 2 は WAN 回線と、コール パス沿いの複数のネットワーク デバイスにまたがっています。WAN に固有のパケット損失、遅延、およびジッタのために音声品質が低下する可能性が高くなります。そのため、（キャンパスからブランチへの）RTP ストリームを支店サイトの Cisco 1040 Sensor でモニタする必要があります。同様に、中央サイトのセンサーで、WAN を渡ってそのセグメントに着信する RTP ストリームをモニタする必要があります。これらの RTP ストリームは重要な音声品質統計情報を提供するため、関連する MOS 値を慎重に分析する必要があります。

戦略的モニタリングと戦術的モニタリング

Cisco 1040 Sensor の配置には、戦略的モニタリングと戦術的モニタリングの 2 つの方法があります。戦略的モニタリングでは、ネットワーク内のすべての IP Phone または IP Phone のサブセットを継続的にモニタするために、Cisco 1040 Sensor を配置します。戦術的モニタリングでは、音声品質問題が識別されているサイトに Cisco 1040 Sensor を配置します。Cisco 1040 Sensor は、FCC クラス B 標準に準拠しているため、企業環境に簡単に配置できます。

小規模ネットワークでは、戦略的モニタリングを配置して、すべての IP Phone を継続的にモニタすることを推奨します。中規模から大規模のネットワークでは、戦略的モニタリングを配置して IP Phone のサブセットを継続的にモニタすると同時に、戦略的モニタリングを使用して残りの IP Phone で発生しているすべての音声品質問題をトラブルシューティングすることを推奨します。

Cisco 1040 Sensor の設計に関する考慮事項

Cisco 1040 Sensor を配置する場合には、次の設計要素を考慮してください。

- Cisco 1040 Sensor では、同時に 100 本の RTP ストリームをモニタできます。図 28-2 に示すように着信 RTP ストリームだけをモニタすると、Cisco 1040 Sensor は（50 本ではなく）100 本の同時音声コールをモニタするメリットを十分に提供できます。大量のコールがある環境では、より多くの Cisco 1040 Sensor を使用する必要がある場合があります。
- RTP ストリームが多すぎて Cisco 1040 Sensor で処理できない場合は、Cisco 1040 Sensor が RTP ストリームをランダムに選択します。
- Cisco 1040 Sensor は Cisco Catalyst スイッチ上の SPAN ポートを使用して、実際の RTP ストリームをモニタします。Catalyst スイッチのタイプごとに、設定できる SPAN ポートの数量は異なります。たとえば、Cisco Catalyst 6500 および 4500 スイッチに設定できる SPAN ポートは最大 2 つですが、Cisco Catalyst 3550 スイッチの最大数は 1 つです。つまり、ネットワーク内に配置されている Catalyst スイッチのタイプによって、配置できる Cisco 1040 Sensor の数が決まります。
- 複数の Cisco Catalyst スイッチ間にトランキング接続がある場合、およびコール量が少ない場合には、すべての Catalyst スイッチに Cisco 1040 Sensor を配置する必要はありません。単一の Cisco 1040 Sensor で同じ VLAN 内の他のスイッチ上の IP Phone をモニタできるように、Remote Switch Port Analyzer（RSPAN; リモート スイッチ ポート アナライザ）を使用できます。
- IP Phone の数が少なく少量のコールしかないサイトのすべてに Cisco 1040 Sensor を配置するのは非効率的です。このような場合は、1 つの Cisco 1040 Sensor で複数のネットワークの音声ストリームをモニタできるように、Cisco Enhanced Switched Port Analyzer（ESPAN; 拡張スイッチド ポート アナライザ）を使用できます。

Unified CM の音声品質のモニタリング

Unified CM は Cisco Voice Transmission Quality（CVTQ）アルゴリズムを使用して、音声品質をモニタします。CVTQ は Klirrfaktor（K ファクタ）方式に基づいて、音声コールの MOS 値を見積もります。各コールの終了時に、Unified CM は Call Management Record（CMR; コール管理レコード）に MOS 値を格納します。CMR および Call Detail Record（CDR; コール詳細レコード）は、60 秒ごとに Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）経由で Unified SM に転送されます。Unified CM と統合するには、Unified CM の Unified Serviceability の設定 Web ページで、Unified SM を課金アプリケーション サーバとして設定する必要があります。Unified CM クラスタごとに最大 3 つの課金アプリケーション サーバを設定できます。次の設定を課金アプリケーション サーバに指定します。

- Unified SM サーバのホスト名または IP アドレス
- SFTP ファイル転送のユーザ名およびパスワード
- プロトコル：SFTP
- CDR および CMR の転送先にする Unified SM サーバのディレクトリ パス

CVTQ は、Unified CM 7.*x* と、SCCP および SIP の両方のモードで実行している Cisco Unified IP Phone によってネイティブにサポートされています。CVTQ をサポートする電話機モデルの一覧は、次の URL で入手可能な互換性情報に示されています。

http://www.cisco.com/en/US/products/ps6535/products_device_support_tables_list.html

さまざまな品質低下メトリクスで詳細な検査を実行する Cisco 1040 Sensor と比較すると、K ファクタ方式は、実際にネットワークに影響を与える品質低下の 1 つの側面、つまりパケット損失だけを検査します。このように、CVTQ のアルゴリズムは、Cisco 1040 Sensor がコール品質のモニタに使用するアルゴリズムほど高機能ではありません。CVTQ を使用して音声品質問題を検出し、Cisco 1040 Sensor を使用してその問題を検証およびトラブルシューティングすることを推奨します。

Cisco ネットワーク解析モジュール（NAM）

Cisco NAM は、Remote Monitoring（RMON; リモート モニタリング）および一部の SNMP Management Information Base（MIB; 管理情報ベース）を利用して、ネットワーク管理者が Unified Communications インフラストラクチャのすべてのレイヤを表示し、アプリケーションや、音声とビデオのアプリケーションの QoS などのネットワーク サービスをモニタ、分析、トラブルシューティングできるようにするトラフィック分析モジュールです。Cisco NAM 4.0 で追加された音声計測手段により、NAM に組み込まれているデータ収集とパフォーマンス分析を使用したコール メトリクスを利用するために、NAM を Unified SM に統合できます。

Cisco NAM は、Cisco Unified Communications Management Suite を補完して、企業全体の音声管理ソリューションを提供します。Cisco NAM は、Cisco Catalyst 6000 シリーズ、7600 シリーズ、およびサービス統合型ルータのさまざまな設定で使用できます。NAM アプライアンスは、トラブルシューティングおよび分析のためのグラフィカル ユーザ インターフェイスを備えており、RTP を使用した音声品質分析、音声制御、およびシグナリング モニタリングのための豊富な機能セットを提供します。表 28-4 に、各タイプの NAM でサポートできる同時 RTP ストリーム（単一方向）の最大数を示します。

表 28-4　NAM タイプごとのサポートされる同時 RTP ストリームの数

Cisco NAM タイプ	1040 Sensor	NME-NAM	NAM-2	NAM 2204 アプライアンス	NAM 2220 アプライアンス
サポートされる同時 RTP ストリームの数	100	100	400	1500	4000

Unified SM は音声品質メトリクス用に 60 秒ごとに NAM に対してポーリングを実行します。Unified SM は、Cisco 1040 Sensor と NAM の両方のデータ収集モジュールをまとめ、Cisco 1040 Sensor と NAM の両方で同じ MOS 計算方式を使用します。これにより、Unified SM はさらに高度な分析を行うために、CDR と、Cisco 1040 Sensor および NAM からのコール ストリーム レポートを相互に関連させることができます。

Cisco NAM の詳細については、次のサイトを参照してください。

http://www.cisco.com/go/nam

トランク使用率

Unified SM は、Unified OM および Cisco Unified Service Statistics Manager（Unified SSM）と密接に統合されています。Unified SM はコール情報を収集して長期トレンドおよびレポートのために Unified SSM に提供し、リアルタイム トランク使用率パフォーマンス グラフ向けに Unified OM に提供します。コール情報は、Unified SM が Unified CM から収集する CDR レコードおよび CMR レコードから提供されます。

フェールオーバーおよび冗長性

Cisco 1040 Sensor に冗長性およびフェールオーバーのサポートを提供するように、プライマリおよびセカンダリの Unified SM を設定できます。プライマリ Unified SM からの SCCP キープアライブ メッセージが 3 つ連続して失われると、Cisco 1040 Sensor はセカンダリ Unified SM への登録を試行します。また、Cisco 1040 Sensor は、登録フェールオーバー プロセスが成功したあと、セカンダリ Unified SM に Syslog メッセージを送信します。

最大 3 台の Unified SM または請求アプリケーション サーバを Unified CM に設定できます。1 台の Unified SM で障害が発生しても、残りの 2 台のサーバは Unified CM から CDR および CMR ファイルを取得します。

（注）　Unified CM パブリッシャ サーバは、SFTP 経由で CDR および CMR ファイルを Unified SM に転送します。パブリッシャ サーバを使用できない場合、Unified CM クラスタ内のコールの MOS 値を含む新しい CDR および CMR ファイルを、Unified SM が取得するためのフェールオーバー メカニズムはありません。Cisco Network Analysis Module（NAM; ネットワーク解析モジュール）では、フェールオーバーまたはハイ アベイラビリティをサポートするためのセカンダリ Unified SM は提供されていません。

Unified SM サーバのパフォーマンス

Unified SM は単一サーバ モードにかぎり動作します。ただし、大規模ネットワークを管理するために複数の Unified SM（すべて Cisco Unified Operations Manager に接続）を配置できます。Unified SM のハードウェア要件および情報については、次の URL で入手可能な『*Cisco Unified Service Monitor Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/ps6536/products_data_sheets_list.html

Unified SM でサポートされている音声品質モニタリング キャパシティは、次のとおりです。

- Unified SM は、最大 50 台の Cisco 1040 Sensor をサポートします。
- Unified SM は、最大 45,000 台の IP Phone をサポートします。

- Unified SM は、次のシナリオをサポートします。
  - 1 分あたり 5,000 本のセンサーベースの RTP ストリーム（Cisco 1040 Sensor または NAM モジュールを使用）
  - 1 分あたり 1,600 本の CVTQ ベースのコール
  - 1 分あたり 1,500 本の RTP ストリームと 666 本の CVTQ コール
- Unified SM は、指定された Unified CM クラスタに設定されているすべての Cisco Unified IP Phone の音声品質情報（CDR および CMR ファイル経由）を、自動的に選択および収集します。クラスタ内の特定の IP Phone だけをモニタする設定オプションはありません。

（注）　Unified SM がフル キャパシティで動作した場合、予想されるデータベース増加（Syslog、CDR、および CMR ファイル）は 1 日あたり約 2.4 GB になると推定されます。

ポートおよびプロトコル

表 28-5 に、Cisco Unified Service Monitor のさまざまなプロトコル インターフェイスで使用されるポートを示します。これらのポートを社内ファイアウォール（該当する場合）で開いて、Unified SM とネットワーク内の他のデバイス間の通信を可能にすることを推奨します。

表 28-5　Unified SM のポート使用

プロトコル	ポート	サービス
TCP	80	HTTP
TCP	443	HTTPS
TCP	1741	CiscoWorks HTTP サーバ
UDP	22	SFTP
UDP	162	SNMP トラップ
TCP	43459	データベース
UDP	5666	Syslog[1]
TCP	2000	SCCP[2]
UDP	69	TFTP[3]

1. Unified SM は、Cisco 1040 Sensor から Syslog メッセージを受信します。
2. Unified SM は SCCP 経由で Cisco 1040 Sensor と通信します。
3. Cisco 1040 Sensor は TFTP 経由で設定ファイルをダウンロードします。

（注）　Cisco NAM は、デフォルト以外のポートを使用して、HTTPS でリモートにアクセスされます。Unified SM は各 Cisco NAM に対して認証を行い、HTTP/S セッションを保持します。

音声品質モニタリング方法の比較

Cisco 1040 Sensor、CVTQ、および NAM は相互に補完し合って、音声品質測定のトータル ソリューションを提供します。Cisco 1040 Sensor、CVTQ、および Cisco NAM を使用した音声品質モニタリングの主な違いは、次のとおりです。

- Cisco 1040 Sensor は、パケット損失、遅延、ジッタ、および隠蔽率に基づいて音声コールをモニタします。CVTQ は、パケット損失だけに基づいて音声コールをモニタします。
- Cisco 1040 Sensor および Cisco NAM は、60 秒ごとに音声品質の統計情報を提供します。CVTQ は、コールが完了したあとに、音声品質の統計情報を提供します。
- Cisco 1040 Sensor は、すべての Cisco Unified CM リリースおよび Cisco Catalyst スイッチに接続しているすべてのタイプのエンドポイントと互換性があります。CVTQ は、Unified CM 4.2 以降のリリースだけをサポートしています。
- クラスタ間コールの場合、Cisco 1040 Sensor はエンドツーエンドのコール セグメントをモニタします。CVTQ は、自身のクラスタ内のコール セグメントだけをモニタします。
- Cisco 1040 Sensor を使用して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、およびアプリケーション サーバをモニタし、音声品質問題を調査およびトラブルシューティングすることを推奨します。ネットワーク内の全体的な音声コール品質を測定するには、CVTQ ベースの音声品質モニタリングを使用する必要があります。

CVTQ を使用していない場合でも、Unified SM は CDR 情報を使用して、次のメトリクス用に NAM レポートと相互に関連します。

- 発信元か宛先、またはその両方の内線番号
- デバイス タイプ
- ゲートウェイへのコールまたはゲートウェイからのコールの場合、コールが送信されるインターフェイス
- コールの切断理由（可能な場合）
- 電話機が接続される（Unified CM クラスだけでなく）正確な Unified CM サーバ

Cisco Unified Service Statistics Manager

Cisco Unified Service Statistics Manager（Unified SSM）は、高度なコール統計情報分析を実行して、経営幹部向け、運用担当向け、およびキャパシティ計画担当向けのレポートを生成します。Unified SSM は Unified OM および Unified SM に完全に依存してコール統計情報を取得するため、Unified SSM を配置する前に、Unified OM および Unified SM を実装して運用する必要があります。Unified SSM では、あらかじめ用意されたテンプレートに沿ったレポートとカスタマイズ可能なレポートの両方を使用でき、これらのレポートで、Cisco Unified Communications システム全体のコール量、サービスの可用性、コール品質、リソース使用率、トランク使用率、キャパシティなどの主要メトリクスを確認できます。機能のサポートや機能の詳細については、http://www.cisco.com で入手可能な Cisco Unified Service Statistics Manager の製品マニュアルを参照してください。

Unified OM および Unified SM との統合

Unified SSM と統合できる Unified OM は 1 つだけですが、Unified SM は複数統合できます。Unified SSM は、Unified OM データベースおよび Unified SM データベースからコール統計データを抽出します。データ抽出プロセスは、Unified SSM エージェントによって実行されます。

Unified SSM エージェントによって、Unified SSM と Unified OM または Unified SM 間の通信が容易になり、Unified OM または Unified SM から Unified SSM にコール統計データが送信されます。抽出されたデータは、Unified SSM によって専用の SQL データベースに格納されます。

Unified OM および Unified SM が Unified SSM と同じ Cisco Media Convergence Server（MCS）に配置されている場合、Unified OM または Unified SM に Unified SSM エージェントをインストールする必要はありません。このような共存配置の場合、Unified SSM は、ネットワークでコール統計データを転送しないで、Unified OM および Unified SM のデータベースから直接データを抽出できます。

Unified OM および Unified SM を Unified SSM とは別に配置している場合、Unified OM および Unified SM のインスタンスごとに Unified SSM エージェントをインストールする必要があります。Unified SSM エージェントの実行可能なインストール ファイルは、Unified SSM の Web 管理ページからダウンロードして、Unified OM および Unified SM にローカルにインストールできます。Unified OM および Unified SM に配布された Unified SSM エージェントを使用すると、Unified SSM でデータ抽出プロセスを制御および管理できます。Unified SSM は、配布されたすべての Unified SSM エージェントにポート 12124 の TCP 経由で接続し、Unified SSM エージェントはコール統計データをポート 12126 の TCP 経由で Unified SSM に送信します。

Unified SSM には異なる 2 つのデータ収集アプローチがあります。1 つめのアプローチは、*ロー データ収集*と呼ばれます。このアプローチでは、Unified SSM は Unified SSM エージェントに、Unified OM および Unified SM のデータベースから直接すべてのコール統計データを取得するように指示します。取得されたデータはすべて、最長で 30 日間、Unified SSM のデータベースに保存されます。このアプローチの利点は、詳細分析およびレポート生成を実行するための包括的なデータ ソースを Unified SSM に提供することです。

2 つめのアプローチは、*モニタベースのデータ収集*と呼ばれます。このアプローチでは、Unified SSM は Unified SSM エージェントに、処理済みのコール統計データだけを転送するように指示します。このアプローチの利点は、ネットワーク上のトラフィックの負荷が少ないことであり、処理済みのデータは最長で 3 か月間、Unified SSM データベースに保存できます。Unified OM および Unified SM のデータベースにある元のコール統計データを処理するには、Unified SSM Administration コンソールで特別なモニタ インスタンスを作成し、そのモニタ インスタンスを適切な Unified SSM エージェントと関連付ける必要があります。モニタ インスタンスは、定義済みの属性に基づいたデータだけを抽出します。たとえば、コール ボリューム モニタの場合、属性にはオンネットで完了したコールの数、オンネットで失敗したコールの数、オンネットの 1 コールあたりの平均保持時間などが含まれます。各モニタ インスタンスには、一意の定義済み属性リストがあります。モニタ インスタンスは、15 分ごとにポーリングを実行してデータを抽出し、Unified SSM エージェントは関連付けられているモニタ インスタンスから処理済みデータを集約して、30 分ごとに Unified SSM に送信します。

各モニタ タイプのすべての属性の完全な一覧と、設定のガイドラインについては、http://www.cisco.com で入手可能な Cisco Unified Service Statistics Manager の製品マニュアルを参照してください。

（注） 現在、Unified SSM での冗長性およびフェールオーバーのサポートはありません。それでも、データは完全にはパージされず、要約または集約されてデータベース内に保管されるため、Unified SSM では 3 か月以上レポートを使用できます。

次のガイドラインでは、Unified SM、Unified OM、および Unified SSM の統合オプションについて概要を示します。

- Unified SSM と Unified OM は 1 対 1 で統合されます。
- Unified SSM と Unified SM は 1 対 5 で統合されます。
- Unified SM の診断ページから、Unified OM の電話機とゲートウェイのデバイス詳細ページを起動できます。

- Unified OM は、NAM の音声品質詳細情報を報告します。NAM ユーザ インターフェイスと Unified OM の品質警告との相互起動がサポートされています。
- Unified SM は、Unified OM のサービス品質アラート ダッシュボードと統合されます。
- Unified SM は、Unified SSM の長期レポート機能およびトレンド機能と統合されます。

Unified SSM サーバのパフォーマンス

Unified SSM は単一サーバ モードにかぎり動作します。Unified SSM のハードウェア要件および情報については、次の URL で入手可能な『*Cisco Unified Service Statistics Manager Data Sheet*』を参照してください。

http://www.cisco.com/en/US/products/ps7285/products_data_sheets_list.html

ポートおよびプロトコル

表 28-6 に、Cisco Unified Service Statistics Manager のさまざまなプロトコル インターフェイスで使用されるポートを示します。これらのポートを社内ファイアウォール（該当する場合）で開いて、Unified SSM とネットワーク内の他のデバイス間の通信を可能にすることを推奨します。

表 28-6　Unified SSM のポート使用

プロトコル	ポート	サービス
TCP	48101	HTTP
TCP	48443	HTTPS
TCP	12123	Unified SSM エージェント コントローラ リスナー
TCP	12124	Unified SSM エージェント リスナー[1]
TCP	12125	Unified SSM と Unified SSM エージェントとの通信[2]

1. Unified SSM は、配布されたすべての Unified SSM エージェントと接続します。
2. Unified SSM エージェントは、Unified SSM にコール統計データを送信します。

Cisco Unified Provisioning Manager

Cisco Unified Provisioning Manager（Unified PM）は、Java 2 Enterprise Edition（J2EE）アーキテクチャに基づいた Web ベースのプロビジョニング アプリケーションです。Unified PM は、Cisco Unified Communications Manager（Unified CM）、Cisco Unified Communications Manager Express（Unified CME）、Cisco Unity、Cisco Unity Connection、および Cisco Unity Express の新規と既存の両方の配置について、簡素化された Web ベースのプロビジョニング インターフェイスを提供します。Unified PM では、1 日目および 2 日目に必要なインフラストラクチャとサブスクライバ（または、電話機ユーザ）の両方のプロビジョニングを提供します。1 日目に必要なものには、新規配置の設定およびサイトまたはロケーションの追加が含まれ、2 日目に必要なものには、Cisco Unified Communications ソリューションのさまざまなコンポーネントにおける継続的な移動、追加、および変更のためのサービスが含まれます。

また、Cisco Unified Provisioning Manager は、Northbound API を提供して、シスコおよびサードパーティが、HR システム、カスタムまたはブランド製のユーザ ポータル、他のプロビジョニング システム、ディレクトリ サーバなどの外部アプリケーションと統合できるようにします。

Unified PM は簡易モードまたは拡張モードでインストールでき、最大 60,000 台の電話機と 120,000 本の回線をサポートします。簡易モードでは、Unified PM を 1 つのシステムに単一サーバとしてインストールして、最大 10,000 台の電話機をサポートします。拡張モードでは、2 つのシステムにインストールでき、1 台のサーバに Unified PM データベース サーバをインストールし、Web およびアプリケーション サーバを別のシステムにインストールして、10,000 ～ 60,000 台の電話機をサポートします。

システム要件とインストール手順の詳細、サポートされるコンポーネントのプロビジョニング ユーザとインフラストラクチャ、およびキャパシティ情報については、次の URL で入手可能な Cisco Unified Provisioning Manager のマニュアルを参照してください。

http://www.cisco.com/go/cupm

さまざまな Cisco Unified Communications コンポーネントをプロビジョニングするために Unified PM をネットワーク管理ソリューションとして使用する方法をより深く理解するために、次の項では Unified PM の基本概念について説明します。

Unified PM の概念

Unified PM は、Cisco Unified Communications システムの次のコンポーネントのプロビジョニング インターフェイスとして機能します。

- コール プロセッサ
  - Cisco Unified Communication Manager（Unified CM）
  - Cisco Unified Communications Manager Express（Unified CME）
- メッセージ プロセッサ
  - Cisco Unity
  - Cisco Unity Connection
  - Cisco Unity Express
- プレゼンス プロセッサ
  - Cisco Unified Presence

（注）　コンポーネント バージョンの互換性の詳細については、http://www.cisco.com/en/US/products/ps7125/products_device_support_tables_list.html で入手可能な Unified PM の情報を参照してください。

次の項では、これらのコンポーネントの設定に関連する Unified PM の概念について説明します。

ドメイン

ドメインは、システム内に複数の論理グループを作成するという管理上の目的で使用されます。ドメインには次の特性があります。

- ドメインは、地理的なロケーションまたは組織ユニットにマッピングできます。
- 1 つのドメインには、複数のコール プロセッサおよび複数のオプションのメッセージ プロセッサを含めることができます。
- 1 つの特定のコール プロセッサまたはメッセージ プロセッサを、複数のドメインのメンバーに設定できます。
- ドメインでサブスクライバを分けて、サブスクライバを別々に管理できます。

サービス エリア

サービス エリアはオフィスを示します。サービス エリアによって、ドメイン内のダイヤル プランおよび他の音声関連の設定が決まります。現実には、各オフィスに複数のサービス エリアが存在することがあります。サービス エリアによって、Unified CM 内で使用されるデバイス グループ、ルート パーティション、コーリング サーチ スペースなどの属性が決まります。サービス エリアには次の特性があります。

- 各サービス エリアは、単一のコール プロセッサおよびオプションの 1 つのメッセージ プロセッサに割り当てられます。
- 各サービス エリアは 1 つのダイヤル プランと関連付けられる必要があります。

ユーザおよびサブスクライバ

*ユーザ*とは、割り当てられたユーザ ロールに基づいて、Unified PM 内のさまざまなタスクを実行する権限を与えられた人をいいます。インストール時に、Unified PM は、Unified PM 内のすべてのタスクを実行する、グローバルな管理権限および完全な許可を持った Unified PM 管理者（Unified PM ではスーパー管理者とも呼ばれる）を作成します。

ユーザ ロールは、Unified PM 内のアクセス レベルを決定します。ドメイン固有のユーザを、ドメイン内の特定のタスクの権限を持つ複数のユーザ ロールに割り当てることができます。個々のユーザ ロールは、ポリシーまたはワークフロー タスクに関連しています。ユーザは、管理者または電話機ユーザになることができます。

Unified PM の *サブスクライバ*は、基になる音声アプリケーションによって提供される IP テレフォニー サービスを使用するエンティティです。サブスクライバは Unified CM の電話機ユーザと同じです。Unified PM のユーザ自身がサービスを使用することもあります。そのため、ユーザ（管理者）がサブスクライバ（または電話機ユーザ）になることもあります。また、Unified PM では Unified CM で存在しない疑似サブスクライバ（会議室やロビーの電話機など）を使用できます。

ワークフローおよびオーダーの管理

新規サイトを展開する場合、または既存のサイトに対して移動、追加、および変更を行う場合、ユーザは、オーダーの作成とそのオーダーの処理という 2 段階のプロセスで基盤となるシステムを変更します。これらの段階の両方にポリシーを設定できます。たとえば、1 つのユーザ グループはオーダーの作成と送信だけができ、別のユーザ グループは処理関連のアクティビティの表示および実行ができるようにシステムを設定できます。Unified PM には、Unified PM の設定方法に基づいて、サービス アクティベーションおよびビジネス フローなどのオーダー処理を実行するオートメーション エンジンが組み込まれています。

ワークフローは、オーダー プロセスのアクティビティ（承認、電話機割り当て、出荷、および受領）を連係させます。

設定テンプレート

Unified PM を使用すれば、設定テンプレートの使用を通して一貫した方法で、Unified CM、Unified CME、Cisco Unity、Cisco Unity Express、および Cisco Unity Connection を設定できます。これらの製品をテンプレートを使用して設定することによって、既存の製品に対する増分ロールアウトを実施したり、既存の顧客全員に新しいサービスを展開したりできます。

バッチ プロビジョニング

ユーザの作成およびそのサービスのプロビジョニングは、新規支店のロール アウトまたはレガシー システムからの移行用のバッチ プロビジョニングで自動的に実行することもできます。

ベスト プラクティス

次のベスト プラクティスおよびガイドラインは、Unified PM を使用して、新規または既存の配置用に Cisco Unified Communications コンポーネントをプロビジョニングする場合に適用されます。

- 新規サイトのロール アウトなどの 1 日目のその他のアクティビティ、および移動、追加、変更などの 2 日目のアクティビティのために Unified PM を使用する前に、管理対象デバイスを起動して、実行しておく必要があります。
- Cisco Unified CM、Cisco Unity、Unified CME、Survivable Remote Site Telephony（SRST）、Cisco Unity Express、および Cisco Unified Presence サーバの事前設定が必要です。
- 正しいドメイン、サービス エリア、およびプロビジョニング属性を定義します。
- 必要に応じて、ワークフロー規則だけを変更します。
- サブスクライバ タイプ、拡張規則の設定、および他の設定パラメータの使用を検討します。

これらのベスト プラクティスは、次のような基本タスクによってサポートされています。

- Unified CM、Unified CME などのコール プロセッサおよび Cisco Unity、Unity Connection、Unity Express などのメッセージ プロセッサの追加
- ドメインの作成、およびコール プロセッサとメッセージ プロセッサの作成済みドメインへの割り当て
- Unified CM または Unified CME 用の設定テンプレートを作成および使用した音声ネットワークのプロビジョニング、または既存の配置からの現在の音声インフラストラクチャ設定のインポート
- Unified PM に対する LDAP ユーザの一括同期の実行（該当する場合）
- 各ドメインのサービス エリアの作成（一般的に、ダイヤル プランごとに 1 つのサービス エリア）および各サービス エリアへのサブスクライバ（ユーザ）タイプの割り当てによる配置の設定
- 各ドメインの管理ユーザの作成
- サブスクライバまたはユーザのサービスのオーダー、更新、または変更

（注） Unified PM では、アプリケーション サーバおよびデータベース サーバの分散インストールは使用できません。また、アプリケーション サーバのクラスタリング機能も一切サポートされていません。

Unified PM の詳細については、次の URL で入手可能な『*Getting Started with Cisco Unified Provisioning Manager Deployment and Best Practices*』のマニュアルを参照してください。

http://www.cisco.com/en/US/prod/collateral/netmgtsw/ps6491/ps6705/ps7125/white_paper_c07-523344.html

Unified PM の設計に関する考慮事項

Unified PM には、次の設計上の考慮事項が適用されます。

- 電話機が 10,000 台以下の場合、Unified PM の 1 システム簡易モード インストールを配置します。
- Unified PM データベースを Web およびアプリケーション サーバとは別のシステムにインストールする場合は、2 システムまたはデュアルプロセッサ Microsoft Windows システムを拡張モードで配置します。
- 2 システム拡張モード インストールを 10,000 ～ 60,000 台の電話機に使用する場合、データベース サーバと Web およびアプリケーション サーバの両方を、使用する配置モデルに関係なく、同じ場所に設置する必要があります。

- 1 つの Unified PM で、最大 60,000 台の電話機または 120,000 本の回線（DN）をサポートできます。
- 次のいずれかの方法でドメインを設定します。
  - 複数のサイトに対して、複数のコール プロセッサと複数のメッセージ プロセッサを持つ単一のドメインを作成します。
  - サイトごとに 1 つのコール プロセッサと 0 個以上のオプションのメッセージ プロセッサで構成されるドメインを作成します。
  - サブスクライバのサブセットを管理するために個別の管理者が必要な場合は、複数のドメインを作成します。
- 複数のダイヤル プランに対して複数のサービス エリアを作成します。
- Unified PM のコール プロセッサとして Unified CM パブリッシャだけを追加します。Unified PM を使用して行った Unified CM パブリッシャの変更はすべて、全部の Unified CM サブスクライバ サーバと同期されます。
- Unified CM、Unified CME、または Cisco Unity Express の設定テンプレートを使用します。
- Unified CME および Cisco Unity Express の設定テンプレートには、Cisco IOS コマンドを使用します。
- Unified CM 設定テンプレート用の Cisco Unified CM インフラストラクチャ データ オブジェクトを追加します。
- 大量の電話機および回線（DN）がある場合は、既存のバッチ プロビジョニング用の設定テンプレートを変更します。
- 2 日目のサービス（電話機、回線、ボイスメールなど）の移動、追加、および変更のために、個々のドメイン管理者でそれぞれのサブスクライバ セットを管理する場合は、単一サイトの配置であっても、複数のドメインを作成します。
- 1 つのダイヤル プランに 1 つのサービス エリアを作成します。
- デバイス プール、ロケーション、コーリング サーチ スペース、および電話機に複数のダイヤル プランが必要な場合は、複数のサービス エリアを作成します。
- Unified PM は次の特性を備えた IPv6 対応アプリケーションです。
  - Unified PM は、IPv4 リンクを介して Unified CM と通信します。Unified CM には IPv4 の SOAP AXL インターフェイスしかないため、Unified PM のユーザ設定インターフェイスでは IPv4 IP アドレスしか入力できません。したがって、Unified PM は IPv4 アドレスを使用して、Unified CM の AXL インターフェイスと通信する必要があります。
  - Unified PM は、SIP トランクの AXL 応答メッセージに含まれている IPv6 アドレスを処理します。
  - IPv6 対応機能のサポートは、現在の Cisco Unified Communications Manager Express、Cisco Unity、Cisco Unity Express、および Cisco Unity Connection のデバイスのサポートには影響を与えません。

Cisco Unified Operations Manager との統合

Unified PM では、サブスクライバまたはユーザの電話機情報を取得するために、Cisco Unified Operations Manager（Unified OM）を起動できます。ユーザは、サブスクライバ レコードの [Details] ボタンを使用することで Unified OM を起動できます。[Details] ボタンによって、Unified OM の [IP Phone Details] ダイアログボックスが起動します。

Unified OM との統合を設定する方法の詳細については、次の URL で入手可能な『*User Guide for Cisco Unified Operations Manager*』を参照してください。

http://www.cisco.com/en/US/products/ps6535/products_user_guide_list.html

冗長性およびフェールオーバー

Unified PM には、現在、本当の冗長性およびフェールオーバーのサポートはありません。複数の Unified PM システムが配置されている場合、この複数のデータベース間の同期はありません。

Unified PM が設定プロセスの途中で失敗した場合、Unified PM GUI から設定デバイスに対して行われていた変更は保存されず、また復元もできない可能性があります。管理者は Unified PM が復旧されるまで、telnet などの他のツールを使用するか、または管理対象デバイスにログイン（HTTP）して、手動手順で設定プロセスを続行する必要があります。管理対象デバイスに手動で追加された設定変更は、次のいずれかの手段を実行しないかぎり、自動的には Unified PM ダッシュボードまたはデータベースに現れません。

- コール プロセッサ（Unified CM および Unified CME）、メッセージ プロセッサ（Cisco Unity、Unity Connection、および Unity Express）、およびドメインに対する Unified PM からの同期化
- Unified PM インストールに付属しているスクリプトを Microsoft Windows スケジューラで使用することによる定期的同期化（毎晩など）

Cisco Unified Provisioning Manager サーバのパフォーマンス

Unified PM のハードウェア要件および情報については、次の URL で入手可能な Cisco Unified Provisioning Manager データ シートを参照してください。

http://www.cisco.com/en/US/products/ps7125/products_data_sheets_list.html

Unified PM には、100 Mbps の Network Interface Card（NIC; ネットワーク インターフェイス カード）が必要です。Unified PM のデフォルトのライセンスでは、最大 750 のコール プロセッサ（Unified CM および Unified CME）、750 のメッセージ プロセッサ（Cisco Unity、Unity Express、および Unity Connection）、または 20 のプレゼンス プロセッサがサポートされます。同期化の時間は、配置されている電話機および回線（DN）の数によって異なります。

ポートおよびプロトコル

表 28-7 に、Unified PM のさまざまなプロトコル インターフェイスで使用されるポートを示します。これらのポートを社内ファイアウォール（該当する場合）で開いて、Unified PM とネットワーク内の他のデバイスとの通信を可能にすることを推奨します。

表 28-7　Unified PM のポート使用

プロトコル	ポート	サービス
TCP	80	HTTP[1] [2]
TCP	8443	HTTPS[2]
TCP	22	SSH[3]
SSH	23	Telnet[3]
TCP	1433	データベース[4]

1. Unified PM Administration の Web ページにアクセスするために使用されます。

2. Unified PM は、Administrative XML Layer（AXL）Simple Object Access Protocol（SOAP）経由で Unified CM をプロビジョニングします。
3. Unified PM が Unified CME および Cisco Unity Express と通信するために使用されます。
4. Unified PM が Cisco Unity および Cisco Unity Connection のデータベースと接続するために使用されます。

その他のツール

上記のネットワーク管理ツール以外に、次のツールにも Cisco Unified Communications システムのトラブルシューティングおよびレポート機能が備えられています。

- 「Cisco Unified Analysis Manager」（P.28-21）
- 「Cisco Unified Reporting」（P.28-22）

Cisco Unified Analysis Manager

Cisco Unified Analysis Manager は Cisco Unified Communications Manager Real-Time Monitoring Tool（RTMT）に含まれています。他の RTMT 機能とは異なり、Unified Analysis Manager は 1 つではなく複数の Unified Communications 要素をサポートするという点で独特です。Unified Analysis Manager は、起動されると Unified Communications システムからトラブルシューティング情報を収集して、その情報の分析を提供します。この情報を使用して独自のトラブルシューティング操作を実行したり、分析のために Cisco Technical Assistance Center（TAC）に情報を送信したりできます。

Unified Analysis Manager は、次の Unified Communications 要素の 8.*x* バージョンをサポートしています。

- Cisco Unified Communications Manager
- Cisco Unified Contact Center Enterprise
- Cisco Unified Contact Center Express
- Cisco IOS 音声ゲートウェイ（3700 シリーズ、2800 シリーズ、3800 シリーズ、5350XM、および 5400XM）
- Cisco Unity Connection
- Cisco Unified Presence

Unified Analysis Manager は、次のような主要機能を提供します。

- Unified Communications 要素からの Unified Communications アプリケーションのハードウェア、ソフトウェア、およびライセンス情報の収集をサポートします。
- Unified Communications 要素全体のトレース レベルの設定およびリセットをサポートします。
- Unified Communications 要素からのログおよびトレース ファイルの収集および定義済み FTP サーバへのエクスポートをサポートします。
- Unified Communications 要素全体のコール パスの分析（コール トレース機能）をサポートします。

レポート オプションの詳細については、次の URL で入手可能な『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』の Cisco Unified Analysis Manager に関する情報を参照してください。

http://www.cisco.com/en/US/docs/voice_ip_comm/cucm/service/8_5_1/rtmt/RTMT.html

Cisco Unified Reporting

Cisco Unified Reporting Web アプリケーションは、Cisco Unified Communications Manager クラスタ データをトラブルシューティングまたは調査するためのレポートを生成します。Unified Communications Manager コンソールからアクセスできる便利なツールです。このツールにより、既存のソースからのデータの収集、データの比較、および異常の報告が容易になります。たとえば、クラスタ内の全サーバのホスト ファイルを表示するレポートを参照できます。このアプリケーションは、パブリッシャ サーバおよび各サブスクライバ サーバから情報を収集します。各レポートは、レポートの生成時にアクセス可能なすべてのアクティブ クラスタ ノードのデータを提供します。

たとえば、Unified CM クラスタの一般的な管理には、次のレポートを使用できます。

- Unified CM Cluster Overview：全サーバの Unified CM バージョン、ホスト名、IP アドレス、ハードウェア詳細の要約など、クラスタの概要を示します。
- Unified CM Device Counts Summary ：Cisco Unified Communications Manager データベースに存在するデバイスの数を、モデルおよびプロトコル別に示します。

Unified CM クラスタのデバッグには、次のレポートを使用できます。

- Unified CM Database Replication Debug：データベース複製のデバッグ情報を提供します。

Unified CM クラスタのメンテナンスには、次のレポートを使用できます。

- Unified CM Database Status：Unified CM データベースの正常性のスナップショットを提供します。アップグレードの前には、このレポートを生成して、データベースが正常であることを保証する必要があります。

レポート オプションの詳細については、次の URL で入手可能な『*Cisco Unified Reporting Administration Guide*』の最新バージョンを参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Cisco Unified Communications 配置モデルとの統合

この項では、さまざまな Cisco Unified Communications 配置モデルに、Cisco Unified Network Management アプリケーションを配置する方法について説明します。配置モデルの詳細については、「Unified Communications の配置モデル」（P.5-1）の章を参照してください。

Cisco Unified Communications Management Suite は、スタンドアロン、共存、および VMware 環境をサポートしています。次のサポート制限およびキャパシティは、この章で説明するすべての配置モデルに適用されます。

- スタンドアロン環境
  - スタンドアロンの Unified OM、Unified SM、または Unified SSM は、最大 45,000 台の電話機をサポートします。スタンドアロンの Unified PM は、最大 60,000 台の電話機をサポートします。
  - IP Phone が 10,000 台を超える場合は、スタンドアロンの Unified PM、Unified OM、Unified SM、および Unified SSM を配置します。
- 共存環境
  - 10,000 台までの電話機を配置する場合は、Unified PM、Unified SM、Unified OM、および Unified SSM を同じ物理サーバに配置できます。

  - IP Phone が 10,000 台より少ない場合は、共存の Unified PM、Unified OM、Unified SM、および Unified SSM を配置します。Unified PM、Unified OM、Unified SM、および Unified SSM の共存に関するシステム要件については、これらの製品のインストール ガイドを参照してください。

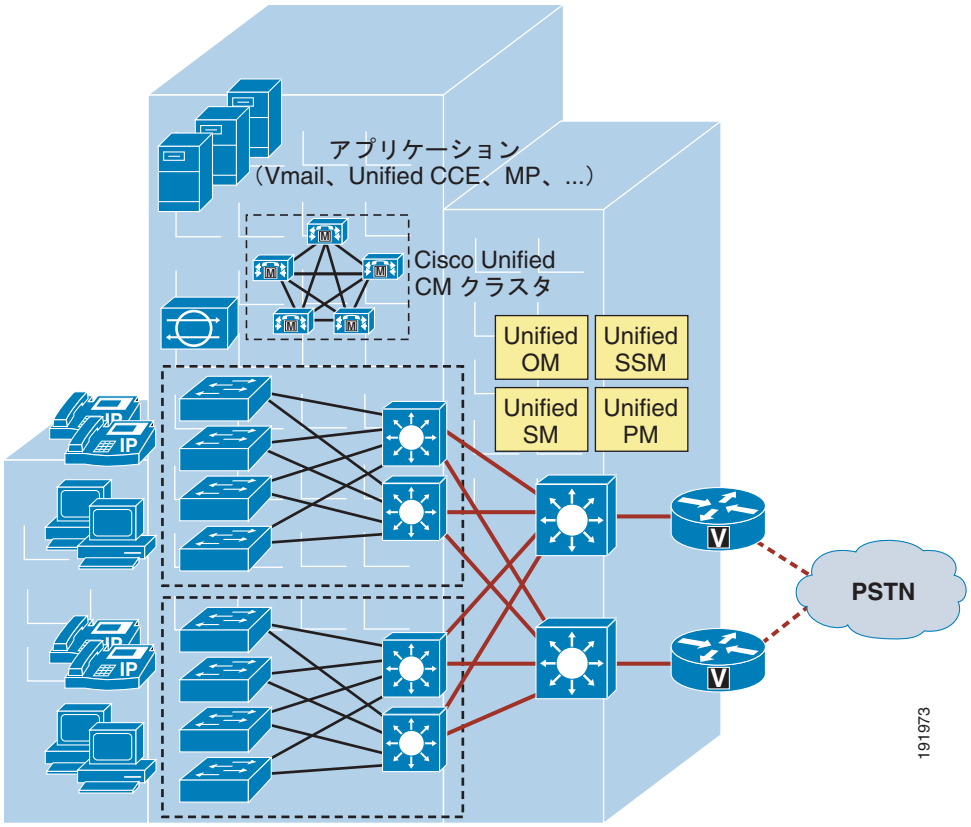
- VMware 環境
  - Unified PM、Unified OM、Unified SM、および Unified SSM のそれぞれを、専用インスタンスとして別々の VMware サーバで実行します。
  - Unified OM インスタンスの最大数は 3 です。
  - Unified SM インスタンスの最大数は 2 です。

（注）　VMware 環境のシステム ハードウェア要件は、この章で説明する各配置モデルに指定されたハードウェア システム要件に加えて、VMware のすべての要件にも従います。

単一サイト

単一サイト モデルでは、Cisco Unified Network Management アプリケーションはコール処理エージェントとともに単一サイト（またはキャンパス）に配置され、IP WAN 上で提供されるテレフォニー サービスを使用しません。企業は、一般的に、LAN または Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）上に単一サイト モデルを配置します。図 28-3 に、Cisco Unified Network Management アプリケーションの単一サイト モデルの配置図を示します。

図 28-3　単一サイトの配置



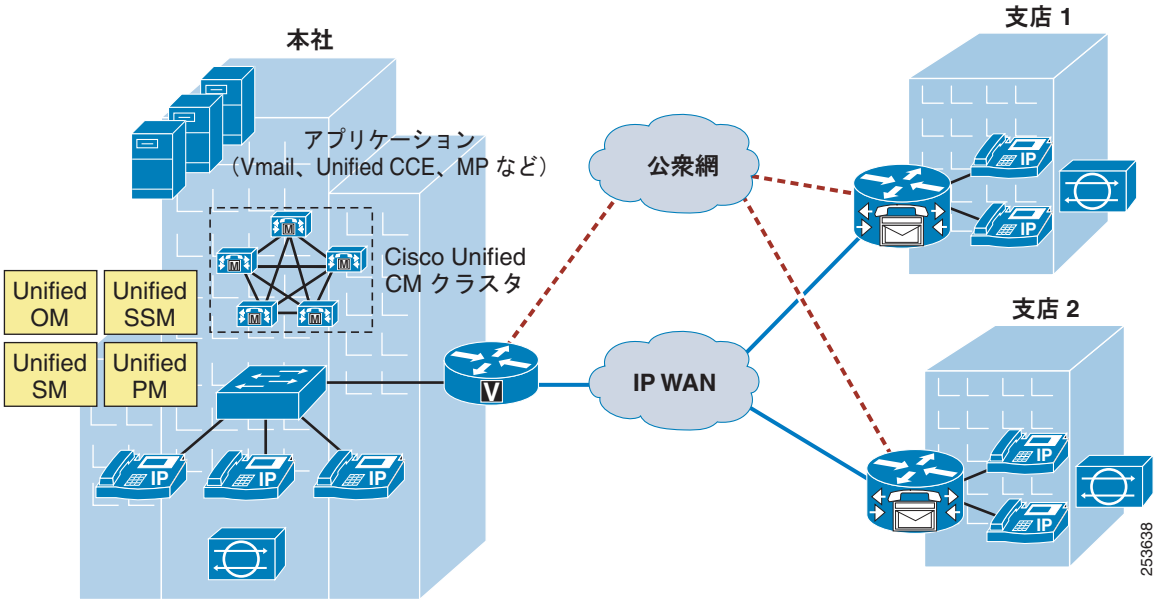
次の設計上の特徴と推奨事項が、Unified OM、Unified SM、Unified SSM、および Unified PM を配置する単一サイト モデルに適用されます。

- CVTQ ベースの音声品質モニタリングを配置して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco 1040 Sensor または NAM を配置して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、およびアプリケーション サーバをモニタし、音声品質問題を調査およびトラブルシューティングすることを推奨します。
- 各 Unified OM は、最大 45,000 台の IP Phone と 30 台の Unified CM クラスタをサポートできます。
- Unified SM は、Cisco 1040 Sensor でモニタされる 1 時間あたり最大 90,000 本の RTP ストリームと、Unified CM でモニタされる 1 時間あたり 15,000 本の CVTQ ベースのコールを同時にサポートできます。
- 各 Unified PM は、最大 60,000 台の IP Phone と複数の Unified CM クラスタをサポートできます。

集中型コール処理を使用するマルチサイト WAN

集中型コール処理を使用するマルチサイト WAN モデルは、実際には単一サイト モデルの拡張であり、中央サイトとリモート サイト間で IP WAN を使用します。IP WAN は、サイト間の音声トラフィックと、中央サイトとリモート サイト間の呼制御シグナリングの転送に使用されます。図 28-4 に、Cisco Unified Network Management アプリケーションの、集中型コール処理を使用するマルチサイト WAN モデルの配置図を示します。

図 28-4　　集中型コール処理を使用するマルチサイト WAN 配置



次の設計上の特徴と推奨事項が、Unified OM、Unified SM、Unified SSM、および Unified PM を配置する、集中型コール処理を使用したマルチサイト モデルに適用されます。

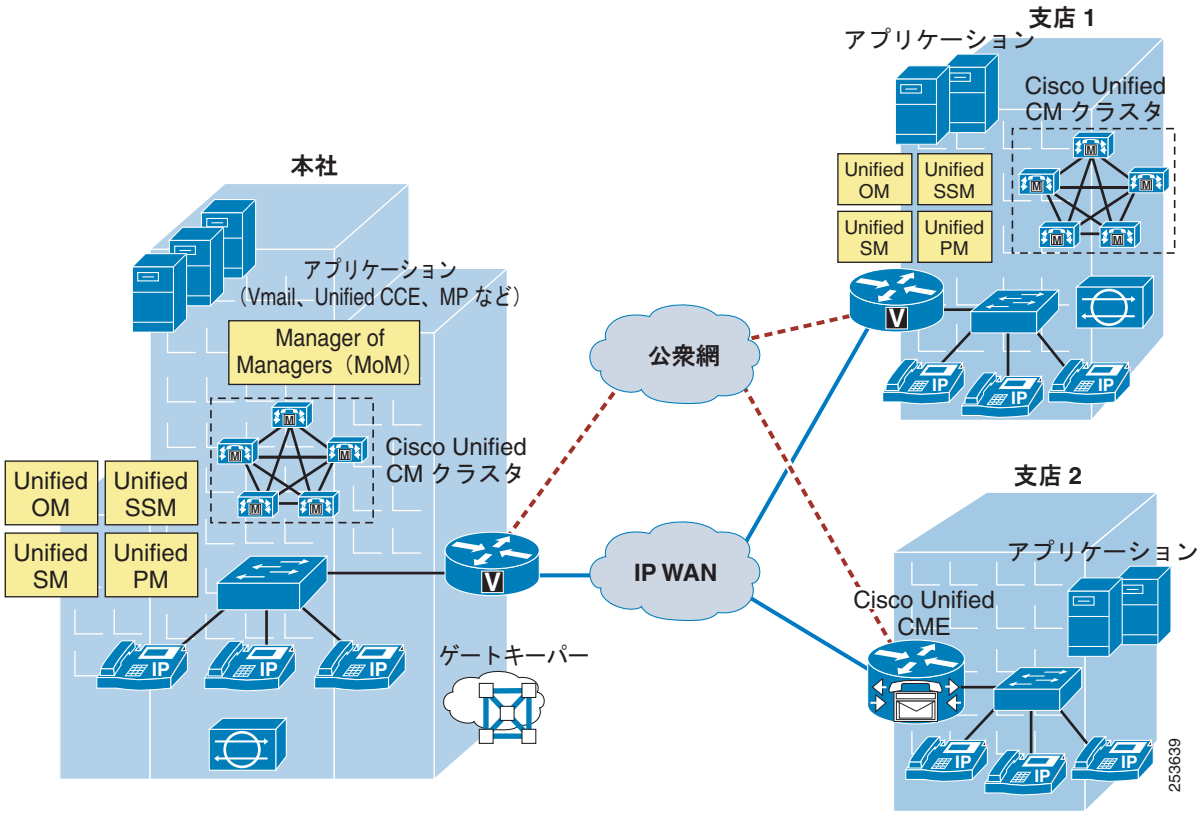
- すべてのネットワーク管理アプリケーション（Unified OM、Unified SM、Unified SSM、および Unified PM を含む）を中央サイトに配置し、これらをコール処理エージェントとともに設置することを推奨します。このような実装のメリットは、コール処理エージェントとネットワーク管理アプリケーション間のネットワーク管理トラフィックを、WAN 回線で送信するのではなく LAN 内で保持できることにあります。
- 複数の Unified OM を配置して、各インスタンスでマルチサイトおよびマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Unified OM では、SNMP トラップ、syslog 通知、および電子メールによる上位レベルの MoM へのリアルタイム通知を使用して、モニタされているネットワークのステータスを報告できます。
- 各 Unified OM は、最大 45,000 台の IP Phone をサポートできます。
- CVTQ ベースの音声品質モニタリングを配置して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco 1040 Sensor または NAM を配置して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、およびアプリケーション サーバをモニタし、音声品質問題を調査およびトラブルシューティングすることを推奨します。

- Unified SM は、Cisco 1040 Sensor でモニタされる 1 時間あたり最大 90,000 本の RTP ストリームと、Unified CM でモニタされる 1 時間あたり 15,000 本の CVTQ ベースのコールを同時にサポートできます。
- 各 Unified SSM は、最大 45,000 台の IP Phone をサポートできます。
- 各 Unified PM は、最大 60,000 台の IP Phone をサポートできます。

分散型コール処理を使用するマルチサイト WAN

分散型コール処理を使用するマルチサイト WAN モデルは、複数の独立したサイトで構成されており、各サイト専用のコール処理エージェントが、IP WAN に接続されています。図 28-5 に、Cisco Unified Network Management アプリケーションの、分散型コール処理を使用するマルチサイト WAN モデルの配置図を示します。

図 28-5　分散型コール処理を使用したマルチサイト WAN 配置



分散型コール処理を使用するマルチサイト WAN 配置には、Unified OM、Unified SM、Unified SSM、および Unified PM の配置に関して、単一サイト、または集中型コール処理を使用するマルチサイト WAN 配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスおよび推奨事項に加えて、このような他のモデルのベスト プラクティスおよび推奨事項にも従ってください。

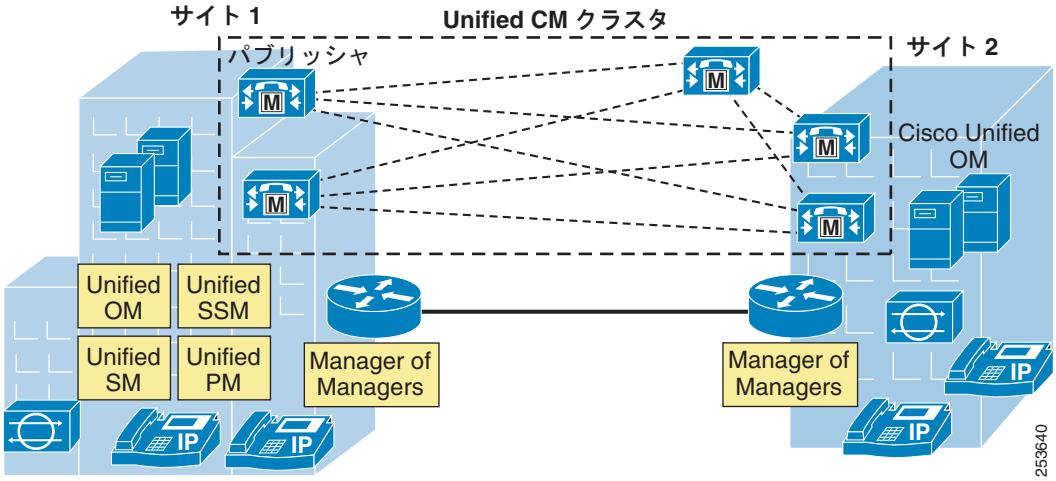
- Cisco Unified Network Management システムを 1 つだけ配置して複数の Unified CM クラスタを管理する場合、Unified OM、Unified SM、Unified SSM、および Unified PM を、コール量とエンドポイント数が最も多い Unified CM クラスタとともに配置することを推奨します。

- 複数の Unified OM を配置して、各インスタンスでマルチサイトおよびマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Unified OM では、SNMP トラップ、syslog 通知、および電子メールによる上位レベルの MoM へのリアルタイム通知を使用して、モニタされているネットワークのステータスを報告できます。
- 各 Unified OM は、最大 45,000 台の IP Phone をサポートできます。
- CVTQ ベースの音声品質モニタリングを配置して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco 1040 Sensor または NAM を配置して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、およびアプリケーション サーバをモニタし、音声品質問題を調査およびトラブルシューティングすることを推奨します。

WAN を介したクラスタリング

WAN を介したクラスタリングとは、QoS 機能対応の IP WAN で相互接続された複数のサイトに、単一の Unified CM クラスタを配置することをいいます。この配置モデルは、IP WAN リンクで障害が発生した場合にコール処理復元性を提供することを目的としています。図 28-6 に、Cisco Unified Network Management アプリケーションの、WAN を介したクラスタリングの配置図を示します。

図 28-6　　WAN を介したクラスタリング



（注）　このモデルでは、Unified SM、Unified SSM、または Unified PM に対するネイティブのハイ アベイラビリティおよび冗長性サポートはありません。

次の設計上の特徴と推奨事項が、Unified OM、Unified SM、Unified SSM、および Unified PM を WAN を介したクラスタリングで配置する場合に適用されます。

- Unified OM、Unified SM、Unified SSM、および Unified PM を、Unified CM パブリッシャが設置されている本社サイトに配置することを推奨します。
- Unified OM をペアで配置することを推奨します。片方のサイトにアクティブな Unified OM を配置して、通常の状況ですべてのサイトを管理します。ウォーム スタンバイの Unified OM はもう 1 つのサイトに設置して、長いポーリング間隔を設定しておく必要があります。ウォーム スタンバ

イの Unified OM は、アクティブな Unified OM が使用不可になったときにアクティブ サーバを引き継いで（ポーリング間隔を短くして）、冗長性サポートを提供します。ウォーム スタンバイ サーバの SNMP ポーリング メッセージ用に追加の WAN 帯域幅をプロビジョニングする必要があります。

- 複数の Unified OM を配置して、各インスタンスでマルチサイトおよびマルチクラスタの Unified Communications 環境を管理できます。この配置シナリオでは、Manager of Managers（MoM）を配置することを推奨します。各 Unified OM では、SNMP トラップ、syslog 通知、および電子メールによる上位レベルの MoM へのリアルタイム通知を使用して、モニタされているネットワークのステータスを報告できます。
- CVTQ ベースの音声品質モニタリングを配置して、ネットワーク内の全体的な音声品質をモニタすることを推奨します。
- Cisco 1040 Sensor または NAM を配置して、ネットワーク内の重要な IP Phone デバイス、ゲートウェイ デバイス、およびアプリケーション サーバをモニタし、音声品質問題を調査およびトラブルシューティングすることを推奨します。
- 各 Unified OM は、最大 45,000 台の IP Phone をサポートできます。
- Unified SM は、Cisco 1040 Sensor でモニタされる 1 時間あたり最大 90,000 本の RTP ストリームと、Unified CM でモニタされる 1 時間あたり 15,000 本の CVTQ ベースのコールを同時にサポートできます。
- 各 Unified SSM は、最大 45,000 台の IP Phone をサポートできます。
- 各 Unified PM は、最大 60,000 台の IP Phone をサポートできます。

GLOSSARY

A

AA Automated Attendant; 自動応答機能

AAD Alerts and Activities Display; 警告とアクティビティの表示

AAR Automated Alternate Routing; 自動代替ルーティング

AC Cisco Attendant Console

ACD Automatic Call Distribution; 自動着呼分配

ACE Cisco Application Control Engine

ACF Admission Confirm; アドミッション確認

ACL Access Control List; アクセス コントロール リスト

ACS Access Control Server

AD Microsoft Active Directory

ADAM Active Directory Application Mode; Active Directory アプリケーション モード

ADPCM Adaptive Differential Pulse Code Modulation; 適応的差分パルス符号変調

ADUC Active Directory Users and Computers; Active Directory ユーザとコンピュータ

AES Advanced Encryption Standard; 高度暗号化規格

AFT ALI Formatting Tool

AGM Cisco Access Gateway Module; Cisco アクセス ゲートウェイ モジュール

ALG Application Layer Gateway; アプリケーション レイヤ ゲートウェイ

ALI Automatic Location Identification; 自動ロケーション識別

AMI Alternate Mark Inversion; 交互マーク反転

AMIS Audio Messaging Interchange Specification

AMWI Audible Message Waiting Indication; 音声メッセージ待機インジケータ

ANI Automatic Number Identification; 発信者番号

AP Access Point; アクセス ポイント

API Application Program Interface; アプリケーション プログラミング インターフェイス

ARJ Admission Reject; アドミッション拒否

ARP Address Resolution Protocol; アドレス解決プロトコル

ARQ Admission Request; アドミッション要求

ASA Cisco Adaptive Security Appliance

ASP Active Server Page

ASR Automatic Speech Recognition; 自動音声認識

ATA Cisco Analog Telephone Adapter

ATM Asynchronous Transfer Mode; 非同期転送モード

AXL Administrative XML Layer

B

BAT Cisco Bulk Administration Tool

BBWC Battery-Backed Write Cache; バッテリ バックアップ式ライト キャッシュ

BES Blackberry Enterprise Server

BFCP Binary Flow Control Protocol

BGP Border Gateway Protocol; ボーダー ゲートウェイ プロトコル

BHCA Busy Hour Call Attempts; 最頻時発呼数

BHCC Busy Hour Call Completions; 最頻時発呼完了

BIB Built In Bridge; ビルトイン ブリッジ

BLF Busy Lamp Field; ビジー ランプ フィールド

BOSH Bidirectional-streams Over Synchronous HTTP

BPDU Bridge Protocol Data Unit; ブリッジ プロトコル データ ユニット

bps Bits per second; ビット / 秒

BRI Basic Rate Interface; 基本速度インターフェイス

BTN Bill-To Number; 請求先番号

C

CA Certificate Authority; 認証局

CAC Call Admission Control; コール アドミッション制御

CAM Content-Addressable Memory; 連想メモリ

CAMA Centralized Automatic Message Accounting

CAPF Certificate Authority Proxy Function

CAR Cisco CDR Analysis and Reporting; Cisco CDR 分析とレポート

CAS Channel Associated Signaling; 個別線信号方式

CBWFQ Class-Based Weighted Fair Queuing; クラスベース WFQ

CCA Clear Channel Assessment

CCD Call Control Discovery

CCS Common Channel Signaling; 共通線信号方式

CDP Cisco Discovery Protocol; シスコ検出プロトコル

CDR Call Detail Record; コール詳細レコード

CGI Common Gateway Interface

CIF Common Intermediate Format

CIR Committed Information Rate; 認定情報レート

CKM Cisco Centralized Key Management

CLEC Competitive Local Exchange Carrier; 競争的地域通信事業者

CLID Calling Line Identifier; 発呼回線 ID

CM Cisco Unified Communications Manager（Unified CM）

CMC Client Matter Code; クライアント識別コード

CME Cisco Unified Communications Manager Express（Unified CME）

CMI Cisco Messaging Interface

CMM Cisco Communication Media Module; Cisco コミュニケーション メディア モジュール

CNG Comfort Noise Generation; コンフォート ノイズ生成

CO Central Office; セントラル オフィス

COM Component Object Model; コンポーネント オブジェクト モデル

COP Cisco Option Package

COR Class Of Restriction; 制限クラス

CoS Class of Service; サービス クラス

CPCA Cisco Unity Personal Assistant

CPI Cisco Product Identification tool; シスコ製品識別ツール

CPN Calling Party Number; 発番号

CRS Cisco Customer Response Solution; シスコ カスタマー応答ソリューション

cRTP Compressed Real-Time Transport Protocol; RTP ヘッダー圧縮

CSF Client Services Framework

CSTA Computer-Supported Telecommunications Applications

CSUF Cross-Stack UplinkFast

CSV Comma-Separated Value; カンマ区切り値

CTI Computer Telephony Integration; コンピュータ テレフォニー インテグレーション

CTL Certificate Trust List

CUBE Cisco Unified Border Element（以前の Cisco Multiservice IP-to-IP Gateway（IP-IP ゲートウェイ））

CUE Cisco Unity Express

CUSP Cisco Unified SIP Proxy

CVTQ Cisco Voice Transmission Quality

D

DC Domain Controller; ドメイン コントローラ

DDNS Dynamic Domain Name Server; ダイナミック ドメイン ネーム サーバ

DDR Delayed Delivery Record

DFS Dynamic Frequency Selection; 動的周波数選択

DHCP Dynamic Host Configuration Protocol

DID Direct Inward Dial; 直通社内通話

DIT Directory Information Tree; ディレクトリ インフォメーション ツリー

DMVPN Dynamic Multipoint Virtual Private Network; Dynamic Multipoint バーチャル プライベート ネットワーク

DMZ Demilitarized Zone; 非武装地帯

DN Directory Number; ディレクトリ番号

DNIS Dialed Number Identification Service; 着信番号識別サービス

DNS Domain Name System; ドメイン ネーム システム

DoS Denial of Service; サービス拒否

DPA Digital PBX Adapter

DSCP Differentiated Services Code Point; 差別化サービス コード ポイント

DSE Digital Set Emulation

DSP Digital Signal Processor; デジタル信号プロセッサ

DTIM Delivery Traffic Indicator Message

DTLS Datagram Transport Layer Security プロトコル

DTMF Dual Tone MultiFrequency

DTPC Dynamic Transmit Power Control; ダイナミック伝送パワー コントロール

DUC Domino Unified Communications サービス

E

E&M 受信（recEive）と送信（transMit）、または Ear and Mouth

EAP Extensible Authentication Protocol

EAPOL Extensible Authentication Protocol over LAN

EC Echo Cancellation; エコー キャンセレーション

ECM Error Correction Mode; エラー訂正モード

ECS Empty Capabilities Set

EI Enhanced Image

EIGRP Enhanced Interior Gateway Routing Protocol

ELIN Emergency Location Identification Number; 緊急ロケーション識別番号

EM Extension Mobility; エクステンション モビリティ

EMCC Extension Mobility Cross Cluster; クラスタ間のエクステンション モビリティ

ER Cisco Emergency Responder

ERL Emergency Response Location; 緊急応答ロケーション

ESF Extended Super Frame; 拡張スーパー フレーム

E-SRST Enhanced Survivable Remote Site Telephony

F

FAC Forced Account Code; 強制アカウント コード

FCC Federal Communications Commission; 米国連邦通信委員会

FCoE Fibre Channel over Ethernet; ファイバ チャネル オーバー イーサネット

FIFO First-In, First-Out; ファーストイン ファーストアウト

FQDN Fully Qualified Domain Name; 完全修飾ドメイン名

FR Frame Relay; フレーム リレー

FWSM Firewall Services Module

FXO Foreign Exchange Office

FXS Foreign Exchange Station

G

GARP Gratuitous Address Resolution Protocol

GC Global Catalog; グローバル カタログ

GKTMP Gatekeeper Transaction Message Protocol

GLBP Gateway Load Balancing Protocol

GMS Greeting Management System; グリーティング管理システム

GPO Group Policy Object; グループ ポリシー オブジェクト

GPRS General Packet Radio Service

GSM Global System for Mobile Communication

GSS Global Site Selector

GUI Graphical User Interface; グラフィカル ユーザ インターフェイス

GUP Gatekeeper Update Protocol

H

H.225D H.225 Daemon; H.225 デーモン

HDLC High-Level Data Link Control; ハイレベル データリンク コントロール

HMS Hardware Media Server

HP Hewlett-Packard

HSRP Hot Standby Router Protocol; ホットスタンバイ ルータ プロトコル

HTTP Hyper-Text Transfer Protocol; ハイパーテキスト転送プロトコル

HTTPS HTTP Secure

Hz Hertz; ヘルツ

I

IANA Internet Assigned Numbers Authority

IAPP Inter-Access Point Protocol; アクセス ポイント間プロトコル

ICCS Intra-Cluster Communication Signaling; イントラクラスタ コミュニケーション シグナリング

ICMP Internet Control Message Protocol; インターネット制御メッセージ プロトコル

ICS IBM Cabling System; IBM 配線システム

ICT InterCluster Trunk; クラスタ間トランク

IETF Internet Engineering Task Force; インターネット技術タスク フォース

IGMP Internet Group Management Protocol; インターネット グループ管理プロトコル

IIS Microsoft Internet Information Server

IM Instant messaging; インスタント メッセージング

IMAP Internet Message Access Protocol

IntServ Integrated Service; 統合サービス

IntServ/DiffServ Integrated Service/Differentiated Service; 統合サービス / ディファレンシエーテッド サービス

IOPS Input/output operations per second; 1 秒当たりの入出力処理

IP Internet Protocol; インターネット プロトコル

IPCC Cisco IP Contact Center; シスコ IP コンタクト センター

IPMA Cisco IP Manager Assistant

IPPM Cisco IP Phone Messenger

IPSec IP Security

ISO International Standards Organization; 国際標準化機構

ISR Integrated Services Router; サービス統合型ルータ

ITEM CiscoWorks IP Telephony Environment Monitor

ITU International Telecommunication Union; 国際電気通信連合

IVR Interactive Voice Response; 音声自動応答装置

J

JTAPI Java Telephony Application Programming Interface; Java テレフォニー API

K

kbps Kilobits per second; キロビット / 秒

KPML Key Press Markup Language

L

LAN Local Area Network; ローカル エリア ネットワーク

LBR Low Bit-Rate; 低ビット レート

LCD Liquid Crystal Display; 液晶ディスプレイ

LCF Location Confirm; ロケーション確認

LCS Live Communications Server

LDAP Lightweight Directory Access Protocol; ライトウェイト ディレクトリ アクセス プロトコル

LDAPS LDAP over SSL

LDIF LDAP Data Interchange Format

LDN Listed Directory Number

LEAP Lightweight Extensible Authentication Protocol

LEC Local Exchange Carrier; 地域通信事業者

LFI Link Fragmentation and Interleaving; リンク フラグメンテーション / インターリーブ

LLDP Link Layer Discovery Protocol

LLDP-MED Link Layer Discovery Protocol for Media Endpoint Devices

LLQ Low-Latency Queuing; 低遅延キューイング

LRG Local Route Group; ローカル ルート グループ

LRJ Location Reject; ロケーション拒否

LRQ Location Request; ロケーション要求

LSC Locally Significant Certificate; ローカルで有効な証明書

LUN Logical unit number; 論理ユニット番号

M

MAC Media Access Control; メディア アクセス コントロール

MAN Metropolitan Area Network; メトロポリタン エリア ネットワーク

Mbps Megabits per second; メガビット / 秒

MCM Multimedia Conference Manager

MCS Media Convergence Server; メディア コンバージェンス サーバ

MCU Multipoint Control Unit; マルチポイント コントロール ユニット

MDN Mobile Data Network; モバイル データ ネットワーク

MDS Mobile Data Services

MFT MultiFlex Trunk; マルチフレックス トランク

MGCP Media Gateway Control Protocol; メディア ゲートウェイ コントロール プロトコル

MIB Management Information Base; 管理情報ベース

MIC Manufacturing Installed Certificate; 製造元でインストールされる証明書

MIME Multipurpose Internet Mail Extension

MIPS Millions of Instructions Per Second

MISTP Multiple Instance Spanning Tree Protocol

MITM Man-In-The-Middle; 中間者

MLA Cisco Multi-Level Administration; Cisco マルチレベル管理

MLP Multilink Point-to-Point Protocol; マルチリンク ポイントツーポイント プロトコル

MLPP Multilevel Precedence and Preemption

MLPPP Multilink Point-to-Point Protocol; マルチリンク ポイントツーポイント プロトコル

MLTS Multi-Line Telephone System

MMoIP Multimedia Mail over IP; マルチメディア メール オーバー IP

MMP Mobile Multiplexing Protocol

MOC Microsoft Office Communicator

MoH Music on Hold; 保留音

MOS Mean Opinion Score; 平均オピニオン評点

MPLS Multiprotocol Label Switching

MRG Media Resource Group; メディア リソース グループ

MRGL Media Resource Group List; メディア リソース グループ リスト

ms Millisecond; ミリ秒

MSP Managed Service Provider; 管理対象サービス プロバイダー

MTP Media Termination Point; メディア ターミネーション ポイント

mW milli-Watt; ミリワット

MWI Message Waiting Indicator; メッセージ待機インジケータ

N

NAT Network Address Translation; ネットワーク アドレス変換

NDR Non-Delivery Receipt

NENA National Emergency Number Association

NFAS Non-Facility Associated Signaling

NIC Network Interface Card; ネットワーク インターフェイス カード

NOC Network Operations Center

NPA Numbering Plan Area; 番号計画エリア

NSE Named Service Event

NSF Network Specific Facilities

NTE Named Telephony Event

NTP Network Time Protocol; ネットワーク タイム プロトコル

O

ORA Open Recording Architecture

OSPF Open Shortest Path First

OU Organizational Unit; 組織単位

OVA Open Virtualization Archive

OWA Outlook Web Access

P

PAC Protected Access Credential

PBX Private Branch eXchange; 構内交換機

PC Personal Computer; パーソナル コンピュータ

PCI Peripheral Component Interconnect

PCM Pulse Code Modulation; パルス符号変調

PCTR Personal Call Transfer Rule; パーソナル着信転送ルール

PD Powered Device; 受電装置

PHB Per-Hop Behavior; ホップごとのふるまい

PIN Personal Identification Number; 個人識別番号

PINX Private Integrated services Network eXchange

PIX Private Internet eXchange

PLAR Private Line Automatic Ringdown

PoE Power over Ethernet

POTS Plain Old Telephone Service; 一般電話サービス

PPP Point-to-Point Protocol; ポイントツーポイント プロトコル

pps Packets per second; 1 秒あたりのパケット数

PQ Priority Queue; プライオリティ キュー

PRI Primary Rate Interface; 一次群速度インターフェイス

PSAP Public Safety Answering Point

PSE Power Source Equipment

PSK Pre-Shared Key; 事前共有キー

PSTN Public Switched Telephone Network; 公衆電話交換網

PVC Permanent Virtual Circuit; 相手先固定接続

Q

QBE Quick Buffer Encoding

QBSS QoS Basic Service Set

QoS Quality of Service

QSIG Q signaling

R

RADIUS Remote Authentication Dial-In User Service

RAS Registration Admission Status

RCP Remote Copy Protocol; リモート コピー プロトコル

RDNIS Redirected Dialed Number Information Service

REST Representational State Transfer

RF Radio Frequency; 無線周波数

RFC Request For Comments

RIM Research In Motion

RIP Routing Information Protocol

RIS Real-time Information Server

RMTP Reliable Multicast Transport Protocol

RoST RSVP over SIP Trunks

RSNA Reservationless Single Number Access

RSP Route/Switch Processor; ルート スイッチ プロセッサ

RSSI Relative Signal Strength Indicator

RSTP Rapid Spanning Tree Protocol

RSVP Resource Reservation Protocol; リソース予約プロトコル

RTCP Real-Time Transport Control Protocol

RTMP Real-Time Messaging Protocol

RTMT Cisco Real-Time Monitoring Tool

RTP Real-Time Transport Protocol; リアルタイム トランスポート プロトコル

RTSP Real Time Streaming Protocol

RTT Round-Trip Time; ラウンドトリップ時間

S

S1、S2、S3、および S4 Severity levels for service requests; サービス リクエストのシビラティ

SaaS Software-as-a-Service

SAF Service Advertisement Framework

SAN Storage area networking; ストレージ エリア ネットワーキング

SBC Session Border Controller; セッション ボーダー コントローラ

SCCP Skinny Client Control Protocol; Skinny クライアント コントロール プロトコル

SCSI Small Computer System Interface; 小型計算機システム インターフェイス

SDI System Diagnostic Interface

SDK Software Development Kit; ソフトウェア開発キット

SDL Signaling Distribution Layer

SDP Session Description Protocol

SE Cisco Systems Engineer; シスコのシステム エンジニア

SF Super Frame; スーパー フレーム

SFTP Secure File Transfer Protocol; セキュア ファイル転送プロトコル

SI Standard Image

SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol; セッション開始プロトコル
SIS	Symbian Installation System
SIW	Service Inter-Working; サービス インターワーキング
SLB	Server Load Balancing; サーバ ロード バランシング
SLDAP	Secure LDAP
SMA	Segmented Meeting Access; セグメント化会議アクセス
SMDI	Simplified Message Desk Interface
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol; 簡易ネットワーク管理プロトコル
SOAP	Simple Object Access Protocol
SPA	Shared Port Adapter : 共有ポート アダプタ
SQL	Structured Query Language; 構造化照会言語
SRND	Solution Reference Network Design; ソリューション リファレンス ネットワーク デザイン
SRST	Survivable Remote Site Telephony
SRSV	Survivable Remote Site Voicemail
SRTP	Secure Real-Time Transport Protocol
SRV	Server; サーバ
SS7	Signaling System 7
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
SSO	Single Sign-On; シングル サインオン
STP	Spanning Tree Protocol; スパニング ツリー プロトコル
SUP1	Cisco Supervisor Engine 1
SUP2	Cisco Supervisor Engine 2
SUP2+	Cisco Supervisor Engine 2+
SUP3	Cisco Supervisor Engine 3

T

TAC Cisco Technical Assistance Center

TAPI Telephony Application Programming Interface

TCD Telephony Call Dispatcher; テレフォニー コール ディスパッチャ

TCER Total Character Error Rate

TCL Tool Command Language

TCP Transmission Control Protocol; 伝送制御プロトコル

TCS Terminal Capabilities Set; 端末機能セット

TDD Telephone Device for the Deaf

TDM Time-Division Multiplexing; 時分割多重

TEHO Tail-End Hop-Off; テールエンド ホップオフ

TFTP Trivial File Transfer Protocol; トリビアル ファイル転送プロトコル

TKIP Temporal Key Integrity Protocol

TLS Transport Layer Security; トランスポート レイヤ セキュリティ

ToD Time of Day; 時刻

ToS Type of service; タイプ オブ サービス

TPC Transmit Power Control; 伝送パワー コントロール

TRaP Telephone Record and Playback; 電話での録音および再生

TRP Trusted Relay Point

TSP Telephony Service Provider; テレフォニー サービス プロバイダー

TTL Time To Live; 存続可能時間

TTS Text-To-Speech; テキストツースピーチ

TTY Terminal Teletype; ターミナル テレタイプ

TUI Telephony User Interface; テレフォニー ユーザ インターフェイス

U

UAC User Agent Client; ユーザ エージェント クライアント

UAS User Agent Server; ユーザ エージェント サーバ

UCCN Unified Client Change Notifier

UCS Cisco Unified Computing System

UDC Universal Data Connector

UDLD UniDirectional Link Detection; 単方向リンク検出

UDP User Datagram Protocol; ユーザ データグラム プロトコル

UDPTL Unnumbered Datagram Protocol Transport Layer

UMTS Universal Mobile Telecommunications System

UN Unsolicited SIP Notify

UNC Universal Naming Convention; 汎用命名規則

UPS Uninterrupted Power Supply; 無停電電源装置

URI Uniform Resource Identifier; ユニフォーム リソース識別子

USB Universal Serial Bus

UTIM Cisco Unity Telephony Integration Manager

UTP Unshielded Twisted Pair; シールドなしツイスト ペア

UUIE User-to-User Information Element

V

V3PN Cisco Voice and Video Enabled Virtual Private Network; シスコ音声ビデオが利用可能なバーチャル プライベート ネットワーク

VAD Voice Activity Detection; 音声アクティビティ検出

VAF Voice-Adaptive Fragmentation

VATS Voice-Adaptive Traffic Shaping

VCS Cisco TelePresence Video Communication Server

VIC Voice Interface Card; 音声インターフェイス カード

VLAN Virtual Local Area Network; バーチャル ローカルエリア ネットワーク

VMO ViewMail for Outlook

VoIP Voice over IP; ボイス オーバー IP

VoPSTN Voice over the PSTN

VoWLAN Voice over Wireless LAN（WLAN）

VPIM Voice Profile for Internet Mail プロトコル

VPN Virtual Private Network; バーチャル プライベート ネットワーク

VRRP Virtual Router Redundancy Protocol; 仮想ルータ冗長プロトコル

VUI Voice User Interface; 音声ユーザ インターフェイス

VWIC Voice/WAN Interface Card; 音声 /WAN インターフェイス カード

W

WAN Wide Area Network; ワイド エリア ネットワーク

WebDAV Web-Based Distributed Authoring and Versioning

WEP Wired Equivalent Privacy

WFQ Weighted Fair Queuing; 重み付け均等化キューイング

WINS Windows Internet Naming Service

WLAN Wireless Local Area Network; ワイヤレス ローカル エリア ネットワーク

WLSM Cisco Wireless LAN Services Module

WMM Wi-Fi Multimedia

WMM TSPEC Wi-Fi Multimedia Traffic Specification

WPA Wi-Fi Protected Access

X

XCP Jabber Extensible Communications Platform

XML Extensible Markup Language; 拡張マークアップ言語

XMPP Extensible Messaging and Presence Protocol

き

共存 同じ物理的な場所にある複数のデバイスを指します。これらのデバイスの間に WAN または MAN 接続はありません。

共存 同じサーバ上で複数のサービスまたはアプリケーションが実行されている状態

INDEX

記号

数字

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

お

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

は

ひ

ふ

へ

ほ

ま

む

め

も

や

ゆ

よ

ら

り

る

れ

ろ

わ