エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャ

Cisco 検証済みデザイン（CVD）ガイド

改訂日：2015 年 1 月 22 日

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを
開設しています。所在地、電話番号、FAX 番号
は以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices

初版：2014 年 10 月 28 日

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

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

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

はじめに

改訂日：2015 年 1 月 22 日

Cisco Validated Design（CVD）は、一般的な使用事例や現在のシステム リリースに基づき、設計と導入に関する重要な決定事項について説明しています。CVD には、お客様のニーズに応えるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。より迅速で信頼性が高く、完全に予測可能な導入を実現するために、シスコのエンジニアは CVD に含まれるガイドラインを包括的にテストした後、文書化しています。シスコのパートナーやお客様は CVD のテスト済みの成果を活用して、独自の設定と構成でシステムの設計/導入を開始できます。

エンタープライズ コラボレーションに関するドキュメント

『Cisco Preferred Architecture（PA）Design Overview』を活用すると、お客様およびセールス チームは組織のビジネス要件に基づいて適切なアーキテクチャを選択し、アーキテクチャ内で使用される製品について理解し、設計上の一般的なベスト プラクティスを習得することができます。これらの資料はセールス プロセスを支援します。

『Cisco Validated Design（CVD）』資料は、シスコ推奨アーキテクチャを導入する手順について詳しく説明しています。これらの資料はプリファード アーキテクチャの計画、設計、および実装を支援します。

『Cisco Collaboration Solution Reference Network Design（SRND）』資料は、シスコ コラボレーションの設計上のオプションについて詳しく説明しています。設計上の要件がシスコ推奨アーキテクチャの適用範囲を超える場合には、SRND を参考にしてください。

このマニュアルについて

エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャに関するこの『シスコ検証済みデザイン』の対象読者は次のとおりです。

- コラボレーション ソリューションの販売、設計、導入に携わるセールス チーム
- シスコ コラボレーションを導入するための設計上のベスト プラクティスと適切な手順について詳しい情報を必要とされているお客様とセールス チーム

このガイドは、読者の皆様がシスコの音声、ビデオ、コラボレーション製品に関する一般的な知識があり、それらの製品の導入方法の基本を理解していることを前提としています。この CVD 資料をお読みになる前に、『Cisco Preferred Architecture for Enterprise Collaboration Design Overview』を参照することをお勧めします。

この CVD に掲載されている設計上の決定事項は、『Cisco Collaboration SRND』のフレームワークに沿ったものです。SRND には設計上および導入上のさまざまなオプションが提示されていますが、本資料では、プリファード アーキテクチャ デザインの基本想定に基づいて 1 つの推奨導入が選択されています。想定が異なると、設計上の決定も異なる可能性があり、その場合は SRND に照らして確認する必要があります。独特の要件と高度なカスタマイズを備えた大規模な導入環境では、シスコ アカウント マネージャと連絡を取り、この CVD および SRND の適用範囲を超えるガイドラインを得ることをお勧めします。

本資料は、次のような方法で設計および販売のプロセスをシンプルにします。

- 『Cisco Preferred Architecture for Enterprise Collaboration Design Overview』にある製品および設計に関する推奨事項に基づいています
- 『Cisco Preferred Architecture Design Overview』
- コラボレーション アーキテクチャについて詳しく説明し、ベスト プラクティスを明示し、これらの推奨事項の根拠を示します

この CVD ガイドは次に示す個別のモジュールで編成され、これらが総合的にコラボレーション ソリューションを構成します。

- コール制御 — ダイヤル プラン設計、コンピュータ テレフォニー インテグレーション（CTI）、Survivable Remote Site Telephony（SRST）、IM and Presence、LDAP ディレクトリ統合、SIP トランク、その他のコール制御機能の概念を示します。また、この章では、企業のコラボレーション向けのプリファード アーキテクチャでコール制御を導入するうえでのベスト プラクティスも紹介します。
- 会議 — 企業のコラボレーション向けのプリファード アーキテクチャで使用可能なさまざまな種類の会議と、会議機能を導入する方法について説明します。
- コラボレーション エッジ — リモート登録サービス、外部通信、および相互運用性を提供する Cisco Collaboration Edge コンポーネントの導入方法を説明します。
- コア アプリケーション — 企業のコラボレーション向けのプリファード アーキテクチャで使用可能なさまざまなアプリケーションと導入ツールについて紹介し、ユニファイド メッセージングおよび会議スケジュール用の 2 つのコア アプリケーションについて詳しく説明します。
- サイジング — お客様の導入環境の要件に合わせて企業のコラボレーション向けのプリファード アーキテクチャ コンポーネントの規模を決定するための簡単な例を示します。

マニュアルの変更履歴

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

http://www.cisco.com/go/cvd/collaboration

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

表 1 は、このマニュアルの改訂履歴を示しています。

表 1　　この CVD ガイドの改訂履歴

改訂日	説明
2015 年 1 月 22 日	Cisco Collaboration System Release（CSR）10.6 向けにこのマニュアルが更新されました。詳細については、各章の「*この章の変更点*」を参照してください。
2014 年 10 月 28 日	このマニュアルの初版

マニュアルの入手方法およびテクニカル サポート

資料の入手方法、Cisco Bug Search Tool（BST）の使用法、サービス要求の送信、および追加情報の収集方法については、「*What's New in Cisco Product Documentation*」（http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html）を参照してください。

「*What's New in Cisco Product Documentation*」に配信登録すると、新しい（または改訂された）シスコ技術情報のリストが RSS フィードとして提供され、リーダー アプリケーションを使ってコンテンツがデスクトップに直接配信されるようにすることができます。RSS フィードは無料のサービスです。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	表示
bold フォント	コマンド、キーワード、およびユーザが入力するテキストは、**bold** フォントで記載されます。
italic フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*italic* フォントで記載されます。
[　]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで記載されます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符(!)またはポンド記号(#)がある場合には、コメント行であることを示します。

コメント

「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント

「*問題解決に役立つ情報*」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。

注意

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

ワンポイント アドバイス

「*時間の節約に役立つ操作*」です。記述されている操作を実行すると時間を節約できます。

警告

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

警告

このシンボルを使ったステート メントは、追加情報および規制要件または顧客要件に準拠するためのものです。

はじめに

改訂日：2015 年 1 月 22 日

このわずか数年の間に、ビジネスの境界を超えてコミュニケーションの強化とコラボレーションの拡大を実現する多くの新しいコラボレーション ツールが市場に投入されました。組織がコラボレーション アプリケーションから得ているビジネスの付加価値は、従業員の生産性向上とお客様との関係強化です。コラボレーション分野の著しい進化により、導入の簡素化、相互運用性の向上、ユーザ エクスペリエンスの全体的な改善が実現しました。

現在のコラボレーション ソリューションでは、ビデオ、音声、そして Web による参加者を一元的な会議環境に統合することが可能になっています。この Cisco Validated Design（CVD）ガイドに含まれるガイドラインは、コラボレーション アーキテクチャ全体を考慮して記載されています。内容をより適切に編成する目的で、サブシステムが使用されています。また、サブシステムの推奨事項をテストし、これらのサブシステムの推奨事項が、関連サブシステムの推奨事項と一致していることを確認しています。

この章の変更点

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

表 1-1　　本リリースで追加または変更された情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco IX シリーズ エンドポイントを追加	表 1-3	2015 年 1 月 22 日

アーキテクチャの概要

このエンタープライズ コラボレーション向けプリファード アーキテクチャの CVD は、シスコ コラボレーション ポートフォリオの全製品のうち、エンタープライズ市場セグメントに最適な製品で構成されます。このプリファード アーキテクチャ導入モデルはすぐに使える規範的な導入モデルで、組織とそのビジネス ニーズの変化に対応できる拡張性を備えています。この規範的なアプローチでは、複数のシステムレベルのコンポーネントを簡単に統合でき、組織がそれぞれのビジネス ニーズに最適な機能、サービス、キャパシティを選択できます。

このエンタープライズ コラボレーション向けプリファード アーキテクチャの CVD は、ユーザ数が 1,000 人を超える導入環境に対応したエンドツーエンドのコラボレーションを実現します。これよりも小規模な導入環境の場合は、『Preferred Architecture Design Overview and CVDs for Midmarket Collaboration』を参照してください。

このエンタープライズ コラボレーション向け推奨アーキテクチャの CVD では、重要なアプリケーションの高可用性を実現します。このアーキテクチャは次の主要なサービスを通じてモバイル ワーカー、パートナー、お客様に拡張できる、高度なコラボレーション サービスをサポートします。

- 音声コミュニケーション
- インスタント メッセージおよびプレゼンス
- 高精細度ビデオおよびコンテンツ共有
- リッチ メディア会議機能
- モバイル ワーカーやリモート ワーカーへの対応
- 企業間（B2B）音声/ビデオ通信
- ユニファイド ボイス メッセージング

シスコのエンドポイントは適応性が高く、IP ネットワークをサポートしているため、このアーキテクチャを導入すれば、組織が現行データ ネットワークを使用して音声通話とビデオ通話の両方に対応できます。一般的に、コラボレーション ソリューション導入のベスト プラクティスは、ネットワーク全体で適切な Quality of Service（QoS）を設定することです。ユーザ エクスペリエンスを維持し、遅延、ロス（損失）、ジッターなどの悪影響を回避するため、音声およびビデオの IP トラフィックを分類して優先度を設定する必要があります。LAN および WAN の QoS については、『Cisco Collaboration SRND』を参照してください。

エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャは、図 1-1 に示すように、可用性とセキュリティを備えた集中管理型のサービスを提供します。これらのサービスはリモート オフィスや移動の多い社員に容易に拡張でき、本社との通信が失われた場合でも重要なサービスの可用性を提供できます。これは、新たな導入環境を設計する場合や既存の導入環境を拡大する場合のベースとなる基本アーキテクチャとして理解しておく必要があります。推奨アーキテクチャの進展に伴い、製品やソリューションが追加され、このアーキテクチャは拡大します。

図 1-1　　エンタープライズ コラボレーション向けシスコ推奨アーキテクチャ

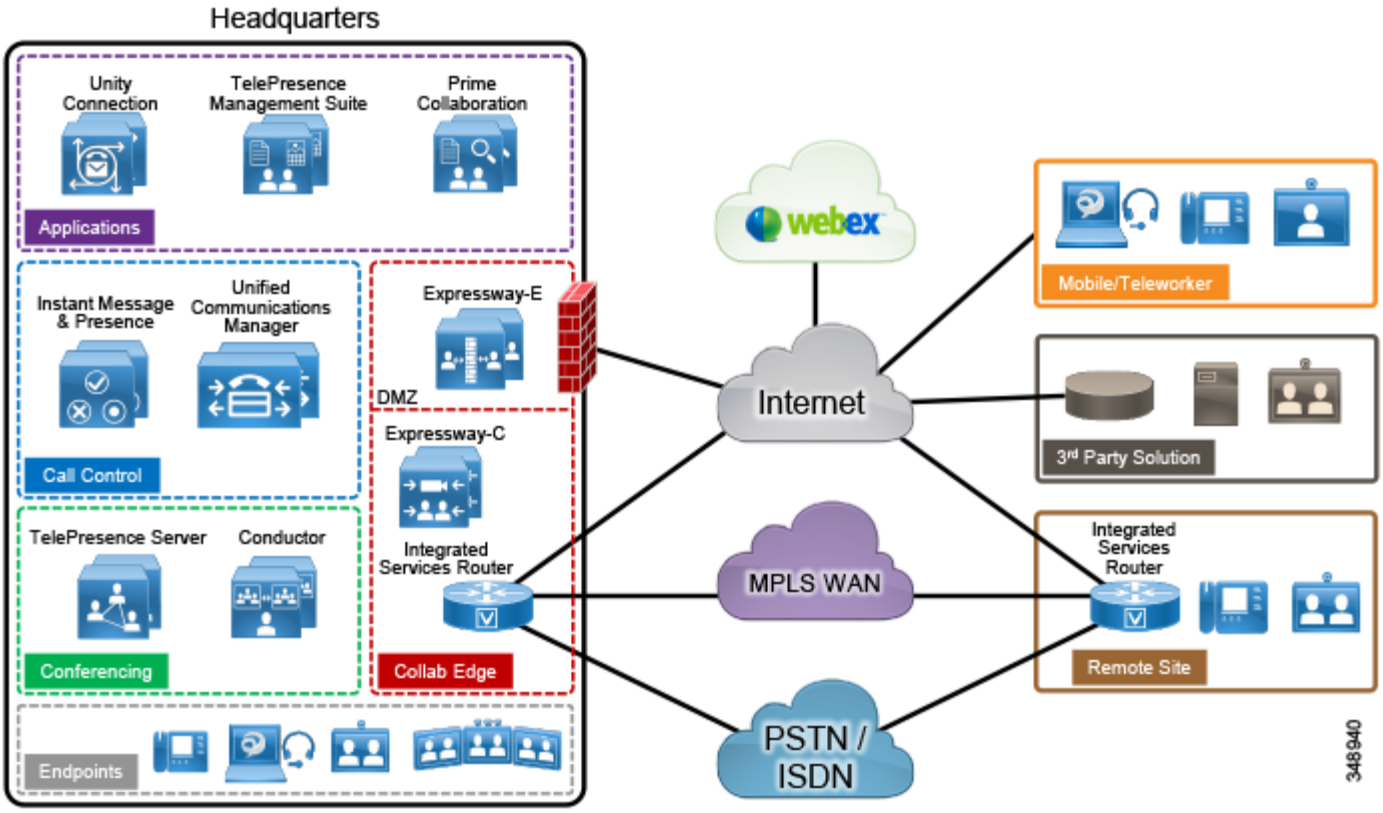


表 1-2に、このアーキテクチャで使用されている製品を示します。製品の分類と役割定義がしやすいように製品をモジュールに分けて記載しています。この CVD の内容はこのモジュールと同じ構成になっています。

表 1-2　エンタープライズ コラボレーション向けシスコ推奨アーキテクチャのコンポーネント

モジュール	コンポーネント	目的
コール制御	Cisco Unified Communications Manager（Unified CM） Cisco Unified Communications Manager IM and Presence Service Cisco Integrated Services Router（ISR）G2/G3	コール制御は、ユーザとエンドポイントに対し、登録、呼処理、リソース管理、およびインスタント メッセージおよびプレゼンスの機能を提供します。また、リモート オフィスのリモート サイト耐障害性も備えています。
会議	Cisco TelePresence Conductor Cisco TelePresence Server Cisco WebEx Software as a Service（クラウド） Cisco WebEx Meetings Server（オンプレミス）	会議では、3 者以上が音声、ビデオ、およびコンテンツ共有によりリアルタイムで通信できます。リソースはオンプレミス、クラウドでのホスティング、またはこの両方で提供されます。
コラボレーション エッジ	Cisco Expressway-C Cisco Expressway-E Cisco Integrated Services Router（ISR）G2/G3 Cisco アグリゲーション サービス ルータ（ASR）	コラボレーション エッジは、リモート登録サービス、外部通信、相互運用性を提供します。
コア アプリケーション	Cisco Unity Connection Cisco Prime Collaboration Provisioning Standard Cisco TelePresence Management Suite（TMS）および機能拡張	アプリケーションにより、音声メッセージ、管理、分析、および会議リソースのスケジュールなど、幅広いサービスがカバーされます。
サイジング	このマニュアルのすべての章に記載されている製品 Virtual Machine Placement Tool（VMPT）	このマニュアルで説明するすべてのモジュールのサイジングと、仮想マシンの配置の例。

ネットワーク サービス

エンタープライズ コラボレーション向けプリファード アーキテクチャでは、構造化されて可用性と回復力が高いネットワーク インフラストラクチャ、およびドメイン ネーム システム（DNS）、DHCP（Dynamic Host Configuration Protocol）、TFTP（Trivial File Transfer Protocol）、ネットワーク タイム プロトコル（NTP）を含むネットワーク サービスの統合セットが必要です。シスコのアプリケーションおよびエンドポイントでこれらの基本ネットワーク サービスがどのように使用されるかについて詳しくは、『Cisco Collaboration SRND』の「Network Services」の項を参照してください。

仮想化

複数のアプリケーションを仮想化して物理サーバ上で統合することで、コストを節約し、ラックスペースを最小限に抑え、所要電力量を削減し、導入と管理を簡素化できます。仮想化は、組織で変更が必要になる際のハードウェアの再導入とソフトウェア アプリケーションのスケーリングにも対応します。

Cisco Unified Communications on the Cisco Unified Computing System（UCS）

Cisco UCS サーバは、ユニファイド コミュニケーション（UC）コア アプリケーションを使用して十分なテストが行われており、仮想環境で信頼性と一貫したパフォーマンスを実現することが確認されています。UC アプリケーションを UCS サーバに導入するには 2 つのオプションがあります。

- UCS テスト済みリファレンス構成（TRC）の UC

  UCS TRC は、UCS サーバ コンポーネントの特定のハードウェア構成です。これらのコンポーネントには、CPU、メモリ、ハード ディスク（ローカル ストレージの場合）、RAID コントローラ、および電源などがあります。特定の TRC については、『UC Virtualization Supported Hardware』の Web サイトを参照してください。

- UCS 仕様ベースの UC

  UCS 仕様ベースのハードウェア構成では、UC アプリケーションの検証は明示的に実施されていません。したがって、UC アプリケーションが UCS 仕様ベースのハードウェアにインストールされる場合に、UC アプリケーション仮想マシンのパフォーマンスの予測や保証は行われません。この場合、シスコはガイダンスのみを提供します。プリセールスでのハードウェア設計によって、UC アプリケーションが必要とするパフォーマンスを実現できるかどうかの確認は、お客様の責任で行っていただきます。

『Unified Communications in a Virtualized Environment 』のすべてのルールに準拠している場合は、これらのオプションはいずれも Cisco Technical Assistance Center（TAC）により完全にサポートされます。

Cisco Business Edition 7000（BE7000）

Cisco BE7000 は、仮想ハイパーバイザとアプリケーション インストール ファイルがプリインストールされており、すぐに利用できる状態で出荷される仮想化 UCS 上に構築されています。BE7000 は、UCS TRC であり、UC アプリケーションが特定の UCS 設定で明示的にテストされています。Cisco BE7000 ソリューションは、1 つの統合プラットフォーム上で、高度な音声、ビデオ、メッセージ、インスタント メッセージおよびプレゼンス、およびコンタクト センターの各機能を提供します。Cisco BE7000 について詳しくは、『Cisco Business Edition 7000 Data Sheet』を参照してください。

コア アプリケーション

エンタープライズ コラボレーション向け推奨アーキテクチャでは、ハードウェアとソフトウェアの冗長性を提供するため、次の仮想化アプリケーションが複数の Cisco UCS サーバに導入されます。

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Unity Connection
- Cisco Expressway（Expressway-C および Expressway-E で構成）
- Cisco TelePresence Conductor
- Cisco TelePresence Server
- Cisco TelePresence Management Suite

重要なビジネス アプリケーションの可用性を最大限に引き出すため、常に冗長構成で導入することを推奨します。

コラボレーション エンドポイント

この CVD ガイドでの推奨事項は、シスコの音声およびビデオ エンドポイント（Cisco Jabber などのソフト クライアントを含む）を前提としています。これらのエンドポイントは SIP を使用して Cisco Unified Communications Manager（Unified CM）に登録します。表 1-3に、最適な機能とユーザ エクスペリエンスを実現するための推奨エンドポイントを示します。

表 1-3　　シスコ コラボレーション エンドポイント

製品	説明
モバイル: • Jabber for Android • Jabber for iPhone/iPad **デスクトップ:** • Jabber for Mac • Jabber for Windows	音声、ビデオ、ボイスメール、インスタント メッセージ、およびプレゼンス機能を統合し、モバイル デバイスとパーソナル コンピュータのためのセキュア エッジ トラバーサルを備えたソフト クライアント。
Cisco Unified IP Phone 7821	Public Space、複数回線電話
Cisco Unified IP Phone 8800 シリーズ	オフィスでの一般利用、複数回線電話
Cisco Unified IP Phone 8831	IP 会議用電話
Cisco EX シリーズ	リモート アクセス機能を備えたデスクトップ向けパーソナル TelePresence エンドポイント
Cisco DX シリーズ	デスクトップ向けパーソナル TelePresence エンドポイント
Cisco MX シリーズ	多目的ルーム向け TelePresence エンドポイント
Cisco SX シリーズ	インテーグレータ向け TelePresence エンドポイント
Cisco IX シリーズ	イマーシブ TelePresence ルーム システム

コール制御

改訂日：2015 年 1 月 22 日

この章では、Enterprise Collaboration 向けのシスコ プリファード アーキテクチャ（PA）のコール制御機能について説明します。

展開に際して、PA 設計ガイドラインおよび推奨事項以外の特定の要件が課せられることがあります。その場合は *Cisco Collaboration SRND* や関連する製品のマニュアルなど、他のマニュアルを使用しなければならない場合があります。

この章の最初の部分では、アーキテクチャについて概説し、いくつかの基本的な設計概念を紹介します。2 番目の部分では、展開に関する考慮事項についてより詳しく説明します。アーキテクチャの項では、冗長の概念、高可用性、コンピュータ/テレフォニー インテグレーション（CTI）、IM and Presence のアーキテクチャなどのトピックについて解説し、本書の例で使用される架空のカスタマー トポロジを紹介します。この章の中心となるのは展開の概要の項です。概念の抽象的な説明よりも、このセクションで紹介されている展開例を見れば、特定の設計に関する決定の背景について、より明確に理解できるようになります。展開の概要の項で取り上げているトピックとしては、DNS 要件、クラスタ プロビジョニング、証明書の管理、ダイヤル プラン設定、LDAP を使用したユーザ プロビジョニング、メディア リソース、SIP トランクの考慮事項、エンドポイント プロビジョニング、マルチクラスタの考慮事項などがあります。展開の概要の項でのトピックの順番は、推奨される設定順になっています。

この章の変更点

表 2-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 2-1　本リリースで追加または変更された情報

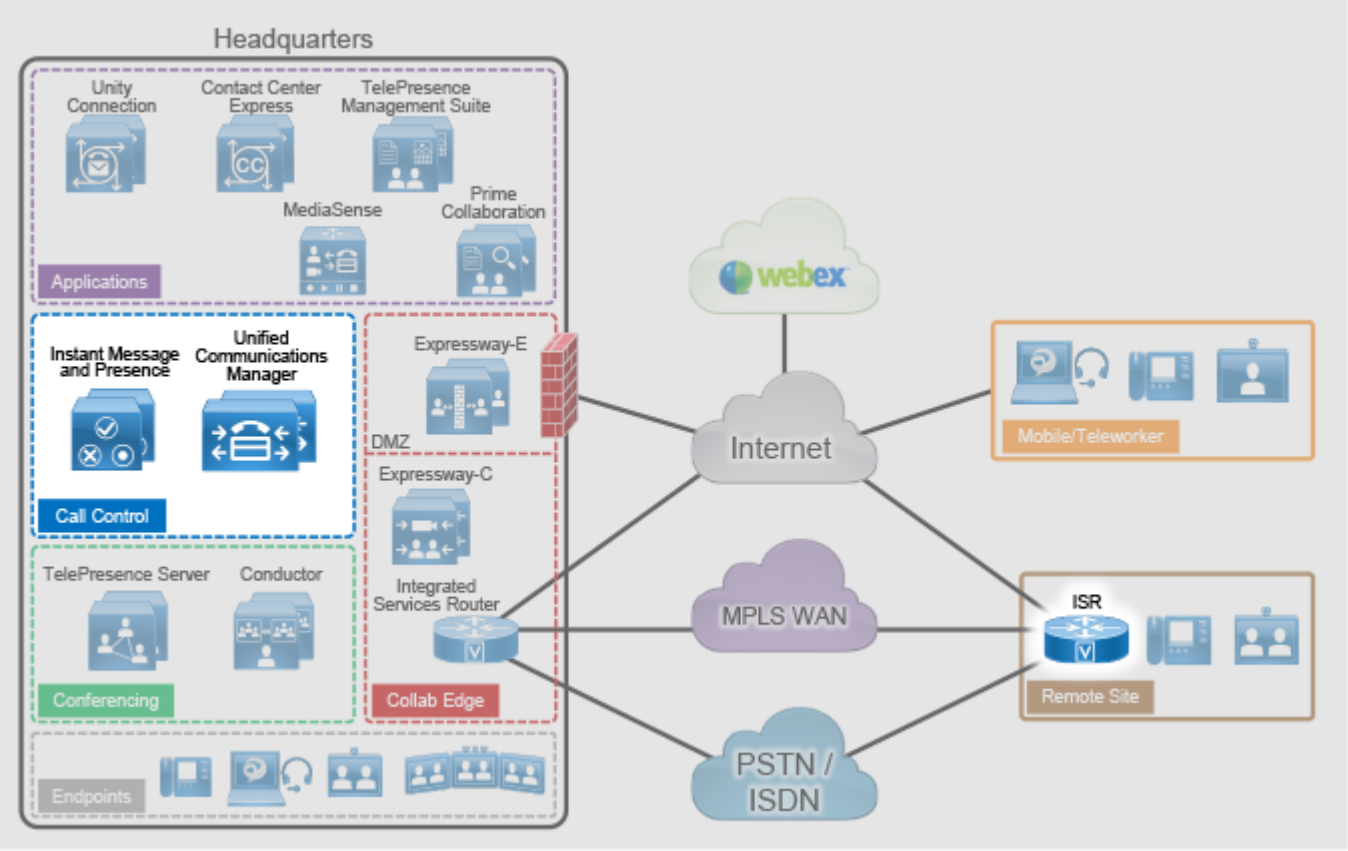
新規トピックまたは改訂されたトピック	説明箇所	改訂日
会議用のエンタープライズ固有の番号付け（ESN）方式が簡素化されました	表 2-11	2015 年 1 月 22 日

コア コンポーネント

コア アーキテクチャには次の重要な要素が含まれています（図 2-1）

- Cisco Unified Communications Manager
- Cisco Unified Communications Manager IM and Presence Service
- Cisco Integrated Services Router（ISR）

図 2-1　　プリファード アーキテクチャの概要



主な利点

- コール制御が 1 か所で集中管理され、そこから複数のリモート サイトが制御されます。
- 操作と管理が一元化されます。
- 一般的なテレフォニー機能がどの音声エンドポイント、ビデオ エンドポイントでも使用できます。
- 音声エンドポイントおよびビデオ エンドポイントのために単一のコール制御および統合されたダイヤル プランが提供されます。
- 重要なビジネス アプリケーションの可用性が高くなり、冗長化されます。

アーキテクチャ

音声コールとビデオ コールの処理は、企業のコミュニケーション システムによって提供される重要な機能です。この機能は、特定のタイプの呼処理エンティティまたは呼処理エージェントによって処理されます。呼処理の操作は重要であるため、ユニファイド コミュニケーションの配置を設計して、呼処理システムが、必要なユーザ数およびデバイス数を処理するのに十分なスケーラビリティと、ネットワークおよびアプリケーションのさまざまな異常または障害を処理するのに十分な復元性を持つようにすることが重要です。

この章では Cisco Unified Communications Manager（Unified CM）および Survivable Remote Site Telephony（SRST）を使った、スケーラブルで復元性の高い呼処理システムを設計するためのガイダンスを行います。集中型 Unified CM クラスタはすべてのカスタマー サイトに対して呼処理サービスを実装します。集中型 Unified CM クラスタの一部である Unified CM IM and Presences Service はエンタープライズに対してインスタント メッセージとプレゼンス サービスを実装します。Cisco Survivable Remote Site Telephony（SRST）は、企業 WAN の信頼性が音声サービスの可用性要件を満たさない場合に、リモート サイトに対してバックアップ サービスを実装するために使用されます。

Cisco Unified CM は、小規模～非常に大規模な単一サイト配置、マルチサイト集中型呼処理配置、およびマルチサイト分散呼処理配置に、呼処理サービスを提供します。Unified CM はシスコ コラボレーション ソリューションの中核をなし、音声、ビデオ、TelePresence、IM and Presence、メッセージング、モビリティ、Web 会議、セキュリティを提供する基盤として機能します。

VPN や Cisco Expressway などのコラボレーションに関する様々な先端ソリューションを使えば、インターネットから Enterprise Collaboration ネットワークおよび Unified CM にアクセスして、リモート アクセスおよび business-to-business のセキュアなテレプレゼンスとビデオ コミュニケーションを可能にすることもできます。

Unified CM の役割

Cisco Unified CM はすべてのシスコ コラボレーション展開における中央のコール制御コンポーネントです。Unified CM は、コール制御、エンドポイントの登録、エンドポイントの設定、コール アドミッション制御、コーデック ネゴシエーション、トランク プロトコル変換、CTI などの基盤サービスを提供します。Unified CM は、管理とプロビジョニングの中心です。会議メディア リソース、ゲートウェイ、およびその他のコンポーネントを含む、すべてのコンポーネントへのアクセスを Unified CM が調整できるように、これらのコンポーネントに対するすべての SIP トランクは Unified CM で終端します。コール ルーティングは Unified CM に適用されるダイヤル プラン設定により制御されます。

IM and Presence Service の役割

Cisco Unified CM IM and Presence Service はオンプレミスのインスタント メッセージおよびプレゼンスを提供します。各種標準に基づく XMPP を使用するほか、SIP IM プロバイダとの相互運用のために SIP もサポートしています。Cisco Unified CM IM and Presence Service はオンプレミス ソリューションです。もう 1 つの Cisco インスタント メッセージおよびプレゼンス サービスである Cisco WebEx Messenger はクラウドベースのサービスであり、このマニュアルでは取り上げません。

SRST の役割

低速な、または信頼できない WAN リンクにより集中型呼処理プラットフォームから切り離された支店のロケーションに Cisco デスク フォンを展開する場合、ローカル呼処理の冗長化を検討することが重要です。各支社のロケーションで集中型呼処理プラットフォームへの接続が失われた場合は、そこにある Cisco IOS ルータで Survivable Remote Site Telephony（SRST）を利用することにより、デスク フォンの基本的な IP テレフォニー サービスを維持できます。ただし、デバイスが SRST に登録された場合に使用可能な一連の対ユーザ機能は、電話が Unified CM に登録された場合よりもずっと少なくなります。

Survivable Remote Site Telephony（SRST）による Unified CM の冗長性

Cisco IOS SRST は、Unified CM クラスタから離れたロケーションにあるエンドポイントに、可用性の高い呼処理サービスを提供します。Unified CM クラスタリングの冗長性方式は、LAN または MAN 環境内の呼処理などのアプリケーション サービスに高レベルの冗長性をもたらします。ただし、WAN などの低速リンクによって中央の Unified CM クラスタから分離されたリモート ロケーションの場合、冗長性方式として SRST を使用すると、リモート サイトと中央サイトの間でネットワーク接続が失われたときに、基本的な呼処理サービスをこれらのリモート ロケーションに提供できます。呼処理サービスが重要であり、Unified CM クラスタへの接続が失われた場合にも呼処理サービスを維持する必要がある各リモート サイトには、SRST 対応の Cisco IOS ルータを配置することを推奨します。これらのリモート ロケーションのエンドポイントは、Unified CM 内の適切な SRST リファレンスとともに設定する必要があります。Unified CM サブスクライバへの接続を使用できない場合に、呼処理サービス用にどのアドレスを使用して SRST ルータに接続するかをエンドポイントが認識するようにするためです。

Unified CM と IM and Presence Service のクラスタリング

Unified CM はクラスタリングの概念をサポートしています。Unified CM アーキテクチャにより、サーバ ノード グループは単一の呼処理エンティティとして連携できるようになります。このサーバ ノード グループをクラスタと呼びます。

Cisco Unified CM にはパブリッシャとサブスクライバの 2 種類のノードがあります。

- Unified CM パブリッシャ

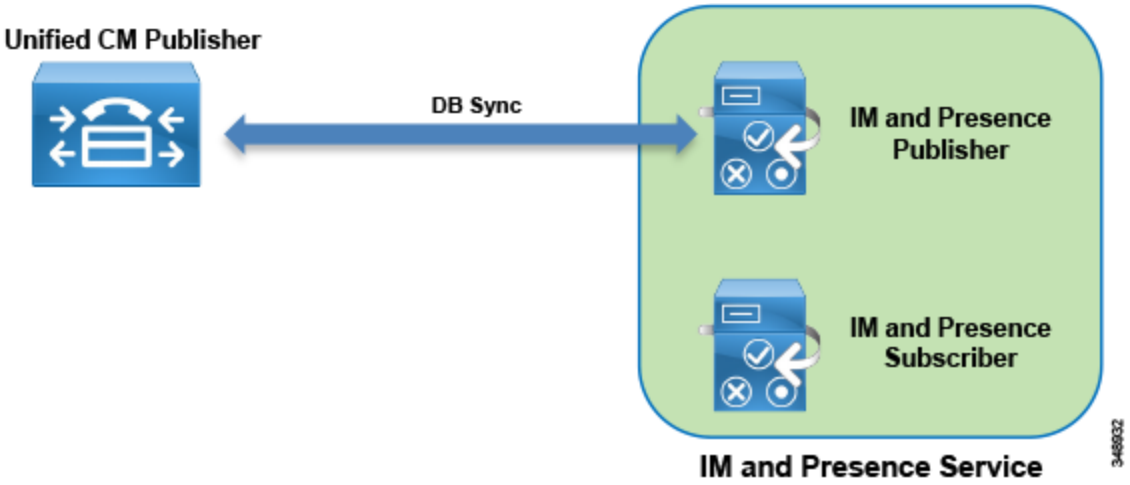
  パブリッシャはすべてのクラスタの必須サーバ ノードです。各クラスタにパブリッシャは 1 つだけ存在できます。このサーバ ノードにはクラスタ設定が含まれており、クラスタ内の他のすべてのサブスクライバにデータベース サービスを提供します。この設計では Unified CM パブリッシャは専用ノードなので TFTP 要求やエンドポイントの登録、呼処理は扱いません。

- Unified CM サブスクライバ

  サブスクライバ ノードは、パブリッシャにサブスクライブして、データベース情報のコピーを取得します。たとえば、サブスクライバ ノードには Unified CM TFTP ノードや Unified CM 呼処理サブスクライバ ノードなどがあります。

Cisco IM and Presence ノードには同じクラスタリングの概念があります。最初の IM and Presence ノードは IM and Presence パブリッシャです。その他の IM and Presence ノードは IM and Presence サブスクライバで、IM and Presence パブリッシャからデータベースのコピーを取得します。IM and Presence パブリッシャは Unified CM パブリッシャと通信を行い、大半の IM and Presence 設定は実際には Unified CM パブリッシャにより行われます（Unified CM ユーザ、プレゼンス ユーザが利用できる UC サービス、サービスのアクティブ化など）。このため、IM and Presence パブリッシャをはじめとするすべての IM and Presence ノードは、より大きな Unified CM and IM and Presence Service クラスタのサブスクライバであると見なされます。図 2-2 に Unified CM パブリッシャと 2 つのノードを持つ IM and Presence クラスタの関係を示します。

図 2-2　　Unified CM と 2 つのノードを持つ IM and Presence クラスタとの関係



高可用性

Unified CM および IM and Presence ノードは高可用性インフラストラクチャで展開する必要があります。たとえば、二重化電源の使用と無停電電源（UPS）の使用を組み合わせると、電力の可用性が最大になります。ネットワーク面から見ると、プラットフォーム サーバは複数の上流側のスイッチに接続する必要があります。

また、Unified CM システムおよび IM and Presence システムは、アプリケーション レベルでも高可用性処理を行います。

この設計の Unified CM では、冗長化のために 2 つの TFTP サーバを配置する必要があります。呼処理ノードは一対一（1:1）の冗長性をもって配置する必要があります。つまり、それぞれのプライマリ呼処理サブスクライバについてバックアップ呼処理サブスクライバがあります。この 100%:0% 冗長化設計は 50%:50% 冗長化設計に比べ、Unified CM グループおよびデバイス プールが少なくてすむ、冗長化オプションが少ないのでデバイス設定と分散が簡素化されるなど、多くの利点があります。

Cisco IOS Survivable Remote Site Telephony（SRST）は Unified CM クラスタから離れたロケーションにあるエンドポイントに対して、WAN リンクがダウンしたときに高可用性のある呼処理を提供します。

個々の Cisco IM and Presence ノードはサブクラスタでグループ化されます。1 つのサブクラスタは 1 つないし 2 つのノードを持つことができます。サブクラスタで 2 番目のノードを追加すると、高可用性が提供されます。高可用性が推奨されるため、この設計では各サブクラスタが 2 つのノードで構成されています。2 つのノードを持つサブクラスタでは、サブクラスタの 1 つのサーバに関連付けられたユーザは、フェイルオーバー イベントが発生した場合に、そのサブクラスタのもう一方のサーバを自動的に使えるようになります。各ノード ペアで 2 つのノード間のユーザ割り当てのバランスをとることが推奨されます。IM and Presence パブリッシャは、他の IM and Presence サブスクライバとまったく同じように、プレゼンス クライアントからの IM and Presence 情報を処理し、IM and Presence サブスクライバの 2 つのノードの 1 つとして配置されます。

コンピュータ テレフォニー インテグレーション（CTI）

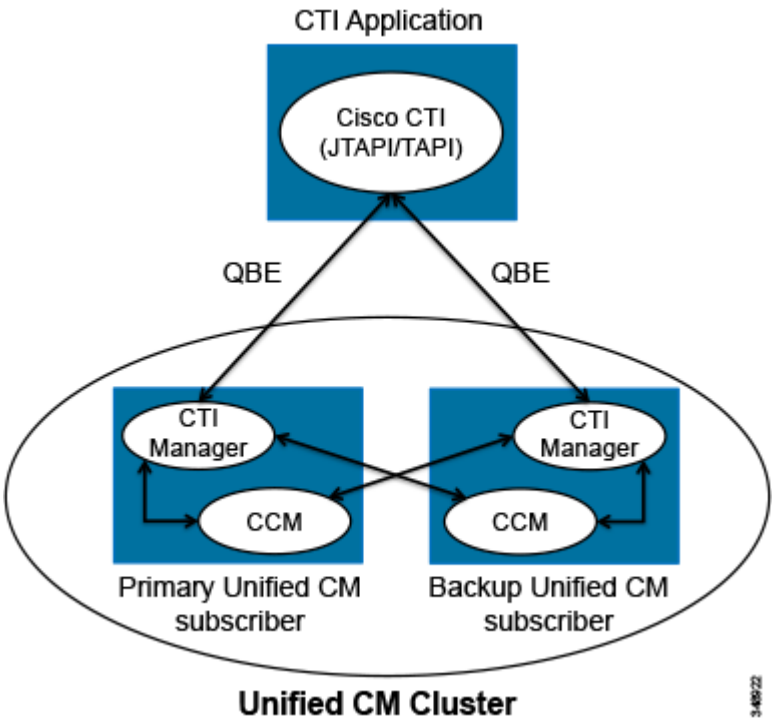
Cisco コンピュータ テレフォニー インテグレーション（CTI）を利用すると、Cisco Unified CM で使用可能な豊富なフィーチャ セットだけでなく、サードパーティ製のアプリケーションも使用できるようになります。

CTI のアーキテクチャ

Cisco CTI は、次のコンポーネントで構成されます（図 2-3 を参照）。これらは互いに対話し、Cisco Unified CM で使用可能なテレフォニーフィーチャ セットを各アプリケーションで利用できるようにします。

- CTI アプリケーション：特定のテレフォニー機能を提供するために作成されたシスコまたはサードパーティのアプリケーション。このアプリケーションは JTAPI または TAPI インターフェイスを使用できます。CTI アプリケーションと Unified CM との間のプロトコルは Quick Buffer Encoding（QBE）です。
- 次のサービスを持つ Unified CM サブスクライバ：
  - CCM：Cisco CallManager サービス。テレフォニー処理エンジンです。
  - CTI Manager（CTIM）：プライマリまたはセカンダリ モードで動作する 1 つ以上の Unified CM サブスクライバで実行され、Cisco IP デバイスを制御およびモニタできるようにテレフォニー アプリケーションを認証および許可するサービス。

図 2-3　　CTI のアーキテクチャ



CTI の高可用性

CTI Manager の高可用性は、プライマリ CTI Manager に障害が発生した場合にバックアップ CTI Manager Service に接続することができる、CTI アプリケーションに依存します。プライマリ Unified CM サブスクライバの CTI Manager と CCM サービスの両方に障害が発生した場合（プライマリ Unified CM サブスクライバ全体に障害が発生した場合など）、バックアップ Unified CM サブスクライバで実行されている CCM と CTI Manager サービスの両方がアクティブ化され、CTI Manager サービスは同じバックアップ Unified CM サブスクライバ上にある CCM サービスに登録されている各デバイスを監視し、制御します。プライマリ CTI Manager Service に障害が発生したものの、プライマリ CCM Service はまだ実行中の場合（1:1 冗長化がプライマリ/バックアップ Unified CM サブスクライバの 100 %/0 % 分散で実現されている場合などが想定されます）、すべてのデバイスはそのままプライマリ Unified CM サブスクライバ上で実行されている CCM Service に登録されたままになり、バックアップ Unified CM サブスクライバで実行されている CTI Manager がアクティブ化されて、別のノード（この場合はプライマリ Unified CM サブスクライバ）で実行中の CCM サービスに登録されてる CTI デバイスであってもそれらを監視し、制御します。

CTI のキャパシティ プランニング

3 種類の CTI リソースについての次のキャパシティの上限を超えないようにしてください。

- 所定の CTI Manager インスタンス（CTI Manager サービスを実行している Unified CM ノード）に接続される CTI アプリケーションの最大数。CTI サーバベースのアプリケーションではこの数は通常少ないのですが、デスクフォン モードの Jabber クライアントなど、CTI クライアントベースのアプリケーション（この場合は各 Jabber クライアントが CTI アプリケーションと見なされます）では、多数の Jabber クライアントを展開する場合にこの上限を超えないようにすることが重要です。
- 所定の Unified CM 呼処理サブスクライバに登録される CTI 対応エンドポイントの最大数。
- 1 つの CTI Manager インスタンスによって監視され、制御される CTI 対応エンドポイントの最大数。Unified CM ノードで実行される CTI Manager サービスは、その Unified CM ノードに登録されたエンドポイントだけを監視するのが理想的です。しかし CTI Manager サービスが他の Unified CM ノードに登録されたエンドポイントを監視することも可能です。

CTI の上限は上記の 3 つの CTI リソースすべてで同じです。CTI のキャパシティの上限は OVA テンプレートの種類によって異なります。CTI の上限に達したら、CTI Manager サービスを実行する別の Unified CM 呼処理ノードのペアを配置します。

IM and Presence のアーキテクチャ

Cisco Unified CM IM and Presence Service はオンプレミスのインスタント メッセージおよびプレゼンスを提供します。このソリューションの主要なプレゼンス コンポーネントは IM and Presence Service です。これには Extensible Communications Platform（XCP）が組み込まれ、ユーザの可用性ステータスとコミュニケーション手段に関する情報を収集する SIP/SIMPLE および Extensible Messaging and Presence Protocol（XMPP）をサポートしています。ユーザの可用性ステータスは、ユーザが電話機などの通信デバイスをアクティブに使用しているかどうかを示します。

アプリケーション（シスコ製またはサードパーティ製）にプレゼンスを統合することによって、エンド ユーザ エクスペリエンスと効率性を向上させるサービスを提供できます。さらに、Cisco Jabber はインスタント メッセージングとプレゼンス ステータスも統合した IM and Presence Service の対応クライアントです。

IM and Presence Service は Cisco Unified Computing System（UCS）プラットフォーム上の Unified CM で使用されるのと同じ基本アプライアンス モデルおよびハードウェアを使用します。

IM and Presence Service は IM and Presence クラスタとして展開されます。IM and Presence クラスタは最大 6 つのノードで構成されます。1 つのノードはパブリッシャとして指定され、最大 5 つのノードがサブスクライバ ノードになります。Unified CM と IM and Presence Service のクラスタリングおよび高可用性の項で説明されているように、IM and Presence ノードはサブクラスタでグループ化され、各サブクラスタは高可用性を得るために 2 つのノードで構成されます。サイジングの項で説明されているように、1 つのサブクラスタを展開すると、最大 15,000 人のユーザをサポートできます。IM and Presence パブリッシャは IM and Presence サブスクライバとまったく同じように IM and Presence 要求を処理するので、最初のサブクラスタは IM and Presence パブリッシャと 1 つの IM and Presence サブスクライバで構成されます。

Unified CM と IM and Presence Service のクラスタリングの項で説明されているように、IM and Presence ノードはより大きな Unified CM and IM and Presence Service クラスタの一部と見なされます。

Unified CM and IM and Presence Service クラスタの展開

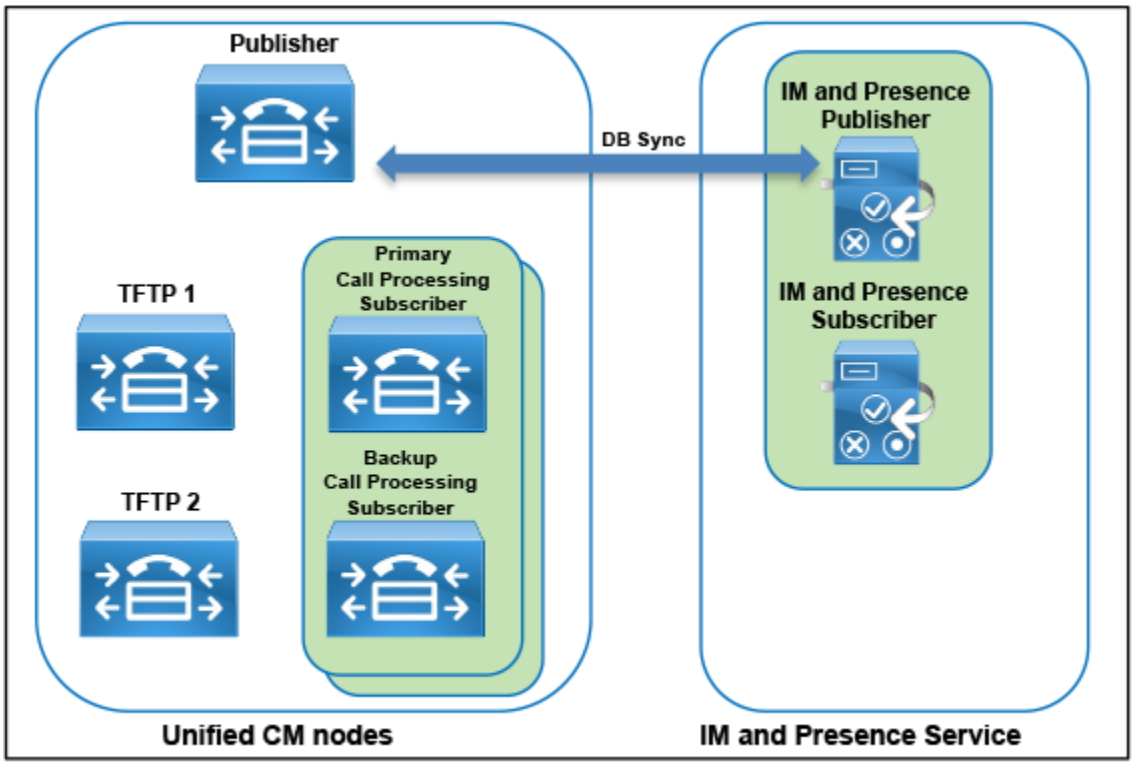
Cisco Unified CM and IM and Presence Service クラスタは次のノードで構成されます。

- 1x Cisco Unified CM パブリッシャ
- 2x（1 ペア）Cisco Unified CM TFTP サーバ サブスクライバ
- 2x（1 ペア）Cisco Unified CM 呼処理サブスクライバ（拡張のためにペアを追加）
- 2x（1 ペア）Cisco Unified IM and Presence ノード（拡張のためにペアまたはサブクラスタを追加）

拡張のために追加する Unified CM 呼処理および IM and Presence のペア数については、サイジングの章で説明します。

図 2-4 は、最大 10,000 台のデバイスおよび 10,000 人のユーザを持つ Unified CM and IM and Presence Service クラスタ展開の例です。サイジング情報の詳細については、サイジングの章を参照してください。

図 2-4　Unified CM and IM and Presence Service クラスタの展開



エンドポイント

Jabber

Cisco Jabber クライアントは、音声、ビデオ、およびインスタント メッセージのためのコア コラボレーション機能をユーザに提供します。Cisco Jabber は Windows、Mac、およびスマートフォンやタブレットなどのモバイル デバイスを含む幅広いプラットフォームで利用できます。

Cisco Jabber は次の 2 つのモードのいずれかで展開できます。

- フル UC と Cisco Jabber for Everyone（IM のみ）モード

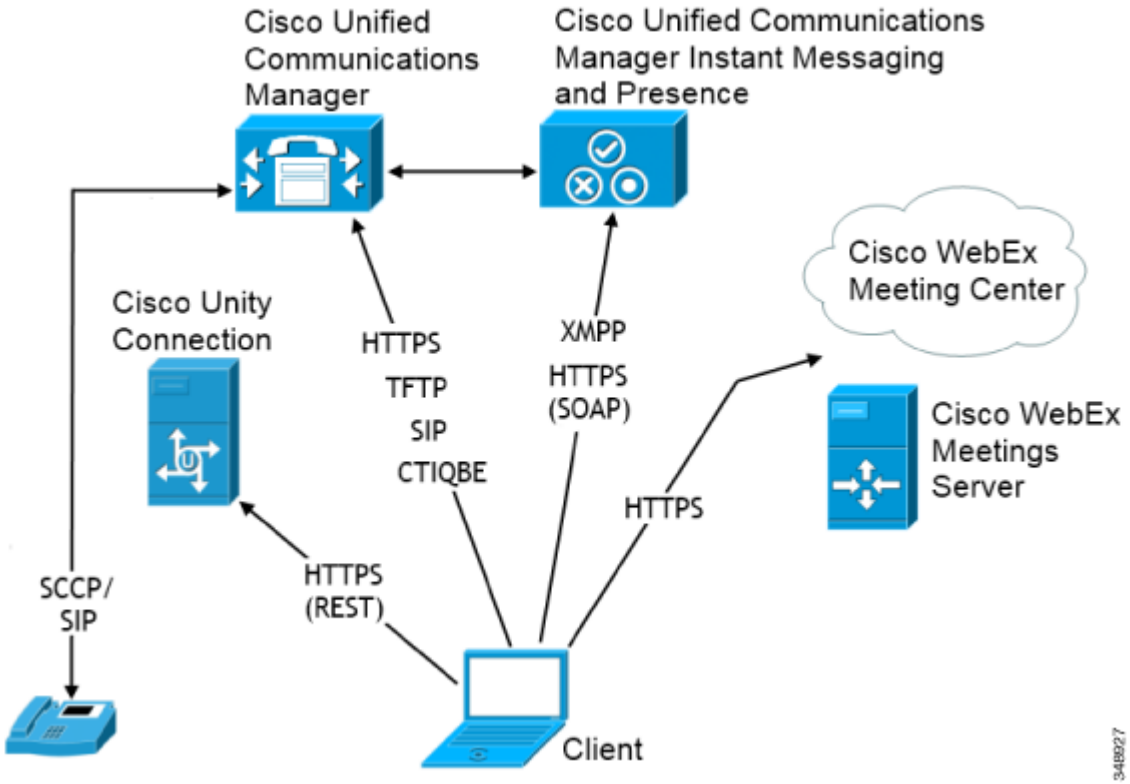
  これはデフォルト モードです。ユーザのプライマリ認証は IM and Presence サーバに対して行われます。これは、このプリファード アーキテクチャ設計で使用されるモードであり、本マニュアルで取り上げられています。

- 電話モード

  電話モードでは IM and Presence Service は必要ありません。

図 2-5 は Cisco Unified Communications Manager IM and Presence が含まれたオンプレミス展開のアーキテクチャを示しています。

図 2-5　Cisco Unified Communications IM and Presence のアーキテクチャ



Cisco Jabber は、サービスに接続するために次の情報を必要とします。

- ユーザがクライアントにサインインできる認証のソース

  フル UC および IM のみモードでは、認証のソースは IM and Presence サービスです。電話のみモードでは、Unified CM です。

- サービスのロケーション

  サービスには IM and Presence、ディレクトリ、CTI、ボイスメール、会議が含まれています。

この情報をクライアントに提供するには、Manual Connection メソッドを介した Service Discovery メソッドの使用を推奨します。Service Discovery メソッドを使うと、クライアントが自動的に配置され、サービスに接続します。

この設計では、ユーザが最初に Jabber クライアントで電子メール アドレスを入力したときに取得される SRV record _cisco-uds を使って、クライアントが自動的にサービスと設定を検出します。

Jabber コンタクト ソースは Enhanced Directory Integration（EDI）（Microsoft Windows デスクトップの場合）か、または Basic Directory Integration（BDI）（OS X、iOS、Android など他のプラットフォームの場合）による LDAP コンタクト ソースが可能です。別のコンタクト ソースとしては Unified CM のユーザ データ サービス（UDS）が可能ですが、その場合は Unified CM でサポートされるユーザ数が少なくなります。

マルチクラスタに関する考慮事項

マルチクラスタ展開では、SIP トランクを介して個々の Unified CM クラスタすべてを相互接続します。個々のクラスタ間のセッション トラバーサルを防ぐには、フルメッシュの SIP トランクを展開します。4 つ以上のクラスタでは、Cisco Unified CM Session Management Edition（SME）を展開してダイヤル プランとトランキングを一元化し、フルメッシュ SIP トランク トポロジの複雑さを回避します。Cisco Unified CM SME については、このマニュアルでは取り上げません。SME の詳細については、『*Cisco Collaboration SRND*』を参照してください。

マルチクラスタ展開では、グローバル ダイヤル プラン レプリケーション（GDPR）を使用して、クラスタ間でダイヤル プラン情報を複製します。GDPR はディレクトリ番号ごとに 1 つの +E.164 番号、1 つの Enterprise Significant Number（ESN）、そして最大 5 個の英数字 URI をアドバタイズできます。ESN はディレクトリ番号に相当する、サイト内の短縮ダイヤルです。GDPR を通じてアドバタイズされ、通知された情報により、次のようなダイヤル手順での決定論的なクラスタ内ルーティングが可能になります。

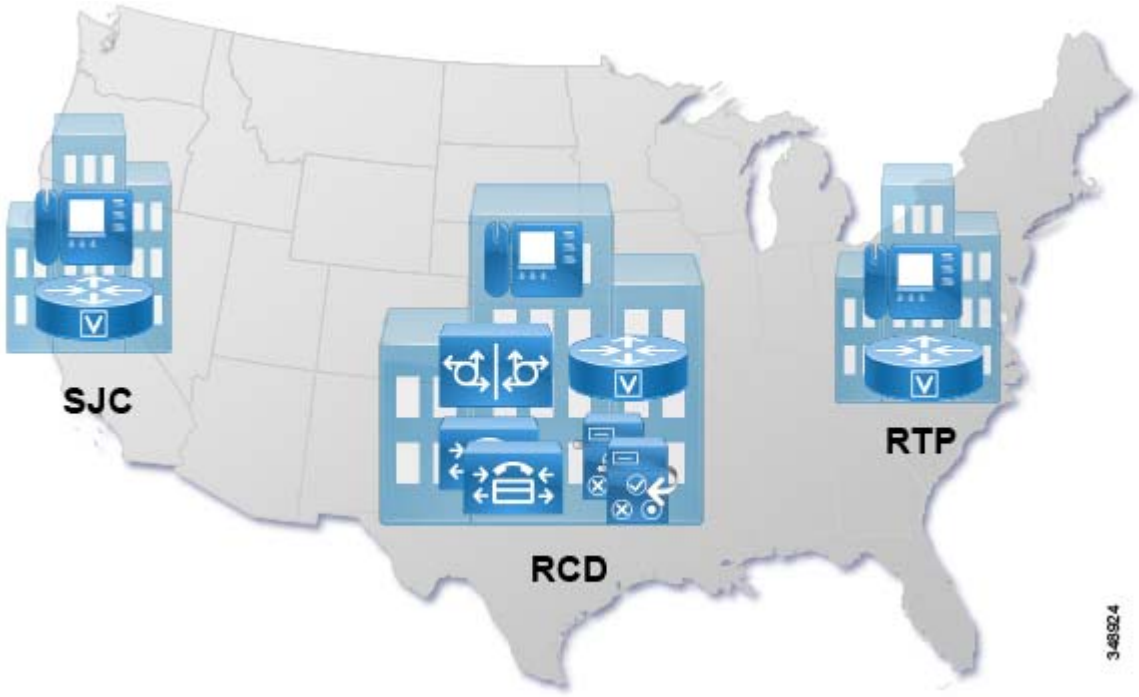
- アドバタイズされた +E.164 番号に基づく +E.164 ダイヤリング
- アドバタイズされた ESN に基づくエンタープライズのサイト内短縮ダイヤリング
- アドバタイズされた URI に基づく英数字 URI ダイヤリング

IM and Presence 機能は、単一クラスタ内での通信により制限されます。プレゼンスとインスタント メッセージングの能力と機能を拡張するには、これらのスタンドアロンのクラスタにピア関係を設定することで、同じドメイン内の複数のクラスタ間で通信できるようになります。この機能により、1 つのクラスタ内のユーザが、同じドメイン内の異なるクラスタにいるユーザと通信したり、プレゼンスをサブスクライブしたりできます。フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence クラスタと、同じドメイン内の他のそれぞれの Cisco IM and Presence クラスタとの間に、個別のピア関係が設定されている必要があります。クラスタ内のピアはリモートの Unified CM cluster IM and Presence パブリッシャ ノードの IP アドレスとして設定されます。

トポロジの例

このマニュアルでは、米国の 3 つのサイト（SJC、RCD、RTP）にサービスを提供する集中型の呼処理展開を想定しています。Unified CM および IM and Presence Service の各サーバは集中的に RCD に配置されます。中央の PSTN アクセスは RCD でも同様に行われます。SJC と RTP は、ローカルで Survivable Remote Site Telephony (SRST) を設定され、RCD サイトへの WAN 接続がダウンした場合のローカル PSTN アクセスを備えた小さなサイトであると想定します。図 2-6 はこのトポロジの例を示しています。

図 2-6　　トポロジの例



マルチクラスタに関する考慮事項のために、このマニュアルでは、2 つのクラスタ（図 2-6 で示されている米国のクラスタと、ヨーロッパ、中東、アフリカ（EMEA）を対象とした 2 つ目のクラスタ）による展開がトポロジの例として使用されます。

展開の概要

展開は集中型の Cisco Unified CM クラスタのプロビジョニングで始まり、さらに設定タスクとプロビジョニング タスクが続きます。次の項では、このマニュアルのプリファード アーキテクチャ設計に従って、コール制御をセットアップし、設定する方法について説明します。

- DNS 要件
- Cisco Unified CM and IM and Presence Service クラスタのプロビジョン
- Cisco Unified CM and IM and Presence の証明書管理
- Cisco Unified CM の初期設定
- その他の IM and Presence 設定
- ダイヤル プラン設定
- LDAP 同期によるユーザ プロビジョニング
- LDAP によるユーザ認証
- Cisco Unified CM グループ設定
- 電話用 NTP
- 日付および時刻グループ
- メディア リソース
- デバイス プール
- SIP トランク
- エンドポイントのプロビジョニング
- マルチクラスタ展開向けの ILS 設定
- GDPR の設定（マルチクラスタのみ）
- Survivable Remote Site Telephony（SRST）展開
- エクステンション モビリティ
- ビジー回線フィールド（BLF）のプレゼンス
- コンピュータ テレフォニー インテグレーション（CTI）の展開

DNS 要件

ソリューションを展開する前に、展開するすべてのサーバで DNS 解決が使用できることを確認します。エンタープライズ DNS では、正引き（DNS 名から IP アドレス）と逆引き（IP アドレスから DNS 名）の両方のルックアップを設定する必要があります。

Jabber クライアント用の UDS ベースのサービス検出を有効にするのに加えて、すべての Unified CM パブリッシャ ノードおよび TFTP サブスクライバ ノードについて、DNS SRV レコードをプロビジョニングし、これらを_cisco-uds のサービス ロケーションとして定義します。例 2-1 は、多くの Unified CM ノードを _cisco-uds のサービス ロケーションとして定義した DNS SRV レコードの例です。

例 2-1　UDS ベースのサービス検出のための DNS SRV レコード

```
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          svr hostname   = us-cm-pub.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          svr hostname   = us-cm-tftp1.ent-pa.com
_cisco-uds._tcp.ent-pa.com     SRV service location:
          priority       = 10
          weight         = 10
          port           = 8443
          svr hostname   = us-cm-tftp2.ent-pa.com
```

例 2-1 では、3 つの Unified CM ノード（パブリッシャ ノードと 2 つの TFTP サブスクライバ ノード）はすべて UDS サービス検出のサービス ロケーションとして定義され、UDS サービス検出を使用した Jabber クライアントからの初回の UDS 要求の負荷が、アクティブなすべての Unified CM ノード間で均等に分散されています。

UDS サービス検出処理の一部として /cucm uds/clusterUser リソースを使用してホーム クラスタを配置した後に、Jabber クライアントは /cucm-uds/servers リソースを使用して、ユーザのホーム クラスタ内のすべての UDS ノードのリストを取得します。これにより、SRV レコードでパブリッシャだけをサービス ロケーションとして定義した場合でも、登録処理中の実際の UDS 要求が、すべての UDS ノード間でロード バランシングされます。

Cisco Unified CM and IM and Presence Service クラスタのプロビジョン

Unified CM and IM and Presence Service クラスタを展開するには、次のタスクを実行します。

1. 対象となるユーザ数とデバイス数に基づいて、必要な呼処理サブスクライバのペア数を決定します。
2. 対象となるユーザ数に基づいて、必要な IM and Presence ノード数を決定します。
3. 必要なすべてのクラスタ メンバーのネットワーク パラメータ（DNS 名、IP アドレスなど）を決定します。TFTP サーバも同様に考慮します。
4. シスコが提供する適切な OVA テンプレート ファイルを使用して、必要な数の仮想マシンを計算インフラストラクチャに展開します。これらの OVA ファイルの取得方法について詳しくは、次の場所にあるマニュアルを参照してください。

   http://docwiki.cisco.com/wiki/Downloading_OVA_Templates_for_UC_Applications
5. Cisco Prime Collaboration 展開で、すべてのメンバを含む Unified CM クラスタを定義し、タスク 4 で作成した仮想マシンにノードをマップします。
6. Cisco Prime Collaboration 展開を使用してすべてのノードを展開します。

Cisco Prime Collaboration 展開を使用してクラスタをプロビジョニングする方法に関する詳細は、以下の場所にある『*Cisco Prime Collaboration Deployment Administration Guide*』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html

Cisco Unified CM and IM and Presence の証明書管理

セッションを確立中に証明書を確認する必要がある場合はいつでも、2 つのサーバ間、または中央のサービスとクライアント アプリケーション（Cisco Jabber for Windows など）の間で、証明書が次のチェックに合格する必要があります。

- 有効性 — 現在の時刻と日付が証明書の有効範囲内になければなりません。
- 信頼性 — 証明書が信頼できるものでなければなりません。署名（発行）側による信頼が存在する場合、証明書は信頼できるものであると見なされます。一般的に、署名側による信頼は、署名側の証明書を信頼された証明書ストアにインポートすることにより確立されます。
- ID — 証明書が発行される対象や ID は、セッションのイニシエータが意図した接続先の ID に一致しなければなりません。

デフォルトでは、Unified CM and IM and Presence で使用される証明書はすべて自己署名証明書です。自己署名証明書に関して、上記の各チェックは有効性および識別の面では特に問題ありませんが、信頼性の面では注意が必要です。自己署名証明書に基づいてサービスの信頼性を確立するには、サービスへのセキュア接続を必要とするすべてのエンティティの信頼された証明書ストアに、その自己署名証明書をインポートする必要があります。通信を行う側が少ない場合、これを処理することはできますが、通信相手が多くなると（Jabber のようなクライアント アプリケーションなど）難しくなります。

証明書の検証が Jabber クライアントで失敗すると、ユーザに対してプロンプトが出され、証明書を受け入れることができます。その後、その証明書は信頼された証明書ストアに追加されます。クライアントの起動中に多くの証明書を受け入れるよう何度もプロンプトが出されることは最良のユーザ エクスペリエンスとは言えないため、これは避けるべきです。より重要なこととして、ほとんどのユーザは、提示された証明書のフィンガープリントを確認してその証明書が正しいものであるかどうかを実際には検証せずに、どの証明書もそのまま受け入れてしまいます。これでは、セキュアなセッションを確立するための証明書ベースの認証のセキュリティの概念が成り立たなくなってしまいます。

こうした理由により、Cisco Jabber クライアントの推奨される展開では、クライアント起動中の証明書の検証が失敗しないことが求められます。これは、次の 2 つの方法のどちらかで実現できます。

- 自己署名証明書を使用し、必要なすべての自己署名証明書をデバイスの証明書ストアに事前配布します。

  Windows 環境では、Microsoft グループ ポリシーを使って証明書をデバイスの証明書ストアに追加できます。

- 証明機関（CA）により発行された証明書を使用します。

  この場合、インフラストラクチャ サービスにより使用される自己署名証明書は、信頼された CA により発行され、署名された証明書と置き換えられます。CA による信頼を確立するには、すべてのクライアントの信頼された証明書ストアにその CA のルート証明書を追加します。デフォルトでは、大半のクライアント デバイスの信頼された証明書ストアに、主なパブリック CA のルート証明書がすべて含まれています。

推奨される方法は、2 番目の選択肢です。これは、署名側 CA のルート証明書がすべてのクライアントの信頼された証明書ストアにすでに追加されている限り、すべてのクライアントの信頼された証明書ストアを更新しなくても、新たなサービス証明書を発行できるためです。表 2-2 では、Cisco Jabber クライアントにより検証済みの CA ルート証明書がリストされています。

表 2-2　Cisco Jabber クライアントにより検証済みの証明書

サービス	証明書	説明	検証元
Cisco Unified CM	Tomcat	Unified CM のWeb サービス証明書	GUI Jabber クライアントにアクセスするブラウザ
Cisco Unified CM IM and Presence Service	Tomcat	Unified CM IM and Presence の Web サービス証明書	GUI Jabber クライアントにアクセスするブラウザ
Cisco Unified CM IM and Presence Service	cup-xmpp	Unified CM IM and Presence の XMPP サービス証明書	Jabber クライアント
Cisco Unity Connection	Tomcat	Unity Connection の Web サービス証明書	GUI Jabber クライアントにアクセスするブラウザ

自己署名証明書を CA が発行した証明書と置き換える前に必要な手順

1. 証明書の発行に使用する予定の CA のルート証明書を入手します。
2. Unified CM の OS 管理 GUI に移動します。
3. tomcat-trust として CA ルート証明書をアップロードします。
4. Unified CM IM and Presence の OS 管理 GUI に移動します。
5. xmpp-trust として CA ルート証明書をアップロードします。
6. Cisco Unity Connection の OS 管理 GUI に移動します。
7. tomcat-trust として CA ルート証明書をアップロードします。

自己署名証明書を CA が発行した証明書と置き換える手順

1. それぞれのプラットフォームの OS 管理 GUI に移動します。
   - Unified CM および Unified CM IM and Presence の Tomcat 証明書の場合、Unified CM OS GUI を使用します。
   - Unified CM IM and Presence の cup-xmpp 証明書の場合、CM IM and Presence OS GUI を使用します。
   - Cisco Unity Connection の Tomcat 証明書の場合、Unity Connection OS GUI を使用します。
2. 希望する証明書の証明書署名要求（CSR）を生成します。必ず配布を [マルチサーバ(SAN)（Multi-Server (SAN)）] に設定してください。
3. CSR をダウンロードします。
4. 生成された CSR の信頼された CA から、CA が署名した証明書を取得します。
5. 手順 1 の OS 管理 GUI で、取得した CA 発行証明書をアップロードします。

ヒント　クラスタごとに必要な所定の種類の証明書が 1 つだけですむように、すべての証明書について 1 つのマルチサーバ証明書署名要求を生成する必要があります。

ヒント　発行された証明書での X.509 鍵の用途と X.509 拡張鍵の用途が CSR の要求に一致していることを確認します（表 2-3 を参照してください）。

上述のように、必要な鍵の用途と拡張鍵の用途を CA により発行された証明書が備えているか、確認することが重要です。提供された CSR に基づいて証明書を発行する CA が、単にその CSR から鍵の用途と拡張鍵の用途をコピーして証明書を発行するのではなく、証明書を発行するために選択したテンプレートの設定に基づいて、発行される証明書の鍵の用途と拡張鍵の用途を設定することが、多くの場合に問題となります。たとえば、一般的な Web サーバ テンプレートに基づいて発行される証明書には、TLS Web クライアント認証の拡張鍵の用途が含まれていません。このために、TLS 接続を開始する側の Tomcat 証明書がクライアント証明書としても使用されるサーバ間通信（クラスタ間検索サービス（ILS）やユーザ データ ストア（UDS）など）において問題が生じ、鍵の用途が正しくないことが原因で TLS 接続のセットアップが失敗します（UDS 証明書要件の検討事項を参照）。

表 2-3　Tomcat 証明書および cup-xmpp 証明書の鍵の用途に関する要件

X.509 鍵の用途	X.509 拡張鍵の用途
デジタル署名	TLS Web サーバ認証
鍵の暗号化	TLS Web クライアント認証
データの暗号化	IPSec 終端システム
鍵共有	

Cisco Unified CM の初期設定

Unified CM クラスタをインストールした後すぐに、次の基本的な設定タスクを実行します。

- ノード名設定
- エンタープライズ パラメータ設定
- サービスのアクティブ化
- サービス パラメータの設定

ノード名設定

正しい証明書検証を許可し、Unified CM クラスタ メンバーへの参照が常に正しく解決できるようにするには、Unified CM 管理 GUI のシステム/サーバで、すべてのクラスタ メンバーに対してノード名に完全修飾ドメイン名（FQDN）を設定します。これを実現するには、Cisco Unified CM 管理 GUI でシステム/サーバに移動し、最初の列に表示されているすべてのサーバが FQDN であることを確認します。DNS ドメインが付いていない、ホスト名だけで表示されているサーバのエントリを FQDN に変更します。

エンタープライズ パラメータ設定

表 2-4 にリストされているエンタープライズ パラメータを確認し、更新します。

表 2-4　　エンタープライズ パラメータ

エンタープライズ パラメータ	説明	値
[クラスタID（Cluster ID）]	クラスタ間検索サービス（ILS）およびクラスタ間コール アドミッション制御をはじめとする多くのクラスタ間機能において、Unified CM クラスタを一意に識別するために使用されます	例：USCluster
[URL認証（URL Authentication）] [URLディレクトリ（URL Directories）] [URL情報（URL Information）] [URLサービス（URL Services）] [保護された認証URL（Secured Authentication URL）] [保護されたディレクトリURL（Secured Directory URL）] [保護された情報URL（Secured Information URL）] [保護されたサービスURL（Secured Services URL）]	さまざまな目的のためのエンドポイントで使用される URL	これらの URL が Unified CM パブリッシャ ノードの FQDN を参照することを確認します
[自動登録フォンプロトコル（Auto Registration Phone Protocol）]	自動登録フォン用にプロビジョニングされたシグナリング プロトコル	[SIP]
[コールリストのBLF（BLF For Call Lists）]	この機能をサポートしている電話のコール リストがプレゼンスを表示するかどうかを指定します	[有効（Enabled）]
[G.722コーデックのアドバタイズ（Advertise G.722 Codec）]	互換デバイス間の G.722 を許可します	[有効（Enabled）]
[URI検索ポリシー（URI Lookup Policy）]	RFC 3261 に従い、SIP URI に相当するものを確定する際に、URI の左側（ユーザ部分）のチェックで大文字小文字を区別する必要があります。Unified CM のデフォルトの動作はこの標準に従いますが、大文字小文字が混合している URI で発生する潜在的な問題を回避するには、通常、このデフォルト設定を変更する方が望ましいです。	[大文字小文字の区別なし（Case Insensitive）]
[すべてのパーティションでDNを自動選択（Auto Select DN on Any Partition）]	管理を簡素化します。有効にした場合、ディレクトリ番号設定ページには、最初に一致したディレクトリ番号が自動的に入力されます。	[はい（True）]

表 2-4　エンタープライズ パラメータ（続き）

エンタープライズ パラメータ	説明	値
[依存性レコードを有効化（Enable Dependency Records）]	依存性レコードは Unified CM の管理を簡素化します。	[はい（True）]
[組織の最上位ドメイン（Organization Top Level Domain）]		例：ent-pa.com
[クラスタの完全修飾ドメイン名（Cluster Fully Qualified Domain Name）]	数値 SIP URI をルーティングする際に、Unified CM は URI の右側（ホスト部分）が、設定したクラスタの完全修飾ドメイン名（CFQDN）に一致する SIP URI を、設定したローカル数値ダイヤル プランに従ってルーティングされる宛先と見なします。設定された数値ダイヤル プランに URI の左側の数値に一致するものが見つからない場合、Unified CM はコールを拒否します。詳細については、『*Cisco Collaboration System 10.x SRND*』の「*Dial Plan*」の章の「*Routing of SIP Requests in Unified CM*」の項を参照してください。	クラスタ内の Unified CM のすべての呼処理ノードのスペース区切りリスト。 例： us-cm-sub1.ent-pa.com us-cm-sub2.ent-pa.com
[CDR ファイルの時間間隔（CDR File Time Interval）]	呼詳細レコード（CDR）ファイル更新の時間間隔を決定します	[10]

サービスのアクティブ化

表 2-5 に、Unified CM パブリッシャ ノード、専用の Unified CM TFTP サーバ サブスクライバ ノード、および Unified CM 呼処理サブスクライバ ノードでアクティブ化されるサービスをまとめます。

表 2-5　Unified CM ノードのサービスのアクティブ化

サービス	パブリッシャ	専用 TFTP サブスクライバ	呼処理サブスクライバ
CM サービス			
Cisco CallManager			対応
Cisco IP Voice Media Streaming App			対応
Cisco CTIManager			対応
シスコ クラスタ間検索サービス	対応		
シスコ ロケーション帯域幅マネージャ			対応
Cisco Dialed Number Analyzer Server	対応		
Cisco Dialed Number Analyzer	対応		
Cisco Tftp		対応	
CTI サービス			
Cisco WebDialer Web Service			対応
データベースおよび管理者サービス			
Cisco Bulk Provisioning サービス	対応		
Cisco AXL Web Service	対応		

表 2-5　Unified CM ノードのサービスのアクティブ化（続き）

サービス	パブリッシャ	専用 TFTP サブスクライバ	呼処理サブスクライバ
パフォーマンスおよびモニタリング サービス			
Cisco Serviceability Reporter	対応		
Cisco CallManager SNMP サービス	対応	対応	対応
セキュリティ サービス			
Cisco CTL Provider	対応	対応	対応
Cisco Certificate Authority Proxy Function	対応		
ディレクトリ サービス			
Cisco DirSync	対応		

表 2-6 に、Cisco Unified CM IM and Presence パブリッシャおよびサブスクライバ ノードでアクティブ化されるサービスをリストします。

表 2-6　Unified CM IM and Presence ノード サービスのアクティブ化

サービス	パブリッシャ	サブスクライバ
Cisco AXL Web Service	対応	対応
Cisco Bulk Provisioning Service	対応	
Cisco Serviceability Reporter	対応	
Cisco SIP Proxy	対応	対応
Cisco Presence Engine	対応	対応
Cisco XCP Connection Manager	対応	対応
Cisco XCP Authentication Service	対応	対応

サービス パラメータの設定

Cisco CallManager サービスの一部のサービス パラメータはグローバルであり、Unified CM Administration で 1 度だけ設定する必要があります。Cisco CallManager サービスのグローバル サービス パラメータ設定を表 2-7 にリストします。

（注） このマニュアルでは、デフォルト以外のサービス パラメータおよびその他の設定フィールドの値だけを示しています。フィールド設定値が示されていない場合は、デフォルト値が想定されます。

表 2-7　グローバル サービス パラメータ

サービス パラメータ	値	説明
[リモート番号に変換を適用（Apply Transformations On Remote Number）]	[はい（True）]	コール側の変換がミッドコールにも適用されることを確認します。たとえば、ある関係者から別の関係者へコールが転送される場合などです。
[T302タイマー（T302 Timer）]	[5000]	接続先へのダイヤリングが Unified CM にプロビジョニングされている数値ダイヤル プランに基づいており、1 桁ずつ行われる場合は常に、プロビジョニングされているどのパターンをダイヤル先で検討する必要があるかに関して、即時の決定論的な意思決定を行うことはできません。マッチングが長くなる（可変長の場合も考えられる）可能性があるため、Unified CM が最適ルートを選択し、コールをルーティングする前に、T302 インターディジット タイムアウトの期限が切れる必要があります。デフォルト値の 15,000 ミリ秒（ms）は、通常は長すぎます。
[自動代替ルーティングの有効化（Automated Alternate Routing Enable）]	[AAR の有効化（Enable AAR）]	このサービス パラメータは、自動代替ルーティング（AAR）をグローバルに有効にします。
[コール診断有効（Call Diagnostics Enabled）]	[CDR有効フラグがTrueの場合にのみ有効（Enable Only When CDR Enabled Flag is True）]	このパラメータは、コール管理レコード（CMR）（コール診断レコードとも呼ばれる）を生成するかどうかを決定します。
[G.722コーデック有効必須フィールド（G.722 Codec Enabled Required Field）]	[レコードを有効化したデバイス以外のすべてのデバイスで有効（Enabled to All Devices Except Recording-Enabled Devices）]	レコーダーによってサポートされていない G.722 での問題を回避するため、レコードを有効化したデバイスでは G.722 を無効化します。
[Q.931接続解除原因コード時のルーティングの中止（Stop Routing on Q.931 Disconnect Cause Code）]	3 21 27 28 38 42 63	特定の Q.850 原因コード受信時に、設定済みのハント リストの追跡を Unified CM がやめることを許可します。

Cisco CallManager サービスの他のサービス パラメータは、表 2-8 に示すように、各 Unified CM 呼処理ノードについて明示的に設定する必要があります。

表 2-8　ノードごとのサービス パラメータ

サービス パラメータ	値	説明
[CDR有効フラグ（CDR Enabled Flag）]	[はい（True）]	このパラメータは、コール詳細レコード（CDR）の生成を有効にします。
[接続時間がゼロのコールをCDRに記録するフラグ（CDR Log Calls With Zero Duration Flag）]	[はい（True）]	このパラメータは、接続されなかった、または接続時間が 1 秒未満だったコールのコール詳細レコード（CDR）のロギングを有効または無効にします。
[ディジット分析の複雑性（Digit Analysis Complexity）]	TranslationAndAlternatePatternAnalysis	このパラメータは、CCM トレース ファイルが提供するディジット分析情報の量を指定します。

その他の IM and Presence 設定

これまでの項では、IM and Presence サービスのアクティブ化、証明書管理、および IM and Presence SIP トランク設定について説明しました。それらに加えて、IM and Presence サーバの次の設定を行います。

- [IM&P Cisco SIP Proxy] サービス パラメータでの Unified CM ドメインの設定。
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [設定（Settings）] > [標準設定（Standard Configuration）]:
  - クラスタ ID の値を設定します。
  - 可用性の共有を有効にします。これを有効にしない場合、ユーザは自分の可用性ステータスしか表示できません。
  - [アドホックプレゼンスサブスクリプションを有効にする（Enable ad-hoc presence subscriptions）] チェックボックスを選択し、Cisco Jabber ユーザのアドホック プレゼンス サブスクリプションをオンにします。
- [Cisco Unified CM IM and Presence の管理（Cisco Unified CM IM and Presence Administration）] > [プレゼンス（Presence）] > [ルーティング（Routing）] > [設定（Settings）]:
  - [プロキシサーバの設定（Proxy Server Settings）]:[**メソッド/イベントルーティングのステータス（Method/Event Routing Status）**] を [有効（Enable）] に設定します
- [Cisco Unified CM IM and Presenceの管理（Cisco Unified CM IM and Presence Administration）] > [メッセージング（Messaging）] > [設定（Settings）]:
  - インスタント メッセージを有効にします。

さらに、Jabber プロビジョニングで説明されているように、Jabber クライアント用の UC サービスを設定します。

ダイヤル プラン設定

すべてのコール制御システムを思い通りに展開するために、構造化され、適切に設計されたダイヤル プランは必要不可欠です。エンタープライズ ダイヤル プランの設計では、次の主要な領域を対象とする必要があります。

- エンドポイントのアドレッシング
- 一般的な番号計画
- ダイヤル手順
- ルーティング
- サービス クラス

推奨されるダイヤル プランの設計は、『*Cisco Collaboration System 10.x SRND*』の「*Dial Plan*」の章に説明されている設計方法に従っています。

トポロジの例

このマニュアルでは、米国の 3 つのサイト（SJC、RCD、RTP）にサービスを提供する集中型の呼処理展開を想定しています。表 2-9 に、これらのサイトの DID（ダイレクト イン ダイヤル）の範囲を示します。

表 2-9　　サイトの例の DID 範囲

サイト	DID 範囲
SJC	+1 408 555 4XXX
RCD	+1 972 555 5XXX
RTP	+1 919 555 1XXX

エンドポイントのアドレッシング

DID アドレスを持つエンドポイントの場合、電話番号は +E.164 のフル番号でプロビジョニングされます。この場合、+E.164 は最初の「+」に続いてグローバルな E.164 フル電話番号を表します。Unified CM で +E.164 電話番号をプロビジョニングするには、最初の「+」をエスケープする必要があります。たとえば、SJC の内線 4001 は \+14085554001 としなければなりません。

プロバイダから十分な DID が入手できない、あるいは関連付けられたデバイスに PSTN から電話をかける必要がない（内線電話など）などの理由から、一部のエンドポイントは DID を持ちません。こうしたエンドポイントには DID（E.164 番号）が存在せず、そのためこれらのエンドポイントには +E.164 以外のアドレス形式が必要です。

外部アクセス用エンタープライズ サービスのアドレッシング

一部のサービスには割り当てられた PSTN 番号があります。こうした例として、ユーザが PSTN からボイスメールに電話をかけられるように、外部から到達可能でなければならないボイスメールの代表番号が考えられます。こうしたサービスの PSTN の E.164 番号は、PSTN プロバイダによって割り当てられる DID の範囲から予約しておく必要があります。

一般的な番号計画

+E.164 アドレスが使用できる DID に関連付けられたエンドポイントに加えて、DID がない、以下のような接続先も数多く存在します。

- 内線電話
- プロバイダが DID を割り当てることができなかった正規のエンドポイント
- 各種サービス（コール ピックアップ番号、コールパーク番号、会議など）

このマニュアルではこれらのタイプの接続先のことを*非 DID* と呼びます。

これら非 DID のアドレスは +E.164 アドレス同様、非 DID のサイト固有パーティションを回避するためにシステム全体で一意でなければなりません。推奨されるソリューションは、すべての非 DID に関してエンタープライズ固有の番号付け（ESN）方式を導入することです。この ESN 方式は一般的なサイト間短縮ダイヤルの構造に従います。

- アクセスコード

  サイト間短縮ダイヤルの 1 桁のアクセスコード。設計段階において、ほかのどのエンタープライズ ダイヤル手順とも重複しないようにアクセスコードを選択します（下記参照）。

- サイトコード

  ネットワーク内のサイトを一意に識別するための一連の番号。設計段階において、すべての既存のサイトを対象とするだけではなく、規模が拡大した場合も考慮したサイト コードの長さを選択します。

- 内線番号

  サイト内で各エンティティを一意に識別するための一連の番号。

このマニュアルでは、サイト間短縮ダイヤルのアクセスコードに 8 を使います。したがって、すべての ESN は 8 で始まります。また、サイト コードには 3 桁、内線番号には 4 桁を使用します。表 2-10 では、本書の例にある各サイトの DID 番号および非 DID 番号の ESN 範囲を示しています。

表 2-10　DID および非 DID の ESN 範囲

サイト	+E.164 範囲	サイト コード	DID の ESN 範囲	非 DID の ESN 範囲
SJC	+1 408 555 4XXX	140	8-140-4XXX	8-140-5XXX
RCD	+1 972 555 5XXX	197	8-197-5XXX	8-197-6XXX
RTP	+1 919 555 1XXX	191	8-191-1XXX	8-191-2XXX

このプランでは DID と非 DID について同じサイト コードを使用しますが、非 DID の内線番号の最初の数字は DID 内線番号の最初の数字とは異なります。これにより、非 DID 番号および DID 番号への 4 桁のサイト内短縮ダイヤルも可能になります。

表 2-10 の ESN 範囲ではサイト固有番号に対して ESN 計画に余地を残していますが、スケジュール済み会議などのサイト固有以外のサービスについても番号を割り当てる必要があります。表 2-11 に、専用のサイト コード（この場合は 099）を予約しておくことにより、この要件に対処する方法の例を示します。

表 2-11　会議用の ESN 範囲

ESN 範囲	使用方法
8099[12]XXX	スケジュール済み会議

ダイヤル手順

ダイヤル手順では、エンド ユーザがさまざまな種類の接続先に電話をかけるためにどのようにダイヤルする必要があるかを記述します。ダイヤル手順はまず、数字でダイヤルするか（914085550123 など）、または英数字でダイヤルするか（bob@ent-pa.com）などで分類されます。

この設計では、英文字の URI でダイヤルする方法に加えて表 2-12 に示すように数字でのダイヤル手順もサポートされています。

表 2-12　サポートされている数字でのダイヤル手順

ダイヤル パターン	例（サイト SJC）	接続先のタイプ
XXXX	4001（DID） 5001（非 DID）	接続先に同時にダイヤルするためのサイト内短縮ダイヤル。 発信先は DID 番号、非 DID 番号、またはサービス番号であることが可能です。
+E.164	+14085554001（ネット上、SJC） +19195551001（ネット上、RTP） +1212551001（ネット外）	ディレクトリなどからの +E.164 フル番号ダイヤル。ダイヤル先はネット上であることもネット外であることも可能です。実装されたダイヤル プランによって、+E.164 でダイヤルされるネット上の接続先へのコールが、確実にネット上にルーティングされます。明らかなこととして、非 DID を +E.164 でコールすることはできません。
アクセス コード–サイト コード –内線番号	8-140-4001（DID、SJC） 8-140-5001（非 DID、SJC） 8-191-1001（DID、RTP） 8-191-2001（非 DID、RTP）	同じサイトまたは別のサイトの接続先にダイヤルするためのサイト間短縮ダイヤル。発信先は DID 番号、非 DID 番号、またはサービス番号であることが可能です。アクセス コード（この例では 8）は、他のダイヤル手順（サイト内短縮ダイヤルなど）と重複しないように選択する必要があります。サイト間ダイヤルにアクセス コード 8 を使うことで、8 で始まる 4 桁のサイト内ダイヤルができなくなります。
*E.164	*12125551567	専用のビデオ ISDN ゲートウェイによるビデオ コールのダイヤル。アスタリスク（*）を使用して、数字（!）による他のダイヤル手順とは重複しない、特定のダイヤル手順を作成します。アスタリスク（*）の使用を避けるために、サイト間短縮アクセス コード 8 で始まる数字領域（8000-<E.164> など）を使用することもできます。
91-<10 digits>	914085554001（ネット上、SJC） 919195551001（ネット上、RTP） 912125551001（ネット外）	国内の接続先にダイヤルするための米国固有の PSTN ダイヤル手順。実装されたダイヤル プランにより、ダイヤル先がネット上の場合は、確実にそのコールがネット上にルーティングされます。
9011-<E.164 number>	90114961007739764	海外の接続先にダイヤルするための米国特有の PSTN ダイヤル手順。実装されたダイヤル プランにより、ダイヤル先がネット上の場合は、確実にそのコールがネット上にルーティングされます。

一般的に、サポートされるダイヤル手順が少ないほど設計は簡易になります。設計プロセスの開始時にすべてのダイヤル手順を考慮することで、番号間タイムアウトにつながる任意の 2 種類のダイヤル手順の重複を確実に見つけて、ダイヤル プランの展開前にそれを解決できます。

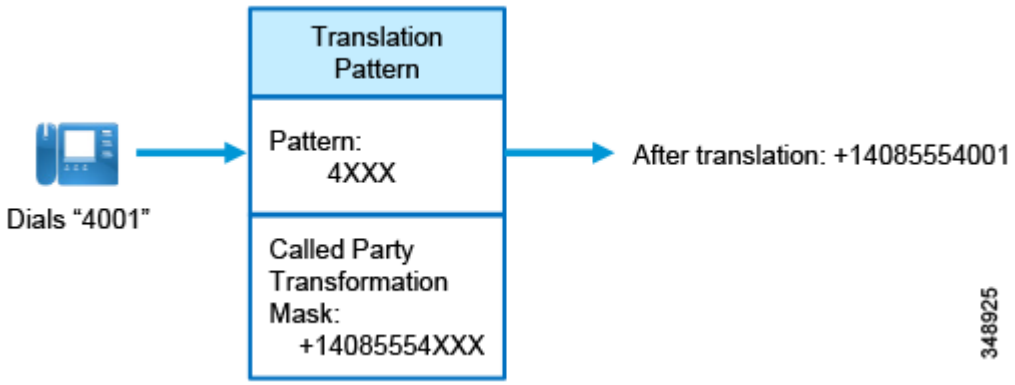
+E.164 ルーティングおよびダイヤリングの正規化

意図した通りのネット上の強制的なルーティング（サポートされている数字でのダイヤル手順のどれを使って任意のネット上の接続先にダイヤルしても、ネット上でルーティングされなければならない）を実現するために、推奨されるダイヤル プランの設計では 2 段階のルーティング方法が使用されます。第 1 段階で、ダイヤルされる数字列は可能であれば +E.164 で正規化されます（非 DID への発信は明らかに +E.164 で正規化されません）。次に第 2 段階で、正規化された +E.164 数字列が、電話番号およびルート パターンを含む +E.164 番号計画に対して照合されます。

ダイヤリングの正規化は、非 +E.164 ダイヤル列での照合を行うトランスレーション パターンをプロビジョニングし、その後に、そのトランスレーション パターンに基づいた発信側トランスフォーメーションにより、ダイヤルした番号が +E.164 に変換されることで実現されます。

図 2-7 に、SJC のサイト内短縮ダイヤルをダイヤル先の +E.164 フル番号に正規化するために使用できる、ダイヤリング正規化トランスレーション パターンの例を示します。サイト SJC のユーザが 4001 にダイヤルすると、この数字列がトランスレーション パターン 4XXX によって照合され、このトランスレーション パターンで設定された着信側のトランスフォメーション マスクが、4001 に適用されるときに、トランスフォーメーションによる数字列 +14085554001 を作成します。その後に、この数字列を +E.164 ルーティング方式でルーティングできます。

図 2-7　　ダイヤリング正規化トランスレーション パターンの例



トランスレーション パターンに基づいて定義された着信側トランスフォーメーションを適用した後に、Unified CM はそのトランスレーション パターンに基づいて定義されたコーリング サーチ スペース（CSS）を使用して数字列に対する 2 回目の検索を実行します。Unified CM は、この 2 回目の検索のために、発信元の CSS と使用するトランスレーション パターンの定義を有効にします。これにより、複数のコンテキストで再利用できるダイヤリング正規化トランスレーション パターンの定義が可能になります。ダイヤリング正規化を適用した後に、単一の固定された CSS に基づくのではなく、そのトランスレーション パターンが用意されたときに有効だった CSS に基づいて、正規化された数字列の 2 回目の検索が実行されるからです。

ヒント　2 回目の検索で使用される CSS が最初の検索で使用される CSS と同一であるようにするために、ダイヤリング正規化トランスレーション パターンでオプション [発信側コーリングサーチスペースを使用（Use Originator's Calling Search Space）] を設定します。

パーティション

パーティションと CSS はサービス クラスを構築するために Unified CM で使用される基本的なコンポーネントです。ダイヤル可能なパターンは、同じクラスに属するパターンを同じパーティションに入れることにより、等価クラスにグループ化されます。このときの各 CSS は、その CSS を使用する発呼側エンティティがどのパーティションおよびパターンにアクセスできるかを定義するパーティションのリストです。

エンタープライズ ダイヤル プランを作成するためにプロビジョニングされるパーティションおよび CSS を定義するときの目標の 1 つは、できるだけ重複設定を防ぐことです。この原則に従い、表 2-13 では、必要とされるグローバル パーティション（サイト別、国別ではない）を示します。

表 2-13　　グローバル パーティション

パーティション	説明
DN	+E.164 電話番号すべてと、その他のローカルのネット上の+E.164 接続先（PSTN から接続可能な代表番号など）を保持します。すべての +E.164 パターンは緊急パターンとしてプロビジョニングされます。
ESN	すべてのエンタープライズ固有番号（ESN）を保持します。これには ESN 電話番号（非 DID 電話など）と、DID のサイト間短縮ダイヤルから +E.164 へ変換するダイヤリング正規化トランスレーション パターンが含まれます。
PSTNInternational	海外の接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。
URI	手動でプロビジョニングした URI を保持します。
onNetRemote	リモートのネット上の接続先のすべてのパターンを保持します。複数の Unified CM クラスタが存在する環境では、グローバル ダイヤル プラン レプリケーション（GDPR）を介して通知されるすべてのリモート番号の範囲が含まれます。
B2B_URI	インターネットを使った business-to-business（B2B）の URI ダイヤルに必要な SIP ルート パターンを保持します。
Directory URI	自動生成されたすべての URI が置かれるシステム パーティション。このパーティションは作成不要です。ここでは、このパーティションの紹介をするために参考としてリストしています。このパーティションについては、このマニュアルの後半で再度使用します。

Directory URI 以外の表 2-13 にリストされたすべてのパーティションを作成する必要があります。これらのグローバル パーティションで表すパターン クラスに加えて、表 2-14 に示すような複数のサイト、国、またはサービス クラス固有のパターン クラスが必要です。

表 2-14　　国またはサイト固有のパーティション

パーティション	説明
USPSTNNational	米国国内の接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。他の国をサポートし、さらには他の国固有のダイヤル手順をサポートするには、当該国の xxPSTNNational パーティション（xx は国を表します。たとえば、DEPSTNNational、UKPSTNNational、ITPSTNNational などです）もプロビジョニングする必要があります。そのパーティションは、その国の国内接続先への PSTN アクセスを提供するために必要な +E.164 ルート パターンを保持します。 海外 PSTN アクセス（表 2-13 を参照）と国内 PSTN アクセスを区別する理由は、国内接続先だけを対象としたコールを許可するサービス クラスや、国内と海外の接続先を対象としたコールを許可するサービス クラスを区別して作成できなければならないからです。
USToE164	米国固有の PSTN ダイヤル手順（91-<*10 digits*> など）を +E.164 へ変換するためのダイヤリング正規化トランスレーション パターンを保持します 他の国をサポートし、さらには他の国固有のダイヤル手順をサポートするには、当該国の xxToE164 パーティション（xx は国を表します。たとえば、DEToE164、UKToE164、ITToE164 などです）もプロビジョニングする必要があります。そのパーティションはその国固有の PSTN ダイヤル手順を +E.164 に変換するために必要なダイヤリング正規化トランスレーション パターンを保持します。
USEmergency	米国固有の緊急ダイヤル手順を使用する緊急コールへのアクセスを提供するために必要なルート パターンを保持します。
USPhLocalize	米国内で電話で +E.164 発呼側番号を短縮表示にローカライズするための発呼側トランスフォーメーション パターンを保持します。
<site>Intra	サイト固有のサイト内ダイヤリング。たとえば、SJCIntra などです。サイト固有のサイト内短縮ダイヤルを DID に、または非 DID を +E164 または ESN にそれぞれ変換するためのダイヤリング正規化パターンを保持します。
<site>PhLocalize	サイト固有です。たとえば、SJCPhLocalize などです。所定のサイトの電話で +E.164 発呼側番号を短縮表示にローカライズするための発呼側トランスフォーメーション パターンを保持します

緊急コールは国固有のダイヤル手順を使用して行われるため、緊急コールの米国のダイヤル手順を可能にするルート パターンを持つパーティション USEmergency も、国固有です。他のダイヤリング ドメイン（国）もサポートするには、それらの他のダイヤリング ドメインに相当するパーティション（DEEmergency：ドイツ、ITEmergency：イタリア、DEPhLocalize：ドイツ、ITPHLocalize：イタリアなど）を作成する必要があります。

ダイヤリング正規化トランスレーション パターン

表 2-15 は、前の項で説明したパーティションを使用してどのダイヤリング正規化トランスレーション パターンをプロビジョニングする必要があるかをまとめています。すべてのダイヤリング正規化トランスレーション パターンは、緊急パターンとしてプロビジョニングされ、[発信側コーリングサーチスペースを使用（Originator's Calling Search Space）] が設定されています（+E.164 ルーティングおよびダイヤリングの正規化項を参照）。これにより、ダイヤリング正規化トランスレーション パターンで定義された着信側トランスフォーメーションを適用した後に、元の CSS を使用してダイヤル先の最終的な一致を検出できます。

表 2-15　　ダイヤリング正規化トランスレーション パターンの概要

パーティション	パターン	着信側トランスフォーメーション マスク	コメント
ESN	81404XXX	+14085554XXX	サイト SJC のサイト間短縮ダイヤル
ESN	81975XXX	+19725555XXX	サイト RCD のサイト間短縮ダイヤル
ESN	81911XXX	+19195551XXX	サイト RTP のサイト間短縮ダイヤル
SJCIntra	4XXX	+14085554XXX	SJC でのサイト SJC から DID へのサイト内短縮ダイヤル
SJCIntra	5XXX	81405XXX	SJC でのサイト SJC から非 DID へのサイト内短縮ダイヤル
RCDIntra	5XXX	+14085554XXX	RCD でのサイト RCD から DID へのサイト内短縮ダイヤル
RCDIntra	6XXX	81976XXX	RCD でのサイト RCD から非 DID へのサイト内短縮ダイヤル
RTPIntra	1XXX	+19195551XXX	RTP でのサイト RTP から DID へのサイト内短縮ダイヤル
RTPIntra	2XXX	81912XXX	RTP でのサイト RTP から非 DID へのサイト内短縮ダイヤル
UStoE164	9.1 [2-9]XX [2-9]XX XXXX	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順
UStoE164	9011.!#	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順。 **（注）** ダイヤリング正規化トランスレーション パターンでは、末尾の「#」は削除されません。これにより、末尾に # が付いた可変長の PSTN ルート パターンで 2 回目の一致が可能になります。
UStoE164	9011.!	マスクなし、ドットの前の番号を削除して、先頭に + を付加	米国内の接続先の米国固有の PSTN ダイヤル手順

米国以外のダイヤリング ドメインの場合、インストールでそうした国固有のダイヤル手順をサポートする必要があるなら、他の国固有のダイヤリング正規化トランスレーション パターンを定義しなければなりません。表 2-16 に、例としてドイツ（DE）とイタリア（IT）に必要なダイヤリング正規化を示します。

表 2-16　ドイツとイタリアのダイヤリング正規化

パーティション	パターン	着信側トランスフォーメーション	コメント
DEtoE164	000.!	ドットの前の番号を削除して、先頭に + を付加	ドイツ：国際コール（000-E.164）。
DEtoE164	000.!#	ドットの前の番号を削除して、先頭に + を付加	ドイツ：国際コール（000-E.164）。 **（注）** ダイヤリング正規化トランスレーション パターンでは、末尾の「#」は削除されません。これにより、末尾に # が付いた可変長の PSTN ルート パターンで 2 回目の一致が可能になります。
DEtoE164	00.[^0]!	ドットの前の番号を削除して、先頭に +49 を付加	ドイツ：国内コール（00-国内番号）。 **（注）** ドイツの番号計画は可変長であり、このパターンはこれを対象にする必要があります。
DEtoE164	00.[^0]!#	ドットの前の番号を削除して、先頭に +49 を付加	ドイツ：国内コール（00-国内番号）。
ITtoE164	000.!	ドットの前の番号を削除して、先頭に + を付加	イタリア：国際コール（000-E.164）。
ITtoE164	000.!#	ドットの前の番号を削除して、先頭に + を付加	イタリア：国際コール（000-E.164） **（注）** ダイヤリング正規化トランスレーション パターンでは、末尾の「#」は削除されません。これにより、末尾に # が付いた可変長の PSTN ルート パターンで 2 回目の一致が可能になります。
ITtoE164	0.0[^0]!	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0-国内番号（NSN）、NSN は 0 で始まる）。 **（注）** イタリアの番号計画は可変長であり、このパターンはこれを対象にする必要があります。
ITtoE164	0.0[^0]!#	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まる）。
ITtoE164	0.[^0]!	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まらない）。 **（注）** イタリアの番号計画は可変長であり、このパターンはこれを対象にする必要があります。
ITtoE164	0.[^0]!#	ドットの前の番号を削除して、先頭に +39 を付加	イタリア：国内コール（0-NSN、NSN は 0 で始まらない）。

表 2-16 の例は、イタリアとドイツではエンタープライズ内部からトランクにアクセスするのに ITU が推奨する 0 が使用され、次に国内および国際アクセスに 0 および 00 が使用されていることを示しています。1998 以降、イタリアの地域番号は 0 で始まり、1 から 9 の数字が国内番号の最初の数字として、番号のさまざまな種類を示します。したがって、2 個のゼロ（00）で始まるダイヤル番号は、ドイツとイタリアでは異なる処理をする必要があります。イタリアでは 2 番目のゼロは NSN の一部であると見なさなければならず、したがって +E.164 数字列に残しておく必要がありますが、ドイツでは地域番号がゼロで始まらないため、ドイツの 2 番目のゼロは削除する必要があります。

これら 2 つの国に必要なダイヤリング正規化の例は、提示する設計方法で国固有のダイヤル手順をどのようにモデル化できるかを示しています。

国際番号計画の詳細については、ITU-T の「*International Numbering Resources*」ページ（http://www.itu.int/en/ITU-T/inr/Pages/default.aspx）を参照してください。このページには、E.164 国コードおよび国内番号計画を含むさまざまなリソースへのリンクがあります。さまざまな国で使用されているダイヤル手順の概要は、「*Operational Bulletin No.994 (15.XII.2011) and Annexed List: Dialling procedures (international prefix, national (trunk) prefix and national (significant) number) (in accordance with ITU-T Recommendation E.164 (11/2010)) (Position on 15 December 2011)*」（http://www.itu.int/pub/T-SP-OB.994-2011）にあります。実際のダイヤル手順のリストはその文書の 25 ページから始まっています。この文書は http://www.itu.int/dms_pub/itu-t/opb/sp/T-SP-E.164C-2011-PDF-E.pdf よりダウンロードできます。

サービス クラスとコーリング サーチ スペース（CSS）

前述のように、CSS は、CSS を使用する発呼側エンティティがアクセスできるパーティションやパターンを定義するパーティションのリストです。このマニュアルでは、サービス クラスを定義する回線 CSS だけを使用するダイヤル プラン方法を使います。

表 2-17 に、この設計で検討するサービス クラスをリストします。この設計のために選択したサービス クラスは例にすぎません。さらにサービス クラスが必要な場合は、同じように定義できます。

ヒント　サービス クラスの数は、エンタープライズ ダイヤル プランの設計の複雑さを決める重要なパラメータの 1 つです。したがって、ダイヤル プランに定義するサービス クラスの数をできる限り少なくすることが肝要です。

推奨される設計では、サービス クラスを定義するために、回線にプロビジョニングされる CSS のみを利用し、デバイス CSS を使用しません。デバイス CSS は、誰にでも利用できることが必要な一般的なダイヤル手順を実装するために使用できます。この例として緊急コールがあります。デバイス CSS を使用して緊急コールを実装する場合の詳細については、多国間環境における緊急コールの考慮事項を参照してください。

表 2-17　　サービス クラス

サービス クラス	アクセス先
国際	すべてのネット上の接続先 国内の PSTN 接続先 国際 PSTN 接続先 Business-to-business URI ダイヤリング 緊急コール
国内	すべてのネット上の接続先 国内の PSTN 接続先 緊急コール
内線	すべてのネット上の接続先 緊急コール

International サービス クラスだけに business-to-business URI ダイヤリングを追加することは、business-to-business（B2B）コールが限られたエッジ リソースを消費するという前提に基づいた例です。また、International、InternationalB2B、National、NationalB2B、Internal、および InternalB2B のサービス クラスを導入することによって、サービス クラスの数の倍増を避けようとしています。

所定の発信者が利用できるサービス クラスとダイヤル手順セットの両方を定義するために回線 CSS だけを使用するため、サイトごと、サービス クラスごとに、CSS をプロビジョニングする必要があります。

表 2-18 に、以前に定義したパーティション セット（表 2-13 および表 2-14 を参照）に基づいてサービス クラス International をサイト SJC のユーザに対して定義する方法を示します。

表 2-18　SJC ユーザ用のサービス クラス International

CSS 名	パーティション
SJCInternational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational PSTNInternational B2B_URI USEmergency

表 2-19 に示すように、残りのサービス クラスは B2B URI ダイヤリング、国際、および国内 PSTN 接続先へのアクセスを選択的に削除することにより、同じように作成できます。

表 2-19　SJC ユーザ用のサービス クラス National および Internal

CSS 名	パーティション
SJCNational	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USPSTNNational USEmergency

CSS 名	パーティション
SJCInternal	DN Directory URI URI ESN onNetRemote SJCIntra UStoE164 USEmergency

他のサイトのユーザ用のサービス クラスの CSS は上述の CSS と同様に作成しますが、サイト固有のダイヤリング正規化パターンと共に使用するパーティションが異なる点だけが違います。表 2-20 に、RTP サイトの National および Internal サービス クラスの例を示します。

表 2-20　RTP ユーザ用のサービス クラス National および Internal

CSS 名	パーティション
RTPNational	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USPSTNNational USEmergency

CSS 名	パーティション
RTPInternal	DN Directory URI URI ESN onNetRemote RTPIntra UStoE164 USEmergency

これらの例は、選択したパーティション方式により、複数サイトのサービス クラスを実装する CSS を作成する際に、パターンとパーティションの理想的な再利用が可能になることをはっきり示しています。

他のダイヤリング ドメイン（国）の場合、上記に示すのと同じ CSS とパーティション方式を利用できますが、上記で使用される米国パーティションの代わりに、特定のダイヤリング ドメインのダイヤリング正規化パーティションおよび国内の PSTN 接続先への国固有のルートを使用する点のみが違います。たとえば、表 2-21 はドイツ（DE）のサイト FRA のサービス クラス International の CSS を示しています。

表 2-21　ドイツ（DE）のサイト FRA のユーザ用のサービス クラス International

CSS 名	パーティション
FRAInternational	DN Directory URI URI ESN onNetRemote FRAIntra DEtoE164 DEPSTNNational PSTNInternational B2B_URI DEEmergency

特殊な CSS

ユーザ向けサービス クラスのほかに、コーリング サーチ スペース（CSS）は Cisco Unity Connection など、トランクを通じて接続されるアプリケーションのサービス クラスの定義にも使用されます。Unity Connection がネット上の接続先にのみアクセスでき、ESN および +E.164 ダイヤリング以外に Unity Connection からの米国ダイヤル手順もサポートされることを前提として、表 2-22 は、このサービス クラスを実装する CSS を示しています。

表 2-22　ボイスメールのサービス クラス

CSS 名	パーティション
VoiceMail	DN ESN URI onNetRemote Directory URI UStoE164

Cisco Unity Connection が複数の国で提供される必要があるシナリオでは、上記の例のパーティション UStoE164 で定義された国固有のダイヤリング正規化の実装はオプションではありません。この場合にサポートできるダイヤル手順は、グローバルで有効なダイヤル手順である ESN と +E.164 だけです。

Unified CM プレゼンスを使用するには、プレゼンス ユーザのサブスクライブ先のすべてのプレゼンティティへのアクセスができるように、何よりもサブスクライブ CSS をプロビジョニングする必要があります。プレゼンス アクセスのさらなる差別化をせずに Unified CM プレゼンスのプロビジョニングを簡素化ができるようにするには、考えられるすべてのネット上の接続先へのアクセスが可能な単一の CSS をプロビジョニングする必要があります。表 2-23 は、このデフォルトのサブスクライブ CSS の設定を示しています。

表 2-23　デフォルトのサブスクライブ CSS

CSS 名	パーティション
DefaultSubscribe	DN ESN URI onNetRemote Directory URI

このサブスクライブ CSS は、すべてのタイプのネット上の接続先へのアクセスを保証します。

表 2-24 に、PSTN トランクでの着信 CSS として使用される（平易な）CSS「DN」を示します。ループを回避するため、PSTN トランクは +E.164 電話番号だけに接続できます。PSTN がサポートする番号方式は 1 つだけで、それが着信時に +E.164 に正規化されるため、PSTN トランクは ESN パターン、ダイヤリング正規化パターン、または URI にアクセスする必要がなくなります。

表 2-24　PSTN ゲートウェイ用の着信 CSS

CSS 名	パーティション
DN	DN

Cisco TelePresence Servers および TelePresence Conductor は、ネット上のすべての接続先へのアクセスが必要であると同時に、すべての PSTN 接続先に電話をかけることができなければなりません。その一方で、ダイヤリング ドメイン固有やサイト固有のダイヤリング正規化パターンへのアクセスは必要ありません。表 2-25 に示す CSS TelePresenceConferencing は、このサービス クラスを実装します。

表 2-25　TelePresence Conferencing のトランク用の着信 CSS

CSS 名	パーティション
TelePresenceConferencing	DN ESN URI onNetRemote Directory URI PSTNInternational

表 2-26 に、他の Unified CM クラスタへのトランクの着信 CSS として使用される CSS ICTInbound を示します。ループを回避するため、これらのクラスタ間トランクの着信 CSS は、リモートのネット上接続先（パーティション onNetRemote）へのアクセスを提供すべきではありませんが、トランク（着信 CSS）はネット上のすべての有効なアドレッシング モード（+E.164、ESN、URI）をサポートする必要があります。ダイヤリング正規化は、この CSS の一部ではありません。コールが着信クラスタ間トランクに着信する前に、+E.164 および ESN 以外のダイヤル手順はリモートの Unified CM クラスタで +E.164 または ESN に正規化されているはずだからです。

表 2-26　他の Unified CM クラスタへのトランク用の着信 CSS

CSS 名	パーティション
ICTInbound	DN ESN URI Directory URI

コール タイプ固有の発信ゲートウェイを選択するためのローカル ルート グループ

発信側デバイスに基づいて柔軟な出口ゲートウェイ選択ができるように、ローカル ルート グループ（LRG）の使用が推奨されます。出口ゲートウェイの選択に LRG を使用すると、サイト固有のルート パターンが不要になります。ローカル ルート グループを使用したルート パターンには固有の特性があります。つまり、コールの発信元デバイスに基づいて出口ゲートウェイを動的に選択できます。それに対し、スタティック ルート グループを使用したルート パターンによってルーティングされるコールでは、コールの発信元デバイスに関係なく、コールが同じゲートウェイにルーティングされます。LRG を使用するルート リストを参照するよう設定されたルート パターンは、発信側のデバイス プールで LRG として設定された実際のルート グループに解決されます。

異なるコール タイプについて別々の LRG を選択できるようにするには、表 2-27 に示すように複数の LRG 名を設定します。

表 2-27　ローカル ルート グループ名

ローカル ルート グループ名	説明
LRG_PSTN_1	PSTN コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ
LRG_PSTN_2	PSTN コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ
LRG_VIDEO_1	PSTN ビデオ コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ

表 2-27　　ローカル ルート グループ名（続き）

ローカル ルート グループ名	説明
LRG_VIDEO_2	PSTN ビデオ コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ
LRG_Emergency_1	緊急コールに使用されるプライマリ PSTN リソースを参照するローカル ルート グループ
LRG_Emergency_2	緊急コールに使用されるセカンダリ PSTN リソースを参照するローカル ルート グループ

これらの LRG 定義により、緊急コールと通常の PSTN コールに別々の PSTN リソース（ゲートウェイ）を使用できるように、「通常の」PSTN コールと緊急コールの両方についてそれぞれ専用のルート リストを作成できます。これは、一元化された PSTN リソースが通常の PSTN コールのためにプロビジョニングされているものの、適切な Public Safety Answering Point（PSAP）へローカルの緊急コールをルーティングできるように、緊急コールがローカル サイトの小さな専用ゲートウェイを依然として使用する必要があるような状況で役立ちます。

ビデオ LRG はビデオ対応の ISDN ゲートウェイ用にプロビジョニングされ、別のリソースとして扱われます。

ローカル ルート グループを使用するルート リスト

前の項で定義した LRG を使用して、表 2-28 に示すようにルート リストを作成する必要があります。

表 2-28　　ルート リストの定義

ルート リスト	メンバー	説明
RL_PSTN	LRG_PSTN_1 LRG_PSTN_1 標準ローカル ルート グループ	通常の PSTN コールは、通常の PSTN コール用に定義されたサイト固有のプライマリおよびセカンダリ PSTN リソースを使用しなければなりません。最後のメンバーである標準ローカル ルート グループは、コール タイプ固有ではない PSTN リソースへのフォールバックが可能です。
RL_Emergency	LRG_Emergency_1 LRG_Emergency_2 LRG_PSTN_1 LRG_PSTN_1 標準ローカル ルート グループ	緊急コールの場合、緊急コール用の最初のコール固有リソースを使用し、次に 2 番目の固有リソースを、その後に通常の PSTN コールに定義された PSTN リソースを、最後に固有ではない PSTN リソースを使用する必要があります。
RL_VIDEO	LRG_VIDEO_1 LRG_VIDEO_2 LRG_PSTN_1 LRG_PSTN_2 標準ローカル ルート グループ	ビデオ コールの場合、最初にビデオ固有のゲートウェイ リソースを使用し、次の正規の PSTN リソースをフォールバック（音声のみ）として検討し、最後に、他のリソースが失敗した場合に標準ローカル ルート グループが使用されます。

各デバイス プールの上記の LRG およびルート リスト定義により、定義済みの LRG 対して最大 7 つのルート グループを選択でき、非常に限定した発信ゲートウェイ選択が可能になります。あるコール タイプに使用される実際の PSTN リソースは、デバイス プールのプロビジョニング中に定義されます。所定のデバイス セットについてコール タイプに基づく異なる発信 PSTN リソースの選択が不要で、すべてのコール タイプについて PSTN リソースが 1 つしか必要ではない場合、それぞれのデバイス プールに標準ローカル ルート グループの実際のルート グループだけを定義し、そのデバイス プール セットの他のすべての LRG は <None> に設定されたままにしておくだけで十分です。　すべてのルート リストで [標準ローカルルートグループ（Standard Local Route Group）] を最後のエントリにすることでできます。

PSTN アクセスと緊急コールのルート パターン

PSTN アクセスは PSTN ルート パターンにより実現します。サービス クラスとコーリング サーチ スペース（CSS）で説明したように、PSTNInternational パーティションでは国際接続先へのルートをプロビジョニングする必要がある一方で、ダイヤリング ドメイン固有パーティション xxPSTNNational（xx は、USPSTNNational のように、ダイヤリング ドメインを表します）では国内 PSTN ルートがプロビジョニングされます。表 2-29 に、設定済みの PSTN ルート パターンを示します。

表 2-29　　PSTN ルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
\+!	PSTNInternational	RL_PSTN	任意の国際接続先にダイヤルできる可変長番号。
\+!#	PSTNInternational	RL_PSTN	可変長のダイヤルを # で終わらせることができるようにするための、国際接続先の代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] に設定。
\+1.[2-9]XX[2-9]XX XXXX	USPSTNNational	RL_PSTN	米国の国内接続先用の明示的なパターン。 国際接続先用に定義された可変長の PSTN ルート パターン \+! との重複を避けるために、[緊急優先（Urgent Priority）] を チェックします。
911	USEmergency	RL_Emergency	米国の緊急コール [緊急優先（Urgent Priority）] をチェックします
9911	USEmergency	RL_Emergency	米国の緊急コール [緊急優先（Urgent Priority）] をチェックします

表 2-29 に明示的に示したルート パターン設定以外のすべてのその他の設定は、表 2-30 に示すデフォルト値のまま残します。これには特に、空白のまま残す発呼側、接続先、着信側のトランスフォーメーションが含まれます（前述の末尾番号の削除を除く）。PSTN 要件に合致することが必要な発呼側および着信側のトランスフォーメーションは、明示的な発呼側および着信側トランスフォーメーションとして設定されるからです。これは、アウトバウンド コール：ISDN ゲート

ウェイでの着信者番号と発信者番号のトランスフォーメーションおよびアウトバウンド コール:SIP トランクでの着信者番号および発信者番号のトランスフォーメーションで説明されています。

表 2-30　　ルート パターンのデフォルト設定

設定	値
パターン定義	
[番号計画(Numbering Plan)]	-- 選択しない --
[ルートフィルタ(Route Filter)]	<なし>
[MLPP優先度(MLPP Precedence)]	[デフォルト(Default)]
[ブロックコール率の適用(Apply Call Blocking Percentage)]	オフ
[リソースプライオリティネームスペースネットワークドメイン(Resource Priority Namespace Network Domain)]	<なし>
[ルートクラス(Route Class)]	[デフォルト(Default)]
[ルートオプション(Route Option)]	[このパターンをルーティング(Route this pattern)]
[コールの分類(Call Classification)]	[オフネット(OffNet)]
[外部コール制御プロファイル(External Call Control Profile)]	<なし>
[デバイスの上書きを許可(Allow Device Override)]	オフ
[外部ダイヤルトーンの提供(Provide Outside Dial Tone)]	オン
[オーバーラップ送信を許可(Allow Overlap Sending)]	オフ
[強制承認コードが必須(Require Forced Authorization Code)]	オフ
[承認レベル(Authorization Level)]	[0]
[クライアント識別コードの要求(Require Client Matter Code)]	オフ
[発呼側トランスフォーメーション(Calling Party Transformations)]	
[発呼側の外線電話番号マスクを使用(Use Calling Party's External Phone Number Mask)]	オフ
[発呼側トランスフォーメーション マスク(Calling Party Transform Mask)]	空白のままにします。値は何も入力しないでください。
[プレフィックス番号(発信コール)(Prefix Digits (Outgoing Calls))]	空白のままにします。値は何も入力しないでください。
[発呼者回線 ID の表示(Calling Line ID Presentation)]	[デフォルト(Default)]
[発呼者名の表示(Calling Name Presentation)]	[デフォルト(Default)]
[発呼側番号タイプ(Calling Party Number Type)]	[Cisco CallManager]

表 2-30　ルート パターンのデフォルト設定（続き）

設定	値
[発呼側番号計画（Calling Party Numbering Plan）]	[Cisco CallManager]
[接続側トランスフォーメーション（Connected Party Transformations）]	
[接続側回線 ID の表示（Connected Line ID Presentation）]	[デフォルト（Default）]
[接続先名の表示（Connected Name Presentation）]	[デフォルト（Default）]
[着信側トランスフォーメーション（Called Party Transformations）]	
[番号の削除（Discard Digits）]	<なし>
[着信側トランスフォーメーションマスク（Called Party Transform Mask）]	空白のままにします。値は何も入力しないでください。
[プレフィックス番号（発信コール）（Prefix Digits (Outgoing Calls)）]	空白のままにします。値は何も入力しないでください。
[着信側番号タイプ（Called Party Number Type）]	[Cisco CallManager]
[着信側番号計画（Called Party Numbering Plan）]	[Cisco CallManager]
[ISDN ネットワーク固有ファシリティの情報要素（ISDN Network-Specific Facilities Information Element）]	
[ネットワークサービスプロトコル（Network Service Protocol）]	-- 選択しない --
[通信事業者識別コード（Carrier Identification Code）]	空白のままにします。値は何も入力しないでください。
[ネットワーク サービス（Network Service）]	-- 選択しない --

パーティション PSTNInternational の PSTN 国際ルート パターンはダイヤリング ドメイン（国）固有ではありませんが、パーティション USPSTNNational および USEmergency のルート パターンは国固有です。ダイヤル プランで他の国をサポートしなければならない場合は、表 2-31 に示すように、それらの国のルート パターンを作成する必要があります。

表 2-31　国内接続先用の米国以外のルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
\+49!	DEPSTNNational	RL_PSTN	国コード 49 を持つドイツの番号計画が可変長のため、可変長。
\+49!#	DEPSTNNational	RL_PSTN	可変長のダイヤルを # で終わらせることができるようにするための、国内接続先の代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] に設定。

表 2-31　国内接続先用の米国以外のルート パターン（続き）

パターン	パーティション	ゲートウェイまたはルート リスト	説明
\+33XXXXXXXXX	FRPSTNNational	RL_PSTN	フランスの国内接続先用の明示的パターン。 国際接続先用に定義された可変長の PSTN ルート パターン \+! との重複を避けるために、[緊急優先（Urgent Priority）] をチェックします。
112	DEEmergency	RL_Emergency	ドイツの緊急コール [緊急優先（Urgent Priority）] をチェックします
0112	DEEmergency	RL_Emergency	ドイツの緊急コール [緊急優先（Urgent Priority）] をチェックします
112	FREmergency	RL_Emergency	フランスの緊急コール [緊急優先（Urgent Priority）] をチェックします
0112	FREmergency	RL_Emergency	フランスの緊急コール [緊急優先（Urgent Priority）] をチェックします

表 2-31 に、固定長と可変長の番号計画の違いを示します。ドイツの国内番号計画は可変長なので、ドイツの国内接続先に一致させるルート パターンは可変長の数字列に一致する必要があります。また、ユーザが電話番号を明示的に # で終わらせることができるように、# で終わる代替ルート パターンをプロビジョニングして、国内接続先にダイヤルする際の番号間タイムアウトを回避する必要もあります。これとは対照的に、フランスの国内番号計画は固定長（米国と同じ）なので、1 つの固定長の緊急用ルート パターンでフランスの全国内番号をカバーできます。

ドイツとフランスは同じ緊急ダイヤル手順を使用するため、緊急用パーティション DEEmergency および FREmergency の両方を組み合わせて 1 つのパーティション 112Emergency とし、CSS 定義で代わりにそのパーティションを使用することにより、緊急用ルーティングを簡素化することができます。

多国間環境における緊急コールの考慮事項

個々のサービス クラスとは独立して、全エンドポイントから常時緊急番号へアクセスできることが必要です。前述のように、これは緊急コール ルート パターンを持つパーティションをすべての CSS に追加することで、簡単に実現します。この方法で問題が生じるのは、複数の国をサポートしなければならず、それらの国で異なる緊急ダイヤル手順が必要であり、エクステンション モビリティやデバイス モビリティなどのモビリティ機能が使用される場合です。

そのような場合、異なる緊急ダイヤル手順のある複数の国の間でユーザがローミングを行うと、このユーザが使用しているデバイスはアクセス中のユーザが使用する緊急ダイヤル手順を継承します。たとえば、ドイツのユーザがアメリカの電話にログインすると、ドイツ人ユーザのエクステンション モビリティ プロファイルで定義された回線 CSS が、アクセス先であるアメリカの電話に割り当てられ、この電話の緊急コールはドイツの緊急電話番号 112 を使ってかけなければならず、米国の緊急コールのダイヤル手順である 911 はサポートされません。

外国人ユーザが電話にログインするかどうかに関わらず、任意の国の電話が常にその国の国内緊急コールのダイヤル手順をサポートするように、緊急コール用に異なる方式を実装できます。USEmergency をすべての CSS に追加する代わりに、専用の USEmergency CSS を作成し、その CSS を米国のすべてのデバイスにデバイス CSS として割り当てます。こうすると、外国人ユーザが米国の電話にログインした場合に、回線 CSS により定義されたアクセス中のユーザの「ホーム」ダイヤル手順が、アクセス先の国の緊急ダイヤル手順と結びつきます。ドイツ人ユーザが米国の電話にログインする上記のケースでは、そのユーザのドイツ式 PSTN ダイヤル手順は、米国固有の緊急ダイヤル手順 911 と一緒にサポートされるようになります。異なる国間でのこうしたダイヤル手順の組み合わせにより、アクセス先の緊急ダイヤル手順とアクセス中のユーザの通常のダイヤル手順との間に重複が生じる可能性があることを念頭に置く必要があります。たとえば、ドイツのサイトが 9 で始まる 4 桁の内線番号を持つ場合（+E.164 範囲が +49 6100 773 9XXX など）、そのドイツのサイトのユーザが米国の電話にログインすると、9XXX ダイヤリング正規化トランスレーション パターンによりそのサイトに定義された 4 桁のサイト内短縮ダイヤルが、米国緊急ダイヤル 911 と重複してしまいます。緊急ダイヤル手順がより固有である限り、緊急パターンとして緊急コール ルート パターンを作成することにより、緊急コールをかけるときに遅滞が生じないことが保証されます。一方で、911 の米国緊急パターンは 911 で始まるすべての 4 桁のダイヤルを「ブロック」する可能性があり、これにより、例えば +49 6100 773 911X などの電話番号への 4 桁のサイト内のダイヤルに影響を与えることがあります。

緊急ダイヤルを回線 CSS からデバイス CSS に移動すると、アクセス中のユーザの緊急ダイヤル手順（ドイツ人ユーザの場合は 112）をアクセス先の国の緊急ダイヤル手順（米国の場合は911）に変換しなければならないという問題も回避できます。

PSTN（ISDN）ビデオ コールのルート パターン

コスト面から見て、通常のボイスコールに ISDN ビデオ ゲートウェイを使用することは実現不可能なため、ダイヤル プランの観点からビデオ用の ISDN ゲートウェイに特別の処理が必要です。この設計では、ビデオ ISDN ゲートウェイの選択を、特別なビデオ PSTN ダイヤル手順に明示的に結びつけます（表 2-12 を参照）。表 2-32 に、このダイヤル手順を有効にするために必要なルート パターンを記載します。

表 2-32　　ビデオ PSTN（ISDN）コールのルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
*!	PSTNInternational	RL_VIDEO	* で表された E.164 をサポートする必要があるため、可変長。
*!#	PSTNInternational	RL_VIDEO	# を使用した可変長のダイヤルを終了できるようにするための代替パターン。 [番号の削除（Discard Digits）] を [末尾番号（Trailing-#）] に設定。
*1XXXXXXXXXX	PSTNInternational	RL_VIDEO	番号間タイムアウトを発生させずに米国の着信先（固定長）にダイヤルできるようにするための補足ルート パターン。 [緊急優先（Urgent Priority）] をオンに設定。

ビデオ ISDN ルート パターンをパーティション PSTNInternational に含めると、実質的に「国際」サービス クラスにビデオ ダイヤル機能が追加されます。

アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーション

このマニュアルで説明するダイヤル プランの設計では、ローカル ルート グループを使用して、発信側デバイスに基づく出力ゲートウェイを選択します。したがって、サービス プロバイダの要件に適応するために必要な発信側および着信側トランスフォーメーションは、ルート パターンまたはルート リストのレベルで行うことができません。その場合、これらのトランスフォーメーションは、すべてのゲートウェイで共有されることになります。そのため、これらのサービス プロバイダ固有の発信側および着信側トランスフォーメーションは、Cisco IOS 音声トランスレーション ルールを使用してゲートウェイに設定するか、発信側または着信側トランスレーション パターン（ゲートウェイまたはゲートウェイのデバイス プールに設定された発信側または着信側トランスレーション CSS によって対処するパターン）を使用して Unified CM に設定します。

ISDN トランクでは、発信側番号および着信側番号の情報が、発信側および着信側の情報要素で送受信されます。これらの情報要素は、番号計画、番号タイプ、および番号の 3 つで構成されます。これらのフィールドをどのように設定しなければならないかは、プロバイダのトランク サービス定義に依存します。一例として、ドイツ国内の同じ市外局番 6100 内のトランクにある E.164 着信番号 4961007739764 へのコールの場合、発信 ISDN SETUP メッセージに含まれる着信側番号は、（番号計画/タイプ/番号の形式で）「ISDN/national/61007739764」、「ISDN/subscriber/7739764」、または「unknown/unknown/061007739764」として送信される場合があります。

ISDN トランクの終端となるゲートウェイが SIP を使用して Unified CM に接続されている場合、SIP は番号タイプの概念を把握しないため、番号タイプを Unified CM からゲートウェイに送信することはできません。コールのタイプによって異なる ISDN 番号タイプをサポートする必要があるかどうかは、プロバイダの SIP トランク サービス定義によって決まります。ISDN トランクでは、一部のプロバイダは常に、着信先にかかわらず、同じ ISDN 計画およびタイプのインジケータを使用した着信側番号と発信側番号の送信を許可します。

表 2-33 に、米国の ISDN プロバイダが許容する可能性のある代替着信側番号形式の例を記載します。

表 2-33　　米国 ISDN トランクでのコールの代替 ISDN 番号形式

コールのタイプ	接続先	PSTN に送信される着信側の番号計画/タイプ/番号	ゲートウェイに送信される数字列
国内	+12125551234	unknown/unknown/12125551234	*12125551234
国際	+4961007739764	unknown/unknown/0114961007739764	*0114961007739764

ゲートウェイに送信される数字列の先頭には、ゲートウェイでのダイヤルピア定義を簡略化したプレフィックス「*」が付加されます。PSTN から受信する着信側番号が「*」で始まることは決してありません。したがって、ゲートウェイに送信する着信側番号にプレフィックス「*」を使用することで、インバウンド コールとアウトバウンド コールに関して、簡単で競合のない宛先パターンに基づいたアウトバウンド ダイヤルピアの選択がゲートウェイで可能です。コールを PSTN に送信する前に、Unified CM によって先頭に付加された「*」をゲートウェイで削除する必要があります。Unified CM からゲートウェイに送信されるすべての着信側番号で、先頭に「*」を使用すると、ゲートウェイで POTS ダイヤルピアに対して「宛先パターン *」を使用することが可能になります。この場合、先頭の「*」は、Cisco IOS のデフォルトでの桁削除動作により自動的に削除されます。

着呼側の +E.164 着信番号から PSTN に送信される数字列へのトランスフォーメーションは、Unified CM で行うことができます。ゲートウェイでは、例 2-2 に記載する Cisco IOS 音声トランスレーション ルールを使用して、簡単に ISDN 計画およびタイプを適用できます。

例 2-2　単一の ISDN 計画およびタイプを適用する Cisco IOS 音声トランスレーション

```
voice translation-rule 1
    rule 1 /^\*/ // type any unknown plan any unknown
    rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
    translate called 1
    translate calling 1
dial-peer voice 1 pots
    translation-profile outgoing ISDNunknown
```

例 2-2 に記載されている、Cisco IOS 設定の抜粋には、特定の POTS ダイヤルピアから PSTN に送信される発信側と着信側の情報に単一の ISDN 計画およびタイプを適用する方法が示されています。voice-translation-rule 1 のルール 1 は、「*」で始まるすべての番号に一致し、この先頭の「*」を除去します。voice translation-rule 1 のルール 2 は、任意の計画およびタイプのすべての番号に一致し、計画とタイプの両方を「unknown」に強制する一方で、番号の実際の数字列は変更しません。ISDN を指す POTS ダイヤルピアに、この Cisco IOS 音声トランスレーション ルールを適用することで、計画とタイプが「unknown」に強制された上で、Unified CM からゲートウェイに送信されるすべての着信側番号と発信側番号が変更されずに PSTN に転送されます。

このトランスレーション ロジックをゲートウェイに設定した場合、Unified CM 側では、+E.164 着信側情報を 表 2-33に従った数字列に変換してから PSTN に送信するようにプロビジョニングする必要があります。表 24 に、ISDN ダイヤル用に +E.164 をローカライズするために必要な着信側トランスフォーメーション パターンを記載します。

表 2-34　SIP を使用した ISDN 用に +E.164 をローカライズするための着信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.1!	USGWLocalizeCd	ドットの前の番号を削除して、先頭に * を付加	+12125551234 –> *12125551234
\+.!	USGWLocalizeCd	ドットの前の番号を削除して、先頭に *011 を付加	+4961007739764 –> *0114961007739764

表 2-34 に記載されている着信側トランスフォーメーション パターンで定義された着信側トランスフォーメーションをゲートウェイに適用するには、まず、USGWLocalizeCd パーティションだけを設定した CSS USGWLocalizeCd を定義します。そして、ゲートウェイのデバイス プールの [デバイスモビリティ関連情報（Device Mobility Related Information）] セクションで、その CSS を [着信側トランスフォーメーションCSS（Called Party Transformation CSS）] として設定します。これらのトランスフォーメーションをデバイス プールに設定すれば、同じ着信側トランスフォーメーション要件を共有する同じサイト内の複数のゲートウェイで、これらの同じ設定を共有することができます。それには、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションで、[デバイスプールの着信側トランスフォーメーションCSSを使用（Use Device Pool Called Party Transformation CSS）] オプションをオンにする必要があります。

また、必要なプロビジョニングとして、+E.164 からサービス プロバイダへ送信しなければならない形式への発信側番号のトランスフォーメーションを行います。ここで、非 DID から発信されるコール、または特定のゲートウェイに関連付けられた DID 範囲に含まれない DN から発信されるコールの発信側情報を処理する方法を検討する必要があります。最も一般的な選択肢は、発信者 ID をサイト固有の主要な内線番号に設定することです。このサイトでは特に、表 2-35 に記載するサイト固有の発信側トランスフォオーメーションを作成する必要があります。

表 2-35　SIP を使用した ISDN 用に +E.164 をローカライズするための発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.19195551XXX	RTPGWLocalizeCn	ドットの前の番号を削除	+19195551001 –> 19195551001 ゲートウェイに関連付けられた DID 範囲の発信者 ID を転送。ただし、発信側番号を 1 プラス 10 桁の数字で送信できることを前提に、先頭のプラス（+）を削除
\+!	RTPGWLocalizeCn	19195551888 をマスク	すべてを 19195551888 に強制
!	RTPGWLocalizeCn	19195551888 をマスク	すべてを 19195551888 に強制

表 2-35 に記載されている発信側トランスフォーメーション パターンは、+E.164 形式の番号であるか、トランクの DN 範囲に一致しない企業固有の番号であるかにかかわらず、すべての発信側番号が主要な番号（19195551888）に強制されるようにするために必要なトランスフォーメーションを行います。

前述のアウトバウンド着信側トランスフォーメーションに適用する手法に相当する、これらのトランスフォーメーションを可能にするには、まず、パーティション RTPGWLocalizeCn だけを使用した CSS RTPGWLocalizeCn を作成します。そして、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションまたはゲートウェイのデバイス プールの [デバイスモビリティ関連情報（Device Mobility Related Information）] セクションで、その CSS を 発信側トランスフォーメーション CSS として適用します。

ゲートウェイごとに特定の着信側または発信側トランスフォーメーションが必要な場合、着信側トランスフォーメーションにデバイス プール レベルの設定を使用すると、複雑になりすぎます。その場合には、ゲートウェイ設定ページの [アウトバウンドコール（Outbound Calls）] セクションで、[デバイスプールの着信側/発信側トランスフォーメーションCSSを使用（Use Device Pool Called/Calling Party Transformation CSS）] オプションをオフにして、着信側または発信側トランスフォーメーション CSS を設定します。

アウトバウンド コール：SIP トランクでの着信者番号および発信者番号のトランスフォーメーション

前述のように、SIP には、番号の「タイプ」という概念がありません。通常、SIP トランクでは、着信先のタイプにかかわらず、すべての着信者番号と発信者番号を単一の形式で送信する必要があります。最も一般的な選択肢は、+E.164 または E.164 です。インバウンド コールおよびアウトバウンド コールの宛先パターンを重複させることなく、より簡単なダイヤルピア設定を行うには、SIP トランクの終端となる Cisco Unified Border Element に送信されるすべての E.164 着信側情報に、プレフィックス「*」を付加する必要があります。

(+ を含まない)E.164 を送信する必要がある場合は、着信側トランスフォーメーション パターンを使用した前述の手法を使用できます。表 2-36 に記載されている着信側トランスフォーメーションを 1 回行えば、すべての +E.164 番号から先頭の + を除去できます。この場合も、パーティション GWNoPlus だけに対応する CSS(例えば、GWNoPlus)を作成してから、ゲートウェイまたはゲートウェイのデバイス プールのいずれかに対し、この着信側トランスフォーメーション パターンを [着信側トランスフォーメーションCSS(Called Party Transformation CSS)] として適用する必要があります。

表 2-36　SIP 用に +E.164 を *E.164 へローカライズするための着信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.!	GWNoPlus	ドットの前の番号を削除して、先頭に * を付加	+4961007739764 –> *4961007739764 +12125551234 –> *12125551234

送信される着信側情報の形式を SIP トランクで変換する必要がないとしても、有効な番号だけがプロバイダに送信されるようにするには、何らかのフィルタリングを着信側情報に適用する必要があります。アウトバウンド コール:ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーションの項で説明し、表 2-35に要約した発信側トランスフォーメーションと同じものを使用できます。さらに、Cisco Unified Border Element の Cisco IOS 音声トランスレーションにより、確実に、プロバイダの形式要件に従って発信側情報がプロバイダに送信されます。例 2-3 に、プロバイダを指す Cisco Unified Border Element(CUBE)上で VoIP ダイヤルピアに適用される Cisco IOS 音声トランスレーションを記載します。これらのトランスレーションにより、着信側情報が *E.164 から +E.164 に変換され、発信側情報が E.164 から +E.164 に変換されます。

例 2-3　CUBE で +E.164 発信側番号と着信側番号に強制される Cisco IOS 音声トランスレーション

```
voice translation-rule 2
    rule 1 /^\*/ /+/
    rule 2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 2 voip
    translation-profile outgoing SIPtoE164
```

例 2-3 のルール 1 は先頭の「*」を「+」に置き換え、ルール 2 はすべての番号の先頭にプレフィックス「+」を付加します。

インバウンド コール：ISDN ゲートウェイでの着信者番号および発信者番号のトランスフォーメーション

Unified CM にルーティングされるコールはすべて、Unified CM に到着するすべての着信コールの +E.164 に基づくため、リンクで受信されたプロバイダからの着信側情報の形式が確実に +E.164 に変換されなければなりません。アウトバウンド コール：ISDN ゲートウェイでの着信者番号と発信者番号のトランスフォーメーションの項で説明したように、ISDN トランクで送受信する発信側情報と着信者情報は、番号計画、番号タイプ、および番号の 3 つで構成されています。SIP では番号タイプをサポートしていないため、実際の番号だけがゲートウェイから SIP トランク経由で Unified CM に転送されるとしたら、プロバイダから受信した番号タイプの意味が失われてしまいます。この状況を回避するためには、ゲートウェイに Cisco IOS 音声トランスレーションを導入し、受信した番号計画、番号タイプ、番号に基づく +E.164 数字列を作成して Unified CM に送信する必要があります。例 2-4 に、この目的を果たすための Cisco IOS 音声トランスレーションの設定を記載します。

例 2-4　ISDN を +E.164 にマッピングする Cisco IOS 音声トランスレーション

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3
dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

例 2-4 に記載されている Cisco IOS トランスレーションは、受信する着信側情報のタイプが「national」であること、したがって番号が 10 桁のみであることを前提とします。ルール 1（/^\(.+\)$/）は、タイプが「international」に設定されたすべての番号にプレフィックス「+1」を付加し（/+\1/）、計画およびタイプを「unknown」に強制します。SIP トランクで Unified CM に転送する場合、計画とタイプは両方とも無関係であるためです。この同じトランスレーション ルールが、トランスレーション プロファイル ISDNtoE164 で発信側情報と着信側情報の両方に適用されます。したがって、タイプが「national」に設定された 10 桁の番号である発信側情報は、ルール 1 によって適切に +E.164 に変換されます。ルール 2 は、実際には着信側情報に適用されません。プロバイダは一般に、単一の形式だけを使用して着信側情報を送信するためです。したがって、ルール 2 が関係してくるのは、国外から受信したコールに限られます。この場合、受信する発信側情報は「international」タイプであり、番号は発信側の完全な E.164 番号に設定されていることになります。

プロバイダによって使用される番号形式は異なる場合があるため、ゲートウェイまたは Unified CM で異なる複数のトランスフォーメーションを使用する必要が生じてきます。音声トランスレーション ルールの詳細については、『*Number Translation using Voice Translation Profiles*』を参照してください。このドキュメントには、以下の URL でアクセスできます。

http://www.cisco.com/c/en/us/support/docs/voice/call-routing-dial-plans/64020-number-voice-translation-profiles.html

何らかの理由で発信側情報と着信側情報の両方に同じ音声トランスレーション ルールを使用できない場合、発信側情報と着信側情報にそれぞれ個別の音声トランスレーション ルールをプロビジョニングして、1 つのトランスレーション プロファイルで発信側トランスレーションと着信側トランスレーションを関連付ける必要があります。

インバウンド Cisco IOS 音声トランスレーション ルールを使用する必要があるのは、プロバイダから複数の異なる番号タイプが送信される場合のみです。たとえば、発信側情報または着信側情報の番号タイプが常に不明である場合は、Unified CM で数字をグローバル化された +E.164 に変換するために、発信側情報と着信側情報にインバウンド プレフィックスを使用するか、発信側および着信側トランスフォーメーション CSS を使用することができます。プレフィックスと発信側および着信側トランスフォーメーションの両方を、トランク レベルまたはデバイス プール レベルで定義することもできます。ただし、SIP では異なる番号タイプをサポートしていないため、デバイス プール レベルで定義する場合は、インバウンド プレフィックスまたは発信側および着信側 CSS を番号タイプ **unknown** に設定する必要があります。

インバウンド コール：SIP トランクでの着信者番号と発信者番号のトランスフォーメーション

一般に、PSTN SIP トランクでのインバウンド コール番号情報の処理は、前述の ISDN の場合の番号処理よりも単純です。その主な理由は、SIP トランクでの番号情報にはタイプが設定されていないためです。したがって、トランスフォーメーションの複雑さは軽減され、考慮しなければならないのは受信した数字列だけとなります。通常、SIP トランクでの発信側情報と着信側情報はすでに +E.164 形式になっているため、トランスフォーメーションは不要です。

E.164 形式で受信した発信側情報と着信側情報を +E.164 形式に変換する最も簡単な方法は、Unified CM の SIP トランクまたはトランクのデバイス プールでプレフィックス「+」を付加するように設定することです。このプレフィックスは、トランクまたはトランクのデバイス プールの [着信の発呼側設定（Incoming Calling Party Settings）] または [着信の着呼側設定（Incoming Called Party Settings）] に設定できます。SIP トランクの場合、[不明な番号（Unknown Number）] の設定は、デバイス プール レベルに適用されることに注意してください。

電話上での発信側情報の表示

+E.164 電話番号から発信されるコールの場合、すべての電話番号は +E.164 番号としてプロビジョニングされるため、発信側情報は自動的に +E.164 形式になります。考えられるあらゆるコール フローでの発信側情報の表示を単純化して一貫性を持たせるために、PSTN などの外部ネットワークから受信するすべての発信側情報は、前述のように +E.164 に正規化されます。電話や外部ネットワークにコールを表示する際には、そのコールに関して表示される発信側情報を、外部ネットワークが必要とする形式（そのコールがゲートウェイに送信される場合）またはユーザが必要とする形式（電話に送信される場合）に変換しなければならないことがあります。

非 DID を使用した電話から発信されるコールには、特殊な考慮事項があります。この場合、使用可能な発信側情報は、ESN（Enterprise Specific Number）形式でプロビジョニングされた非 DID と同一です。表 2-10 に、サンプル トポロジーで使用されている ESN 範囲を要約します。

電話の場合、優先される発信側の表示情報が +E.164 形式ではない場合もありますが、この情報を +E.164 として保持すると、展開が簡素化されるため、この方法が推奨されます。その場合の望ましい形式は、通常、発信側エンティティと着信側エンティティの両方に依存します。表 2-37 に、サイト SJC の電話で、各種のソースからのコールで必要とされる発信側情報表示の例を記載します。

表 2-37　　SJC 電話で必要とされる発信側情報表示

発信側エンティティの「ネイティブ」発信側情報	期待される表示	コメント
+12125551234+12125551234	912125551234	米国からのコール。PSTN ダイヤル手順に従った表示。
+14085554001	4001	SJC DID 範囲の +E.164 DN からのコール。サイト内短縮ダイヤル手順に従った表示。
81405001	5001	SJC ESN 範囲の非 DID からのコール（表 2-10 を参照）。サイト SJC 内の非 DID への 4 桁のサイト内短縮ダイヤル手順に従った表示。
+4961007739764	90114961007739764	国際 PSTN 接続先からのコール。国際コール着信先に対する米国 PSTN ダイヤル手順に従った表示。

表 2-37 に記載されている表示形式を実現するには、発信側トランスフォーメーション パターンを適切なパーティションにプロビジョニングし、それらのパーティションに基づく発信側トランスレーション CSS を電話に設定して、トランスフォーメーションを有効にする必要があります。

表 28 に、表 2-10 に記載された番号範囲に基づき、米国のすべてのサイトに関して、表 2-37 に記載された短縮発信側番号を表示するためにプロビジョニングする必要がある、すべての発信側トランスフォーメーション パターンを記載します。

表 2-38　　電話ローカリゼーション発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+.1!	USPhLocalize	ドットの前の番号を削除して、先頭に 9 を付加	米国のすべての着信先： +12125551234 –> 912125551234
\+.!	USPhLocalize	ドットの前の番号を削除して、先頭に 9011 を付加	すべての国際コール着信先： +4961007739764 –> 90114961007739764
\+14085554XXX	SJCPhLocalize	4XXX をマスク	ローカル DN 範囲からのコール： +14085554001 –> 4001
81405XXX	SJCPhLocalize	5XXX をマスク	ローカル非 DID 範囲からのコール： 81405001 –> 5001
\+19725555XXX	RCDPhLocalize	5XXX をマスク	ローカル DN 範囲からのコール： +19725555001 –> 5001
81976XXX	RCDPhLocalize	6XXX をマスク	ローカル非 DID 範囲からのコール： 81976001 –> 6001
\+19195551XXX	RTPPhLocalize	1XXX をマスク	ローカル DN 範囲からのコール： +19195551001 –> 1001
81912XXX	RTPPhLocalize	2XXX をマスク	ローカル非 DID 範囲からのコール： 81912001 –> 2001

表 2-39 に、米国の全サイトの電話の発信側ローカリゼーションを有効にするための発信側トランスフォーメーション CSS を記載します。このスキーマを使用すると、ダイヤル発信ドメイン（国）に固有の発信側ローカリゼーション トランスフォーメーション パターンを、そのダイヤル発信ドメイン（国）内のすべてのサイトに再利用できます。国固有の発信側ローカリゼーション パターンは、基本的に、国番号と国際番号をその国に固有の国内および国際ダイヤル手順にマッピングします。

表 2-39　米国のサイトの電話ローカリゼーション発信側トランスフォーメーション CSS

CSS	パーティション
SJCPhLocalize	SJCPhLocalize USPhLocalize
RCDPhLocalize	RCDPhLocalize USPhLocalize
RTPPhLocalize	RTPPhLocalize USPhLocalize

表 2-40 に、国固有の電話ローカリゼーション発信側トランスフォーメーション パターンの例を記載します。これは、イタリアおよびドイツに対してプロビジョニングする必要があるパターンの例です。

表 2-40　イタリアおよびドイツの電話ローカリゼーション発信側トランスフォーメーション パターン

パターン	パーティション	トランスフォーメーション	説明
\+49.!	DEPhLocalize	ドットの前の番号を削除して、先頭に 00 を付加	ドイツのすべての着信先: +4941001234 –> 0041001234
\+.!	DEPhLocalize	ドットの前の番号を削除して、先頭に 000 を付加	すべての国際コール着信先: +14085551234 –> 00014085551234
\+39.!	ITPhLocalize	ドットの前の番号を削除して、先頭に 0 を付加	イタリアのすべての着信先: +390730123456 –> 00730123456 +393012345678 –> 03012345678
\+.!	ITPhLocalize	ドットの前の番号を削除して、先頭に 000 を付加	すべての国際コール着信先: +14085551234+14085551234 –> 00014085551234

自動代替ルーティング

登録済みエンドポイントへのコールが帯域幅の不足により失敗した場合（コール アドミッション制御の失敗）、自動代替ルーティング（AAR）を使用して、そのコールを PSTN に再ルーティングできます。AAR をアクティブ化するために必要な手順は、以下のとおりです。

- [自動代替ルーティングの有効化（Automated Alternate Routing Enable）] サービス パラメータを設定します（サービス パラメータの設定の項を参照）。
- [ダイヤルプレフィックス（Dial Prefix）]（デフォルト）を設定せずに、Default という単一の AAR グループを設定します。

- +E.164 PSTN ルート パターンへのアクセスだけを設定した CSS PSTNReroute を設定します。この設計例に基づく CSS には、パーティション PSTNInternational だけを含める必要があります。
- AAR の対象となる可能性があるコールを開始するエンドポイント、トランク、およびその他のデバイスのすべてで、以下を設定します。
  - [AARコーリングサーチスペース（AAR Calling Search Space）] を PSTNReroute に設定します。
  - [AARグループ（AAR Group）] を Default に設定します。
- すべてのデバイス ポートで、[AARコーリングサーチスペース（AAR Calling Search Space）]を PSTNReroute に設定します。
- [AARグループ（AAR Group）] を Default に設定します。
- +E.164 電話番号に AAR マスクを設定し、その電話番号が +E.164 番号になるようにします。固定長の番号計画を使用する国では、すべての電話番号でマスクを同じ値に設定できます（たとえば米国では、+1XXXXXXXXXX など）。可変長の電話番号に対応する必要がある場合、単一のサイトをカバーする具体的なマスクをプロビジョニングします。あるいは最悪の場合、それぞれの電話番号と同じ完全修飾子を付けた +E.164 AAR マスクをプロビジョニングする必要があります。非 DID の場合、AAR マスクは空のままにします。これにより実質的に、非 DID が呼び出された場合は AAR が無効になります。非 DID には同等の E.164 アドレスがなく、PSTN を介してアクセスできないため、これは理にかなっています。

上記のリストでは、+E.164 電話番号を使用したダイヤル プランの利点の 1 つが示されています。この場合、他に変更を加えることなく、着信側 +E.164 アドレスを PSTN 経由の代替ダイヤルに直接再使用できるためです。

未登録エンドポイントの代替ルーティング

コール処理を一元化したマルチサイト展開環境で WAN に障害が発生した場合、その障害によって中央の Unified CM との接続を失ったエンドポイントは、代わりにローカル SRST ゲートウェイに登録します（Survivable Remote Site Telephony（SRST）展開の項を参照）。これにより、影響を受けた電話をそのまま配置して、受信したコールを同じサイト内の電話と PSTN との間で受け渡すことができます。ただし、中央の Unified CM の観点からは着信デバイスは登録されていないため、そのデバイスには到達できません。したがって、中央の Unified CM に登録された電話からのコールは失敗します。PSTN を介した未登録エンドポイントへのコールの自動再ルーティングを有効にするには、自動再ルーティングが必要な電話番号のそれぞれに対して、以下のタスクを実行します。

- [未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）] の宛先を、E.164 電話番号と同じ値に設定します。
- [未登録内線の不在転送のCSS（Forward Unregistered Internal CSS）] および [未登録外線の不在転送のCSS（Forward Unregistered External CSS）] を、PSTNReroute に設定します。これは、自動代替ルーティングの項で定義したのと同じ CSS です。これにより、PSTN ルート パターンにアクセスできるようになります。

未登録エンドポイントに対する PSTN を介した代替ルーティングが意味を持つのは、+E.164 電話番号のみです。DID を使用しないエンドポイント（電話番号として ESN を使用するエンドポイント）の場合、未登録エンドポイントに対して意味を持つ再ルーティングは、着信コールをボイスメールに転送するというルーティングだけです。未登録エンドポイントへのコールをボイスメールに転送するには、以下のタスクを実行します。

- [未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）] に [ボイスメールオプション（Voicemail options）] を選択します。
- [未登録内線の不在転送のCSS（Forward Unregistered Internal CSS）] および [未登録外線の不在転送のCSS（Forward Unregistered External CSS）] を、「国内」サービス クラスを実装する CSS（たとえば、SJCInternal）に設定します。実質的に、この CSS ではボイスメール パイロット番号にのみアクセスできます。

LDAP 同期によるユーザ プロビジョニング

Unified CM を社内 LDAP ディレクトリに同期すると、管理者は Unified CM データ フィールドをディレクトリ属性にマッピングすることにより、ユーザを容易にプロビジョニングできるようになります。LDAP ストアに保持されている重要なユーザ データは、スケジュール ベースで Unified CM データベース内の対応する適切なフィールドにコピーされます。社内 LDAP ディレクトリのステータスは、中央リポジトリのままとなります。Unified CM は、ユーザ データを保存するための統合データベースを備え、またユーザ アカウントおよびデータを作成して管理するための Web インターフェイスを、Unified CM Administration 内に備えています。LDAP 同期を有効にすると、ローカル Unified CM データベースを引き続き使用しながら、追加のローカル エンドユーザ アカウントを作成できます。エンドユーザ アカウントは、LDAP ディレクトリのインターフェイスおよび Unified CM 管理 GUI で管理できます。

LDAP システムの設定

実際の同期アグリーメントを定義する前に、LDAP システムを有効にする必要があります。[LDAPシステムの設定（LDAP System Configuration）] メニューでは、次の操作を実行できます。

- [LDAPサーバからの同期を有効にする（Enable Synchronizing from LDAP Server）] オプションを選択する（チェックボックスをオンにする）。
- 展開環境に適切な [LDAPサーバタイプ（LDAP Server Type）] を選択する。
- 展開環境に適切な [ユーザIDのLDAP属性（LDAP Attribute for User ID）] を選択する。

Microsoft Active Directory からユーザが同期される環境では、表 2-41 に記載する設定を使用します。

表 2-41　Microsoft Active Directory の場合の LDAP システム設定

設定	値
[LDAPサーバタイプ（LDAP Server Type）]	Microsoft Active Directory
[ユーザIDのLDAP属性（LDAP Attribute for User ID）]	sAMAccountName

LDAPカスタムフィルタ

Unified CM ベースのディレクトリ検索が電話で使用されている場合は、社内 LDAP ディレクトリ全体を Unified CM に同期することが理にかなっています。その場合、実際にローカル クラスタの UC サービスを使用するユーザと、完全な社内 LDAP ディレクトリを Unified CM に反映するためだけに同期されるユーザとを区別可能にする必要があります。

この目標を達成するには、カスタム LDAP フィルタを使用して、ローカル ユーザ グループとリモート ユーザ グループの 2 つを定義できます。ここで言うリモート ユーザとは、ローカル Unified CM クラスタの UC サービスを一切使用しないユーザを意味します。表 2-42 に、2 つのカスタム LDAP フィルタを記載します。ここでは、展開環境のユーザが米国と欧州に存在し、米国のユーザのみがローカル ユーザであることを前提としています。

表 2-42　　カスタム LDAP フィルタ設定

LDAP フィルタ名	フィルタ
[ローカル(Local)]	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (telephoneNumber=+1*))
[リモート(Remote)]	(& (objectclass=user) (!(objectclass=Computer)) (!(UserAccountControl:1.2.840.113556.1.4.803:=2)) (| (telephoneNumber=+3*) (telephoneNumber=+4*)))

読みやすくするために、表 2-42では、インデント レベルに LDAP フィルタ文字列の構造を反映して、LDAP フィルタ文字列を複数の行に分けて記載しています。これらの LDAP フィルタを Unified CM にプロビジョニングするには、特定のフィルタのすべての行を 1 行に連結する必要があります。

上記の LDAP フィルタは、どちらも Microsoft Active Directory のデフォルト LDAP フィルタを拡張したものです。他のディレクトリ タイプのデフォルト LDAP フィルタは、『*Cisco Collaboration System 10.x SRND*』の「*Directory Integration and Identity Management*」の章に記載されています。また、ディレクトリ設定については、Unified CM オンライン ヘルプを参照してください。

表 2-42 に記載されている LDAP フィルタでは、電話番号の開始部分を基準として、個々のユーザがローカル ユーザまたはリモート ユーザのどちらであるかを判別します。

複数の LDAP 同期アグリーメントを使用する場合は、それらの同期アグリメーメントで使用される LDAP フィルタを分離して、同じユーザが複数のフィルタに一致しないようにしてください。

機能グループ テンプレート

LDAP からユーザを同期する機能は、機能グループ グループ テンプレート（FGT）に定義されています。表 2-43 に、Unified CM クラスタのアクティブ デバイスでのユーザの機能を定義する FGT の設定を要約します。

表 2-43　ローカル ユーザの機能グループ テンプレート

設定	値	コメント
[名前（Name）]	FGTlocal	名前でローカル ユーザ用の FGT であることを示す必要があります。
[説明（Description）]	ローカルユーザ用の FGT	
[ホームクラスタ（Home Cluster）]	オン	このユーザの UDS ベースのサービス検出がローカル Unified CM クラスタに解決されるようにします。
[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）]	オン	IM and Presence のユーザを有効にします。
[BLFプレゼンスグループ（BLF Presence Group）]	標準のプレゼンス グループ	展開を簡素化するために、すべてのユーザを単一の BLF プレゼンス グループに割り当てます。
[SUBSCRIBEコーリングサーチ（SUBSCRIBE Calling Search）]	DefaultSubscribe	特殊な CSSの項で説明している、デフォルトのサブスクライブ CSS を使用します。

その他すべての設定には、デフォルト値をそのまま使用できます。

リモート ユーザも LDAP から同期されるため（LDAPカスタムフィルタの項を参照）、リモート ユーザ用の FGT もプロビジョニングする必要があります。主な違いは、リモート ユーザ用の FGT では、[ホームクラスタ（Home Cluster）] および [Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）] オプションをオンにしないことです。表 2-44 に、これらの設定を要約します。

表 2-44　リモート ユーザの機能グループ テンプレート

設定	値	コメント
[名前（Name）]	FGTremote	名前にリモート ユーザ用の FGT であることを示す必要があります。
[説明（Description）]	リモート ユーザ用の FGT	
[ホームクラスタ（Home Cluster）]	オフ	このユーザの UDS ベースのサービス検出がローカル Unified CM クラスタに解決されないようにします。
[Unified CM IM and Presenceのユーザを有効化（Enable User for Unified CM IM and Presence）]	オフ	IM and Presence のユーザは有効にしません。

その他すべての設定には、デフォルト値をそのまま使用できます。

LDAP 同期アグリーメント

すべてのローカル ユーザを Unified CM に同期させるには、LDAP 同期アグリーメントを構成する必要があります。表 2-45 に、[システム/LDAP/LDAP ディレクトリ（System/LDAP/LDAP Directory）] に構成する必要がある設定を記載します。

表 2-45　ローカル ユーザの LDAP 同期アグリーメント

設定	値	コメント
[LDAP設定名（LDAP Configuration Name）]	[ローカル（Local）]	ローカル ユーザを同期する LDAP 同期アグリーメントであることを示します。
[LDAPマネージャの識別名（LDAP Manager Distinguished Name）]	管理ユーザの名前	ldapaccess@ent-pa.com または cn=ldapaccess,cn=users,dc=ent-pa,dc=com の形式で指定できます。
[LDAPパスワード（LDAP Password）]	LDAP 管理者のパスワード	
[LDAPユーザ検索ベース（LDAP User Search Base）]	LDAP 検索ベース	例：dc=ent-pa,dc=com
[LDAPカスタムフィルタ（LDAP Custom Filter）]	[ローカル（Local）]	LDAPカスタムフィルタの項で説明しているカスタム LDAP フィルタを参照してください。
[同期を1回だけ実行する（Perform Sync Just Once）]	オフ	LDAP 同期を定期的に実行します。
[再同期の実行間隔（Perform a Re-sync Every）]	妥当な間隔	社内ディレクトの変更内容が妥当な間隔で反映されるように、小さな値を設定します。ただし、LDAP 同期を実行すると、Unified CM パブリッシャにかなりの負荷がかかることに注意してください。おそらく、デフォルトの 24 時間間隔で同期を行うのが妥当です。
Directory URI	メール アドレス	通常、ユーザのディレクトリ URI は、ユーザの電子メール アドレスと同じです。
[アクセスコントロールグループ（Access Control Groups）]	[標準CCMエンドユーザ（Standard CCM End Users）] [標準CTIを有効にする（Standard CTI Enabled）]	必要に応じて、その他のアクセス コントロール グループを追加または削除します。ただし、標準 CCM エンドユーザが設定されていないと、ユーザはセルフサービス ポータルにログインできません。
[機能グループテンプレート（Feature Group Template）]	[ローカル（Local）]	機能グループ テンプレートの項で説明している FGT を参照してください。
[LDAPサーバ情報（LDAP Server Information）]	ソースとして使用する社内 LDAP サーバを参照	可能な場合は、冗長サーバをプロビジョニングするようにしてください。

表 2-45 に記載されている LDAP 同期アグリーメントは、前に定義した FGT とカスタム LDAP フィルタを関連付けます。これにより、カスタム LDAP フィルタに一致する社内ディレクトリ内のすべてのユーザについて、Unified CM に、FGT に定義された機能が割り当てられたユーザが作成されます。

ローカル Unified CM クラスタで UC サービスを使用しないリモート ユーザを同期するための専用の LDAP 同期アグリーメントも必要です。表 2-46 に、この LDAP 同期アグリーメントを要約します。

表 2-46　　リモート ユーザの LDAP 同期アグリーメント

設定	値	コメント
[LDAP設定名（LDAP Configuration Name）]	[リモート（Remote）]	これがリモート ユーザを同期する LDAP 同期アグリーメントであることを示します。
[LDAPマネージャの識別名（LDAP Manager Distinguished Name）]	管理ユーザの名前	ldapaccess@ent-pa.com または cn=ldapaccess,cn=users,dc=ent-pa,dc=com の形式で指定できます。
[LDAPパスワード（LDAP Password）]	LDAP 管理者のパスワード	
[LDAPユーザ検索ベース（LDAP User Search Base）]	LDAP 検索ベース	例：dc=ent-pa,dc=com
[LDAPカスタムフィルタ（LDAP Custom Filter）]	[リモート（Remote）]	LDAPカスタムフィルタの項で説明しているカスタム LDAP フィルタを参照してください。
[同期を1回だけ実行する（Perform Sync Just Once）]	オフ	LDAP 同期を定期的に実行します。
[再同期の実行間隔（Perform a Re-sync Every）]	妥当な間隔	社内ディレクトの変更内容が妥当な間隔で反映されるように、小さな値を設定します。ただし、LDAP 同期を実行すると、Unified CM パブリッシャにかなりの負荷がかかることに注意してください。おそらく、デフォルトの 24 時間間隔で同期を行うのが妥当です。
Directory URI	メール アドレス	通常、ユーザのディレクトリ URI は、ユーザの電子メール アドレスと同じです。
[アクセスコントロールグループ（Access Control Groups）]	アクセス コントロール グループの選択なし	リモート ユーザは、どのアクセス コントロール グループにも属しません。
[機能グループテンプレート（Feature Group Template）]	[リモート（Remote）]	機能グループ テンプレートの項で説明している FGT を参照してください。
[LDAPサーバ情報（LDAP Server Information）]	ソースとして使用する社内 LDAP サーバを参照	可能な場合は、冗長サーバをプロビジョニングするようにしてください。

上記の LDAP 同期アグリーメントを使用すると、すべてのユーザを社内ディレクトリから識別できるようになり、LDAP 同期アグリーメントに関連付けられた FGT によって確実に、すべてのユーザに適切な機能が設定されます。

LDAP によるユーザ認証

LDAP 認証機能により、Unified CM が LDAP で同期されたユーザを社内 LDAP ディレクトリに対して認証できます。ローカルに設定されたユーザは、常にローカル データベースに対して認証されます。また、すべてのエンドユーザの PIN も、常にローカル データベースで確認されます。

認証を有効にするには、クラスタ全体に単一の認証アグリーメントを定義します。

認証を有効にした場合の Unified CM の動作説明を、次に示します。

- LDAP からインポートされたユーザのエンドユーザ パスワードは、単一のバインド操作により、社内ディレクトリに対して認証される。
- ローカル ユーザのエンドユーザ パスワードは、Unified CM データベースに対して認証される。
- アプリケーション ユーザ パスワードは、Unified CM データベースに対して認証される。
- エンド ユーザ PIN は、Unified CM データベースに対して認証される。

複数のドメイン コントローラを地理的に分散させた分散型 Active Directory トポロジを採用している環境では、認証速度が許容されない可能性があります。認証アグリーメント用のドメイン コントローラにユーザ アカウントが保持されていない場合、他のドメイン コントローラでそのユーザの検索が実行される必要があります。この設定を適用するときに、ログイン速度が許容範囲外である場合、グローバル カタログ サーバを使用するように認証設定を設定できます。

ただし、重要な制限があります。デフォルトでは、グローバル カタログに employeeNumber 属性が組み込まれません。その場合、ドメイン コントローラを認証に使用するか（上記にリストされた制限に注意）、グローバル カタログを更新して、employeeNumber 属性を組み込みます。詳細については、Microsoft Active Directory のマニュアルを参照してください。

グローバル カタログに対する照会を有効にするには、グローバル カタログ ロールが有効になっているドメイン コントローラの IP アドレスまたはホスト名を指すように [LDAP認証（LDAP Authentication）] ページの [LDAPサーバ情報（LDAP Server Information）] を設定し、LDAP ポートを 3268 として設定するだけです。

表 2-47 に、LDAP 認証設定の例を記載します。

表 2-47　　LDAP 認証設定

設定	例	コメント
[エンドユーザ用LDAP認証（LDAP Authentication for End Users）]		
[エンドユーザにLDAP認証を使用する（Use LDAP Authentication for End Users）]	オン	Unified CM クラスタの LDAP 認証を有効にします。
[LDAPマネージャの識別名（LDAP Manager Distinguished Name）]	cn=ldapmanager,dc=ent pa,dc=com	目的のユーザ検索ベース内のすべてユーザ オブジェクトに対する読み取りアクセス権限が割り当てられた AD アカウントの識別名。
[LDAPパスワード（LDAP Password）]	何らかのパスワード	
[パスワードの確認（Confirm Password）]	同上	
[LDAPユーザ検索ベース（LDAP User Search Base）]	ou=enterprise,dc=ent-pa,dc=com	
[LDAPサーバ情報（LDAP Server Information）]		
[サーバのホスト名またはIPアドレス（Host Name or IP Address for Server）]	ent-dc1.ent-pa.com	グローバル カタログ ロールが割り当てられたサーバ
[LDAPポート（LDAP Port）]	3268	グローバル カタログにアクセスするためのポート（推奨）

Cisco Unified CM グループ設定

Cisco Unified CM グループを使用して、クラスタ内に Unified CM インスタンスのグループを定義し、デバイスが Unified CM クラスタに登録するために使用する Unified CM インスタンスを指定することができます。単一の Unified CM コール処理ペアだけが展開されている場合（詳細については、Cisco Unified CM and IM and Presence Service クラスタのプロビジョンの項を参照）、Default という名前の単一の Unified CM グループも導入し、クラスタ内の単一の Unified CM コール処理サブスクライバ ペアで実行する両方の Unified CM インスタンスを、この単一の Unified CM グループのメンバにする必要があります。

複数の Unified CM コール処理サブスクライバ ペアが存在する場合、追加の Unified CM グループ（各 Unified CM コール処理サブスクライバ ペアごとに 1 つのグループ）をプロビジョニングして、各 Unified CM グループに、その特定のペアで実行する 2 つの Unified CM インスタンスを追加する必要があります。

最初のペアに ucm1a.ent-pa.com および ucm1b.ent-pa.com という名前の 2 つの Unified CM コール処理サブスクライバがあり、2 番目のペアに ucm2a.ent-pa.com および ucm2b.ent-pa.com という名前の 2 つの Unified CM コール処理サブスクライバがあり、それぞれのペアで ucm1a、ucm2a がプライマリ Unified CM コール処理サブスクライバとなっている Unified CM クラスタの場合、表 2-48 にリストされているように Unified CM グループをプロビジョニングします。

表 2-48　　Unified CM グループ定義の例

Unified CM グループ	Unified CM グループ メンバ
CM_1	CM_ucm1a.ent-pa.com CM_ucm1b.ent-pa.com
CM_2	CM_ucm2a.ent-pa.com CM_ucm2b.ent-pa.com

Unified CM グループ間ですべての登録のバランスを取る必要があります。それには、デバイス プールの項で説明しているデバイス プール設定を使用して、デバイスを Unified CM グループに割り当てます。

電話用 NTP

必要に応じて、SIP を実行している電話が NTP サーバから日時を取得するように、[Cisco Unified CMの管理（Cisco Unified Communications Manager Administration）] で電話用 Network Time Protocol（NTP）を設定することができます。すべての NTP サーバが応答しない場合、SIP を実行している電話は、REGISTER メッセージに対する 200 OK 応答の日付ヘッダーを日時に使用します。

電話用 NTP を Cisco Unified CM の管理に追加した後は、日付/時刻グループにその電話用 NTP を追加する必要があります。

電話用 NTP を定義するには、使用する予定の NTP サーバの IP アドレスを取得し、表 2-49 に従って設定を行います。

表 2-49　電話用 NTP の設定

設定	例	コメント
[IPアドレス（IP Address）]	66.228.35.252	使用する NTP サーバの IP アドレス
[説明（Description）]	0.pool.ntp.org	入力した IP アドレスのホスト名を参照する必要があります。
[モード（Mode）]	[ユニキャスト（Unicast）]	ユニキャストを設定すると、デバイスはリストされたサーバからの NTP 応答のみを使用するように制限されます。

冗長性をもたらすためには、複数の電話用 NTP をプロビジョニングする必要があります。

日付および時刻グループ

日付および時刻グループを使用して、Unified CM に登録する一連のデバイスに使用するタイム ゾーンおよび日付と時刻の形式を定義できます。日付および時刻グループはデバイス プールに設定し、デバイス プールは電話ページで指定します。デバイス プールの詳細については、デバイス プールのセクションを参照してください。

SIP 電話で NTP サーバから日付と時間を取得したい場合は、電話用 NTP の優先順位を設定している日時グループで、電話を接続する最初のサーバを最も高い優先順位にします。

エンドポイントを展開するそれぞれのタイム ゾーンに対して、表 2-50 に示すように 1 つの日時グループを作成します。

表 2-50　日時グループの定義例

日時グループ	タイム ゾーン
RCD_Time	America/North_Dakota/New_Salem
RTP_Time	America/New_York
SJC_Time	America/Los_Angeles

メディア リソース

メディア リソースとは、ソフトウェア ベースまたはハードウェア ベースのエンティティであり、接続中のデータ ストリームに対してメディア処理を行うものです。メディア処理機能には、複数のストリームを混合して 1 つの出力ストリームを作成する機能（会議）、ある接続から別の接続にストリームを渡す機能（メディア ターミネーション ポイント）、ある圧縮タイプから別の圧縮タイプにデータ ストリームを変換する機能（トランスコーディング）、保留中の発信者への音楽のストリーミング（保留音）、エコー キャンセレーション、シグナリング、TDM 回線からの音声インターフェイス（コーディング/デコーディング）、ストリームのパケット化、オーディオのストリーミング（Annunciator）などが含まれます。ソフトウェアベースのリソースは、Cisco Unified CM IP Voice Media Streaming アプリケーションによって提供されます。

メディア リソース マネージャ

Unified CM のソフトウェア コンポーネントであるメディア リソース マネージャ（MRM）は、メディア リソースの割り当ておよびメディア パスの挿入が必要であるかどうかを判別します。MRM は、メディア リソースのタイプを判別および特定すると、当該デバイスに関連付けられているメディア リソース グループ リスト（MRGL）およびメディア リソース グループ（MRG）の構成の設定値に応じて、使用可能なリソース全体を検索します。MRGL および MRG は、割り当ての目的のためにメディア リソースの関連グループをまとめて保持している構成体です。

メディア リソースの選択とデフォルト MRG の回避

メディア リソース グループ（MRG）とメディア リソース グループ リスト（MRGL）は、リソースの割り当て方法を制御する方式を提供するもので、リソースに対するアクセス権、リソースの場所、特定のアプリケーションのリソース タイプが含まれます。MRG の使用により、類似の特性を持つメディア リソースがまとめてグループ化されます。MRGL は、セッションのために必要なメディア リソースを選択するときに考慮される MRG のセットを定義します。メディア リソース マネージャが設定されている MRGL を検索しても必要なリソースが見つからない場合は、すべてのメディア リソースがリストの MRG のメンバーであると見なして、メディア リソース マネージャがデフォルトのメディア リソース グループでメディア リソースをチェックします。特定の MRG のメンバーであることが明示的に設定されている場合を除き、デフォルトではすべてのメディア リソースはこのデフォルトの MRG のメンバーです。

この設計では、メディア リソース選択のトラブルシューティングがより複雑になってしまうため、デフォルトの MRG は使用されません。デフォルトの MRG が確実に空になるようにするには、すべてのメディア リソースを少なくとも 1 つの MRG に割り当てる必要があります。

Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアベースの次のメディア リソースを提供します。

- 会議ブリッジ
- 保留音（MoH）
- アナンシエータ
- メディア ターミネーション ポイント（MTP）

Unified CM クラスタのノードで IP Voice Media Streaming Application が アクティブになると、上記ースの 1 つが自動的に設定されます。サービスのアクティブ化についての推奨事項は、表 2-5 を参照してください。

この設計では、ユニキャスト MoH のみが使用され、Unified CM クラスタのサブスクライバ ノード上で稼働している Cisco IP Voice Media Streaming Application からメディアが流されます。

アナンシエータは Cisco IP Voice Media Streaming Application のソフトウェア機能で、これを使用すると、音声メッセージや各種コール プログレス トーンをシステムからユーザに流すことができます。

Unified CM 上で実行されている Cisco IP Voice Media Streaming Application によって作成されたすべての MOH およびアナンシエータ メディア リソースは、以下のタスクを実行することにより 1 つの MRG に組み込まれます。

- Software という名前の MRG を作成する。
- Cisco IP Voice Media Streaming Application で作成したすべてのアナンシエータ リソースを MRG Software に割り当てる。

- Cisco IP Voice Media Streaming Application で作成したすべての MoH リソースを MRG Software に割り当てる。

Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースの会議およびメディア ターミネーション ポイントは、この設計では使用されません。これらのものを無効にするには、次のタスクを実行します。

- Unused という名前の MRG を作成する。
- Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースの会議ブリッジを MRG Unused に割り当てる。
- Cisco IP Voice Media Streaming Application で作成されたソフトウェアベースのメディア ターミネーション ポイントを MRG Unused に割り当てる。

このようにすると、これらのリソースはデフォルトの MRG に属さないため、メディア リソース マネージャのメディア リソース選択プロセスでは考慮されなくなります。

MRG および MRGL の定義

プロビジョニングされた MRGL の数を最小に保持しておくことは重要なポイントです。必要な MRGL の数に影響を与える要因には、次のものがあります。

- サイトの特異性

  サイト固有のメディア リソースが存在する場合は、それらのリソースに対してサイト固有の MRG を設定する必要があります。また一般的には、サイト固有のメディア リソースの選択（通常はローカル）を可能にするには、サイト固有の MRGL も必要になります。

- 同じクラスにおける異なるタイプのメディア リソース

  Unified CM は音声のみの会議リソースと、音声/ビデオの会議リソースを区別しません。音声のみと音声/ビデオの両方の会議メディア リソースがプロビジョニングされている場合、これらのリソースに対して異なるアクセス ポリシーを設定できるようにするには、メディア リソースのタイプごとに MRG（および MRGL）が必要になります。会議リソースの詳細については、会議の章を参照してください。

サイト固有のメディア リソースがなく、メディア リソースのタイプを区別する必要がない場合は、Standard という名前の MRGL を少なくとも 1 つ設定する必要があります。

サイトの特異性およびメディア リソース タイプのプロビジョニングに基づいて必要なそれぞれの MRGL に対して、次のタスクを実行して MRGL を作成します。

- サイトの特異性、および MRGL のメディア リソース タイプを反映するように、MRGL に名前を付けます。
- MRGL に対して適切な MRG を選択します。MoH およびアナンシエータに対するアクセスが保証されるよう、Software MRG は必ず含めるようにします。

表 2-51 は、音声会議とビデオ会議について処理が異なる MRGL の定義例を示しています。MRGL Video ではビデオ会議リソースへアクセスすることができますが、MRGL Audio は、音声会議メディア リソースへのアクセスのみが必要なデバイスへ割り当てる必要があります。

表 2-51　音声会議とビデオ会議の MRGL の定義例

MRGL 名	MRG	コメント
[音声（Audio）]	[音声（Audio）] [ソフトウェア（Software）]	MRG Audio の音声会議メディア リソースへのアクセス権を持っている MRGL。 MRG Software は MoH およびアナンシエータへのアクセスを提供するために追加されました。
[ビデオ（Video）]	[ビデオ（Video）] [ソフトウェア（Software）]	MRG Video のビデオ会議メディア リソースへのアクセス権を持っている MRGL。 MRG Software は MoH およびアナンシエータへのアクセスを提供するために追加されました。

デバイス プール

デバイス プールはデバイスの共通の特性セットを定義します。デバイス プールで定義されている特性には、表 2-52 に示されている設定が含まれています。

表 2-52　デバイス プールの設定

設定	説明
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	Unified CM グループは、Unified CM の呼処理サブスクライバのペア間で登録を均等に分配する必要があります（Cisco Unified CM グループ設定のセクションを参照してください）。デバイス プール上にプロビジョニングされている Unified CM グループは Unified CM の呼処理サブスクライバを決定します。特定のデバイス プールに関連付けられているデバイスは、このサブスクライバに対して登録を試行します。
[ローカルルートグループ（Local Route Groups）]	コール タイプ固有の発信ゲートウェイを選択するためのローカル ルート グループのセクションに説明されているように、LRG に基づいてコール タイプ特有の出口ゲートウェイを選択できるように、複数の LRG が定義されています。定義されている各 LRG 名では、LRG 名に対して選択されたルート グループによって、選択されたタイプのコールについてどのデバイスが考慮されるかが定義されます（着信番号と特定の LRG を参照しているルート リストへのポインティングについてのルート パターン マッチングによって定義されます）。ルート リストに有効な PSTN リソースが含まれていないために通話が失敗することを回避するためには、定義されているすべての LRG 名に対してルート グループを設定することが重要です。
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]	
[日時グループ（Date/Time Group）]	日付と時間の形式、および電話用 NTP を定義します。電話用 NTPのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	デバイスのグループで使用できるメディア リソースを定義する MRGL。MRG および MRGL の定義のセクションを参照してください。
[デバイスモビリティ関連情報（Device Mobility Related Information）]	
[AARコーリングサーチスペース（AAR Calling Search Space）]	PSTN の他の通知先へコールをルートするために使用する CSS。このドキュメントのダイヤル プラン設計では、どのような場合でも同じ AAR CSS（PSTNReroute）を使用することができます（自動代替ルーティングのセクションを参照してください）。
[AARグループ（AAR Group）]	AAR を有効にするには、AAR グループを定義する必要があります。+E.164 の電話番号を使用すると、1 つの AAR グループ Default を使用して AAR を展開することができます（自動代替ルーティングのセクションを参照してください）。

表 2-52　デバイス プールの設定（続き）

設定	説明
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	この CSS は、影響を受けるデバイスの方向へ送信される発呼側情報に適用される、発呼側のトランスフォーメーションを定義します。 ゲートウェイの場合、この CSS は、ゲートウェイの設定ページの [アウトバウンドコール（Outbound Calls）] セクションで定義された発呼側トランスフォーメーション CSS に関連付けられています。 電話の場合、この CSS は、電話の設定ページの [リモート番号（Remote Number）] セクションで定義された発呼側トランスフォーメーション CSS に関連付けられています。
[着信側トランスフォーメーションCSS（Called Party Transformation CSS）]	この CSS は、影響を受けるデバイスの方向へ送信される着信側情報に適用される、着信側のトランスフォーメーションを定義します。 ゲートウェイの場合、この CSS は、ゲートウェイの設定ページの [アウトバウンドコール（Outbound Calls）] セクションで定義された着信側トランスフォーメーション CSS に関連付けられています。 電話の場合、この CSS は電話の設定ページに相当する機能がなく、電話で使用されるデバイス プール上で設定しても何も影響を与えません。
[コールルーティング情報（Call Routing Information）]	この設定により、着信の発呼側および着呼側の番号タイプごとのトランスフォーメーションを、ゲートウェイ上の着信コールに適用するように定義できます。ゲートウェイ固有の個別の設定が必要な場合は、同じ設定をゲートウェイの設定ページで行うこともできます。

デバイス プールのその他のレベルの設定はすべて、この設計では使用されません。

デバイスのグループに対して、表 2-52 に記載されている設定オプションで同じ設定を適用する必要がある場合は、これらの設定を持つデバイス プールを作成し、このデバイス プールにすべてのデバイスを割り当てることを推奨しています。すべてのデバイスに対して 1 つの設定を変更する必要がある場合は、デバイス プールのレベル設定を使用して、すべてのデバイスに対してその部分だけを変更することができます。

デバイス プールの数を最小にするには、複数のデバイスで同じ特性を共有している場合のみデバイス プールを作成します。次に、同じサイト内の電話の例を示します。表 2-53 は、RTP サイト内でビデオ会議機能を使用している電話に対するデバイス プールの設定例です。

表 2-53　RTP サイト内でビデオ会議機能を使用している電話のデバイス プール設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[RTPPhoneVideo]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。この場合はこのデバイス プールを、ビデオ会議機能を使用している RTP サイト内の電話に対して使用します。
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	[CM_1]	

表 2-53　RTP サイト内でビデオ会議機能を使用している電話のデバイス プール設定（続き）

設定	値	コメント
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	すべてのルート リストは最後のオプションとして [標準ローカルルートグループ（Standard Local Route Group）] を使用します。[標準ローカルルートグループ（Standard Local Route Group）] は必ずローカル PSTN ゲートウェイのルート グループに設定します。
[LRG_PSTN_1]	[RTP_PSTN]	PSTN コールの最初のオプションは、ローカル RTP ゲートウェイを使用することです。
[LRG_PSTN_2]	[SJC_PSTN]	フォールバックとして HQ ゲートウェイを使用します。
[LRG_VIDEO_1]	[SJC_VIDEO]	サイト固有のビデオゲートウェイはありません。サイト SJC のビデオ ゲートウェイを使用します。
[LRG_VIDEO_2]	<なし>	
[LRG_EMERGENCY_1]	<なし>	設定なし：[標準ローカルルートグループ（Standard Local Route Group）] にフォールバックします。
[LRG_EMERGENCY_2]	<なし>	設定なし：[標準ローカルルートグループ（Standard Local Route Group）] にフォールバックします。
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	[ビデオ（Video）]	ビデオ会議メディア リソースへのアクセスを提供します（表 2-51 を参照）。
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべてのデバイスおよびデバイス プールで同じです。
[AARグループ（AAR Group）]	[デフォルト（Default）]	すべてのデバイスおよびデバイス プールで同じです。
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	[RTPPhLocalize]	サイト固有の発呼側トランスフォーメーション（表 2-38 および表 2-39 を参照）。
[着信側トランスフォーメーションCSS（Called Party Transformation CSS）]	<なし>	電話には適用されません。

表 2-53 は、実際のサイト固有の PSTN ゲートウェイがどのように LRG 名に割り当てられて、異なるサイトの電話に関して、サイト固有の出口ゲートウェイの選択を実現しているかを示しています。

図 2-8 は、サイト RTP および SJC の電話のデバイス プールで、同じ LRG 名（LRG_PSTN_1）に対して異なる LRG を選択することにより、サイト RTP および SJC で同じルート パターンおよびルート リストが使用されている場合でも、それぞれの電話からの PSTN コールを、異なるゲートウェイを介してどのように PSTN へストリームするかを示しています。

図 2-8　　サイト固有の出力ゲートウェイの選択

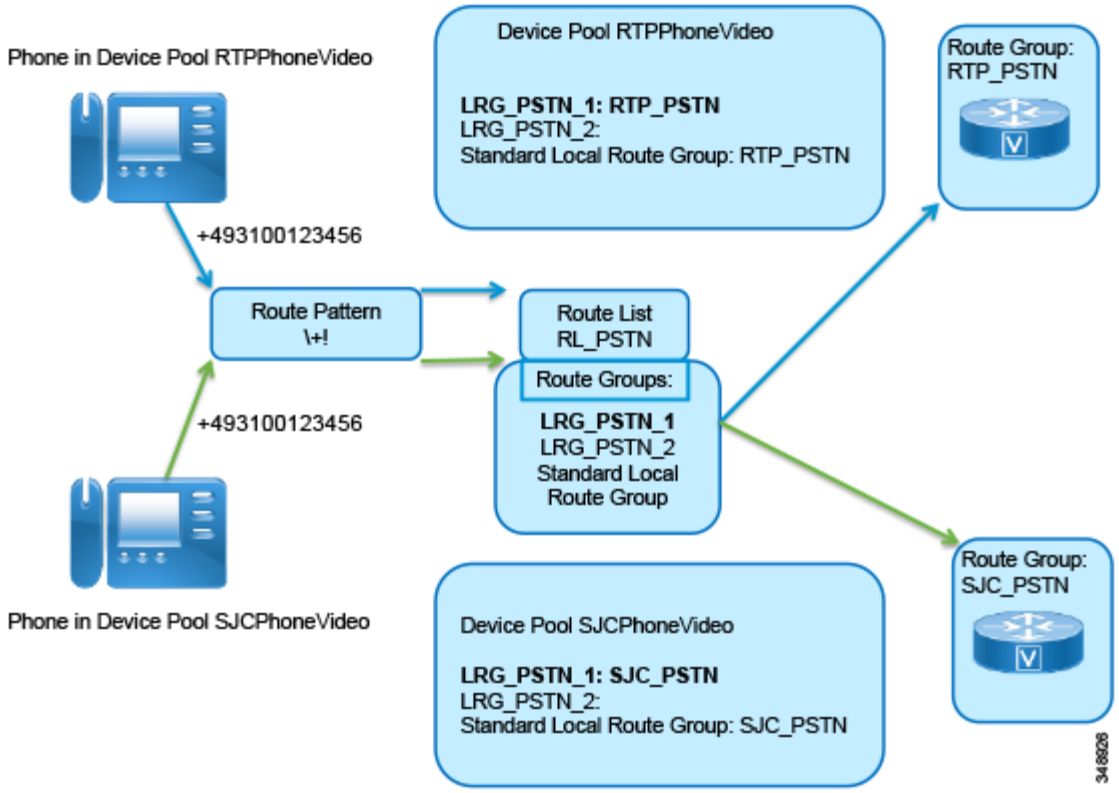


表 2-53 の例と同じスキーマで考えると、1 つのサイトについて 2 つのデバイス プールをプロビジョニングして、ビデオ会議の機能を備えたデバイスと、備えていないデバイスを区別できるようにする必要があります。ビデオ会議機能が例外になっている場合は、デバイス設定で MRGL を Audio（音声）に設定して、1 つのサイトにつき 1 つのデバイス プールのみを使用し、ビデオ対応の少数のデバイスで MRGL を Video（ビデオ）に設定するように決定できます。

表 2-54 は、特定のサイトのゲートウェイで使用されるデバイス プールの設定についてまとめています。ここでは、例としてサイト RTP を使用します。

表 2-54　　サイト RTP の PSTN ゲートウェイに関するデバイス プールの設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[RTP_PSTN]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。この場合は、このデバイス プールをサイト RTP の PSTN ゲートウェイ用に使用します。
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	[CM_1]	

表 2-54　サイト RTP の PSTN ゲートウェイに関するデバイス プールの設定（続き）

設定	値	コメント
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	実際には、PSTN トランクで PSTN リソースを必要とするコール フローはありません。ルート グループのセクションの設定順序の注意についても参照してください。デバイス プールを作成する時点では、必要なルート グループはまだ存在していません。したがって、デバイス プールを設定し、LRG マッピングを <なし（None）> に設定しておく必要があります。SIP トランクとルート グループが設定できたら、戻って LRG マッピングを設定することができます。
[LRG_PSTN_1]	<なし>	
[LRG_PSTN_2]	<なし>	
[LRG_VIDEO_1]	<なし>	
[LRG_VIDEO_2]	<なし>	
[LRG_EMERGENCY_1]	<なし>	
[LRG_EMERGENCY_2]	<なし>	
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	[音声（Audio）]	PSTN から着信するコールは、ビデオ会議リソースへアクセスする必要はありません。
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	実際には PSTN トランクではほとんど必要ではありませんが、すべてのデバイスおよびデバイス プールで同じにします。
[AARグループ（AAR Group）]	[デフォルト（Default）]	実際には PSTN トランクではほとんど必要ではありませんが、すべてのデバイスおよびデバイス プールで同じにします。
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	[RTPGWLocalizeCn]	正当な発呼側情報のみが確実に送信されるようにするためのサイト固有の発呼側トランスフォーメーション（RTP DID の範囲外の番号はすべてマスクされます）。また、番号の文字列が ISDN ゲートウェイに適した形式に設定されます（表 2-35を参照してください）。
[着信側トランスフォーメーションCSS（Called Party Transformation CSS）]	[USGWLocalizeCd]	表 2-34を参照してください。このトランスフォーメーションにより、着呼側の番号が、+E.164 から、プラン **unknown** およびタイプ **unknown** として送信できるような形式に変換されることが保証されます。
[コールルーティング情報（Call Routing Information）]		
[着信の発呼側設定（Incoming Calling Party Settings）]	ここでは何も設定されません。ISDN の番号形式から +E.164 へのトランスフォーメーションは、ゲートウェイ上で Cisco IOS の音声変換ルールを使用して行われることを前提としています（インバウンド コール：ISDN ゲートウェイでの着信者番号および発信者番号のトランスフォーメーションのセクションを参照してください）。	
[着信の着呼側設定（Incoming Called Party Settings）]		

表 2-55 は、他の Unified CM クラスタおよびアプリケーション サーバへの、SIP トランクに関するデバイス プールの設定についてまとめています。他の Unified CM クラスタへの SIP トランクでは、発呼側および着呼側の情報について変換は必要ありません。着呼側の番号は、ダイヤル プランでプロビジョニングされているダイヤル正規化変換パターンによってすでに +E.164 にグローバル化されているため、およびプロビジョニングされているダイヤル プランに基づいた Unified CM 内部の発呼側の情報は +E.164 または ESN であり、どちらの形式もネット上のクラスタ間コールの状態で有効になるためです。

表 2-55　セントラル トランクおよびアプリケーションに関するデバイス プールの設定

設定	値	コメント
[デバイスプール名（Device Pool Name）]	[Trunks_and_Apps]	名前は、このデバイス プールを使用するデバイスを一意に識別できるようなものにします（タイプや詳細な分類など）。
[Cisco Unified CMグループ（Cisco Unified Communications Manager Group）]	[CM_1]	
[ローカルルートグループの設定（Local Route Group Settings）]		
[標準ローカル ルート グループ（Standard Local Route Group）]	[RTP_PSTN]	実際にはトランクで PSTN へのアクセスは必要ありませんが、アプリケーションでは PSTN へのアクセスが必要になる場合があります。そのため、1 つのサイトの PSTN リソースは、[標準ローカルルートグループ（Standard Local Route Group）] の設定を介して選択します。他のサイトの PSTN リソースはフェールオーバーとして使用できます。
[LRG_PSTN_1]	[RTP_PSTN]	
[LRG_PSTN_2]	[SJC_PSTN]	
[LRG_VIDEO_1]	<なし>	
[LRG_VIDEO_2]	<なし>	
[LRG_EMERGENCY_1]	<なし>	
[LRG_EMERGENCY_2]	<なし>	
[ローミングに合わせて変化する設定（Roaming Sensitive Settings）]		
[日時グループ（Date/Time Group）]	[RTP_Time]	日付および時刻グループのセクションを参照してください。
[メディアリソースグループリスト（Media Resource Group List）]	[ビデオ（Video）]	クラスタ間コールでは、ビデオ メディア リソースが必要になる可能性があります。
[デバイスモビリティ関連情報（Device Mobility Related Information）]		
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべてのデバイスおよびデバイス プールで同じです。
[AARグループ（AAR Group）]	[デフォルト（Default）]	すべてのデバイスおよびデバイス プールで同じです。
[発呼側トランスフォーメーションCSS（Calling Party Transformation CSS）]	<なし>	クラスタ間のトランクと、アプリケーション サーバに対するトランクで変換はありません。

表 2-55　セントラル トランクおよびアプリケーションに関するデバイス プールの設定（続き）

設定	値	コメント
[着信側トランスフォーメーションCSS（Called Party Transformation CSS）]	[USGWLocalizeCd]	クラスタ間のトランクと、アプリケーション サーバに対するトランクで変換はありません。
[コールルーティング情報（Call Routing Information）]		
[着信の発呼側設定（Incoming Calling Party Settings）]	設定はありません。発呼側および着呼側の番号はすでに正規化されていると仮定しています。	
[着信の着呼側設定（Incoming Called Party Settings）]		

SIP トランク

コール制御、アプリケーション、会議リソースなどの他のエンティティへのすべての接続は SIP トランクを使用します。

SIP プロファイル

SIP プロファイルは、SIP トランクおよび SIP エンドポイントに関連付けられている一連の SIP 属性で構成されています。SIP プロファイルの数を最小に保持するには、次のルールに従います。

- 最初にデフォルトのプロファイルを考慮します。
- 次に、すでに定義されているデフォルト以外のプロファイルを考慮します。
- デフォルトのプロファイルが一致しなかった場合のみ、新しい SIP プロファイルを作成します。
- トランクごとにプロファイルを定義しないようにします。

表 2-56 は、他の Unified CM クラスタまたは SIP ゲートウェイへのすべての SIP IP 電話および SIP トランクで使用する SIP プロファイルについての設定を示しています。

表 2-56　SIP 電話および標準トランク向けの SIP プロファイル

設定	値	コメント
[標準 SIP プロファイルのコピー（Copy of Standard SIP Profile）]		
[名前（Name）]	[FQDN]	
[SIP要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）]	オン	Unified CM サーバの IP アドレスが、Unified CM によって送信される SIP の発呼側情報に表示されないようにします。
[音声コールとビデオコールに対する早期オファーサポート（Early Offer support for voice and video calls）]	[ベストエフォート（MTPの挿入なし）]	これは、すべての Unified CM トランクに対して推奨される設定です。ベスト エフォート早期オファー トランクは早期オファーを作成するために MTP を使用することはありませんが、発信側デバイスによっては早期オファーまたは遅延オファーのいずれかを使用して、送信 SIP トランクを開始することができます。この設計では、発信コールは常に早期オファーを使用します。

表 2-56　SIP 電話および標準トランク向けの SIP プロファイル（続き）

設定	値	コメント
[サービスタイプ"なし（デフォルト）"のトランクの接続先ステータスをモニタするためにOPTIONS Pingを有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"）]	オン	SIP トランク ピアの到達性の監視を可能にします（SIP トランクのみに適用されます）。
[インサービスおよび一部インサービスのトランクのPing間隔（秒）（Ping Interval for In-service and Partially In-service Trunks (seconds)）]	[10]	再試行回数 6 回で 10 秒ごとに ping を実行し、SIP トランクが使用不可能な状態が 1 分以内に確実に検出されるようにします。
[アウトオブサービスのトランクのPing間隔（秒）（Ping Interval for Out-of-service Trunks (seconds)）]	[60]	トランクが停止または使用不可の場合は、ここで設定した秒数を経過するまでピアへの到達を試行する必要はありません。
[Ping再試行タイマー（ミリ秒）（Ping Retry Timer（milliseconds））]	[500]	
[Ping再試行数（Ping Retry Count）]	[6]	

SIP トランク セキュリティ プロファイル

Cisco CallManager Administration は SIP トランク セキュリティ関係の設定（デバイス セキュリティ モード、ダイジェスト認証、着信/発信転送タイプの設定など）をグループ化して、[SIPトランクの設定（SIP Trunk Configuration）] ウィンドウでプロファイルを選択するときに、設定したすべての内容を 1 つの SIP トランクに適用することができます。

表 2-57 は、SIP トランクのセキュリティ プロファイルである非セキュア SIP トランク プロファイル（Non Secure SIP Trunk Profile）で生成された、システム上のデフォルト設定について示しています。この SIP トランク セキュリティ プロファイルは、ISDN PSTN ゲートウェイ向けの SIP トランクなどで使用されます。

表 2-57　SIP トランク セキュリティ プロファイル（非セキュア SIP トランク プロファイル）の設定

設定	値
[名前（Name）]	[非セキュアSIPトランクプロファイル（Non Secure SIP Trunk Profile）]
[デバイスセキュリティモード（Device Security Mode）]	[非セキュア（Non Secure）]
[着信転送タイプ（Incoming Transport Type）]	[TCP+UDP]
[発信転送タイプ（Outgoing Transport Type）]	[TCP]
[ダイジェスト認証を有効化（Enable Digest Authentication）]	オフ
[着信ポート（Incoming Port）]	[5060]
[アプリケーションレベル認証を有効化（Enable Application Level Authorization）]	オフ

表 2-57　SIP トランク セキュリティ プロファイル（非セキュア SIP トランク プロファイル）の設定（続き）

設定	値
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	オフ
[Out-of-Dialog REFERの許可（Accept Out-of-Dialog REFER）]	オフ
[Unsolicited NOTIFYの許可（Accept unsolicited notification）]	オフ
[Replacesヘッダーの許可（Accept replaces header）]	オフ
[セキュリティステータスの送信（Transmit security status）]	オフ
[Chargingヘッダーの許可（Allow charging header）]	オフ
[SIP V.150アウトバウンドSDPオファーのフィルタリング（SIP V.150 Outbound SDP Offer Filtering）]	[デフォルトのフィルタを使用（Use Default Filter）]

表 2-58 は、IM and Presence ノード向けの SIP トランクで使用される SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の設定について示しています。これは、表 2-57 のデフォルトの設定とは異なります。

表 2-58　IM and Presence トランク向けの SIP トランク セキュリティ プロファイル

設定	値	コメント
[名前（Name）]	[IM and Presence]	SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の用途を説明するためのわかりやすい名前。
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	オン	
[Out-of-Dialog REFERの許可（Accept Out-of-Dialog REFER）]	オン	
[Unsolicited NOTIFYの許可（Accept unsolicited notification）]	オン	
[Replacesヘッダーの許可（Accept replaces header）]	オン	

表 2-59 は、他の Unified CM クラスタへのクラスタ間トランクで使用する SIP トランク セキュリティ プロファイルの設定について示しています。これらのトランクでは、プレゼンスの SUBSCRIBE を許可して、クラスタ間のビジー ランプ フィールド（BLF）プレゼンスを有効にするとよいでしょう。

表 2-59　クラスタ間トランクの SIP トランク セキュリティ プロファイル

設定	値	コメント
[名前（Name）]	[ICT]	SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）の用途を説明するための名前。
[プレゼンスのSUBSCRIBEの許可（Accept Presence Subscription）]	オン	
[セキュリティステータスの送信（Transmit security status）]	オン	

SIP トランク接続

SIP トランクは、Unified CM のクラスタ間、および Unified CM と（ゲートウェイ、アプリケーション、メディア リソースなどの）他のシステム間での接続を設定する場合に推奨される方法です。接続するシステムのタイプによって、各 SIP トランクで設定されるパラメータは少し異なります。表 2-60 は、サイト RTP における、PSTN ゲートウェイ向けの SIP トランクについての設定をまとめて示しています。

表 2-60　サイト RTP での ISDN ゲートウェイ向けトランクの SIP トランク設定

設定	値	コメント
[名前（Name）]	[ST_RTP_PSTN_1]	同じテーブルに内部で格納されている他のデバイスとの名前のコリジョン（衝突）を回避するためのプレフィックス ST_。名前の残りの部分はゲートウェイの場所を特定するもので、複数のゲートウェイに対して数字を割り当てることができます。
[説明（Description）]		わかりやすい説明
[デバイスプール（Device Pool）]	[RTP_PSTN]	すべての RTP PSTN ゲートウェイに対する共通のデバイス プール。すべての RTP ゲートウェイ間でサイト特定の設定を共有できるようにします。
[メディアリソースグループリスト（Media Resource Group List）]	<なし>	デバイス プールで定義されている MRGL を使用します。
[AARグループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[PSTNアクセス（PSTN Access）]	オン	
[すべてのアクティブなUnified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	この設定は、すべての SIP トランクで推奨されます。この設定により、SIP への発信コールで、Unified CM コールを処理するサブスクライバ間でのクラスタ間のシグナリング制御が不要になります。

表 2-60　サイト RTP での ISDN ゲートウェイ向けトランクの SIP トランク設定（続き）

設定	値	コメント
[着信コール（Inbound Calls）]		
[コーリングサーチスペース（Calling Search Space）]	[DN]	着信コールには +E.164 の着呼側の番号が定義されているため、PSTN からコールできるのはローカルな通知先のみになります。したがって、ESN 番号およびクラスタ間の通知先へはアクセスする必要はありません。
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	
[アウトバウンドコール（Outbound Calls）]		
[デバイスプールの着信側トランスフォーメーションCSSを使用（Use Device Pool Called Party Transformation CSS）]	オン	
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	オン	
[SIP情報（SIP Information）]		
接続先	[X.X.X.X]	ISDN ゲートウェイの IP アドレス
[SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	[非セキュアSIPトランクプロファイル（Non Secure SIP Trunk Profile）]	デフォルトの SIP トランク セキュリティ プロファイル
[SIPプロファイル（SIP Profile）]	[FQDN]	

ここでは、着信 CSS はローカルな +E.164 の通知先のみにアクセスを提供することがポイントです。これらの通信先には、ボイスメール パイロットや、PSTN から到達可能であることが必要な他のサービスが含まれますが、PSTN のルート パターン、ダイヤル正規化変換パターン、ESN、URI、およびクラスタ間の通知先へのアクセスは必要ありません。

他の Unified CM クラスタへの SIP トランクの設定は、ISDN ゲートウェイへの SIP トランクの設定とは少し異なります。表 2-61 に、これらの設定を要約します。

表 2-61　他の Unified CM クラスタ向けクラスタ間トランクについての SIP トランクの設定

設定	値	コメント
[名前（Name）]	[ST_UCM_EMEA]	同じテーブルに内部で格納されている他のデバイスとの名前のコリジョン（衝突）を回避するためのプレフィックス ST_。名前の残りの部分は、トランクの目的を表します。
[説明（Description）]		わかりやすい説明
[デバイスプール（Device Pool）]	[Trunks_and_Apps]	セントラル トランクに対する共通のデバイス プール（表 2-55 を参照してください）。

表 2-61　他の Unified CM クラスタ向けクラスタ間トランクについての SIP トランクの設定（続き）

設定	値	コメント
[メディアリソースグループリスト（Media Resource Group List）]	<なし>	デバイス プールで定義されている MRGL を使用します。
[AARグループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ
[PSTNアクセス（PSTN Access）]	オフ	
[すべてのアクティブな Unified CMノードで実行（Run on All Active Unified CM Nodes）]	オン	この設定は、すべての SIP トランクで推奨されます。この設定により、SIP への発信コールで、Unified CM コールを処理するサブスクライバ間でのクラスタ間のシグナリング制御が不要になります。
[着信コール（Inbound Calls）]		
[コーリングサーチスペース（Calling Search Space）]	[ICTInbound]	トランク上の着信コールは +E.164、ESN、および URI ダイヤルをサポートしている必要があります。この特別な CSS は、3 つのダイヤリング手順をすべてサポートしていますが、PSTN またはリモートのネット上での通知先へのアクセスは提供していません（特殊な CSSのセクションの表 2-26 を参照してください）。 PSTN へのアクセスが必要なアプリケーションについては、PSTN アクセス ルート パターンを使用してパーティションへアクセスするために、もうひとつの特別なサービス クラス（CSS）が必要になります（PSTN アクセスと緊急コールのルート パターンのセクションの表 2-29 を参照してください）。
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべての場所で同じ CSS
[アウトバウンドコール（Outbound Calls）]		
[デバイスプールの着信側トランスフォーメーションCSSを使用（Use Device Pool Called Party Transformation CSS）]	オン	
[デバイスプールの発呼側トランスフォーメーションCSSを使用（Use Device Pool Calling Party Transformation CSS）]	オン	
[発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみURIおよびDNを配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]	他の Unified CM クラスタ向けのクラスタ間トランクで、数値の ID と URI 情報の ID の 2 つが混在している場合は、リモート クラスタに配信する必要があります。2 つのタイプの ID が存在する場合は、着呼側のエンドポイント機能に基づいて、コールを終了するクラスタが ID 情報のどの部分を最終的な着信側に表示するかを決定することができます。

表 2-61　他の Unified CM クラスタ向けクラスタ間トランクについての SIP トランクの設定（続き）

設定	値	コメント
[SIP情報（SIP Information）]		
[接続先（Destination）]	[X.X.X.X]	リモートの Unified CM クラスタのサブスクライバを処理する、すべての Unified CM コールの IP アドレスがリストされます。発信コールは、定義された通知先の中でランダムに配信されるため、IP アドレスの順序は関連していません。
[SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	[ICT]	表 2-59を参照してください
[SUBSCRIBEコーリングサーチスペース（AAR Calling Search Space）]	[ICTInbound]	+E.164、ESN、および URI のサブスクリプションを許可する必要があります。CSS の定義については、特殊な CSSのセクションを参照してください。
[SIPプロファイル（SIP Profile）]	[FQDN]	表 2-56を参照してください

PSTN ISDN ゲートウェイ向けの SIP トランクとは異なり、+E.164 番号だけでなく他の Unified CM クラスタからの着信コールも ESN と URI へのアクセスが必要です。ただし、ルーティングのループやトランジット ルーティングを回避するために、クラスタ間のトランクはクラスタ間の通知先（パーティション remoteOnNet、表 2-13 を参照）へのアクセス権は持っていません。

IM and Presence ノードへの SIP トランクについては、Unified CM と IM and Presence 間の SIP トランクを設定します。SIP トランクについては、IM and Presence のすべてのノードの通知先 IP アドレスを設定します。IM and Presence サービスに対して自身が設定した SIP トランク セキュリティ プロファイルを選択します。標準の SIP プロファイルも選択します。

ルート グループ

すべての SIP トランクはルート グループに割り当てられます。ルート グループは、トランクと、共通の特性を組み合わせます。表 2-62 は、サイト RTP における PSTN ゲートウェイに対するルート グループの定義を示しています。

表 2-62　RTP PSTN ゲートウェイに対するルート グループ

設定	値	コメント
[ルートグループ名（Route Group Name）]	[RTP_PSTN]	わかりやすい名前
[分配アルゴリズム（Distribution Algorithm）]	[ラウンドロビン（Circular）]	ゲートウェイ全体で確実に負荷を均等化できるようにします。
[ルートグループメンバ（Route Group Members）]	[ST_RTP_PSTN_1] [ST_RTP_PSTN_2] [ST_RTP_PSTN_3]	サイト RRP のすべての SIP ゲートウェイにすべての SIP トランクを追加します。

（注）　ルート グループは、SIP トランクが作成された後でのみ設定することが可能で、SIP トランクは、それぞれのデバイス プールが設定された後でのみ追加することが可能です。これは、PSTN ゲートウェイに対してデバイス プールを作成するときには、ルート グループはまだ存在していないことを意味しています。したがって、設定の順序は次のようになります。

1. デバイス プールで LRG マッピングを定義せずに、PSTN ゲートウェイに対するデバイス プールを設定します。
2. SIP トランクを設定します。
3. ルート グループを作成します。
4. デバイス プールに戻り、（必要に応じて）LRG マッピングを追加します。

他の Unified CM クラスタ向けのクラスタ間トランクでは、1 つのトランクにつき 1 つのルート グループを定義する必要があります。表 2-63 は、リモート Unified CM クラスタ向けのクラスタ間トランクに対するルート グループの例を示しています。

表 2-63　　他の Unified CM クラスタ向けのクラスタ間トランクのルート グループ

設定	値	コメント
[ルートグループ名（Route Group Name）]	[UCM_EMEA]	わかりやすい名前。この場合は、EMEA Unified CM クラスタ向けのクラスタ間トランクのみを保持しているルート グループの名前。
[分配アルゴリズム（Distribution Algorithm）]	[ラウンドロビン（Circular）]	ルート グループ メンバーが 1 つだけ存在する場合は不適切。
[ルートグループメンバ（Route Group Members）]	[ST_UCM_EMEA]	リモート Unified CM クラスタ向けの SIP トランク。

Unified CM にプロビジョニングされているそれぞれの非 PSTN SIP トランクに対しては、簡単な類似のルート グループを作成する必要があります。

特定の非 LRG ルート リスト

ローカル ルート グループを使用するルート リストのセクションでは、ローカル ルート グループのみを使用した PSTN アクセスのルート リストについて概要を説明します。非 PSTN トランクでは、特定のルート リストは、これらの非 PSTN トランクを参照するルート グループを使用して作成する必要があります。1 つのメンバーのみを持つ簡単なルート グループと、メンバーとして 1 つの非 LRG ルート グループのみを持つ簡単なルート リストを定義する理由は、Unified CM のルート パターンはトランクを直接指定しないためです。具体的には、Unified CM でルート パターンが変更されるたびに、ルート パターンが指定しているデバイスがリセットされます。（トランクの代わりに）ルート リストに対してルート パターンを指定すると、ルート パターンの編集によってトランク自身はリセットされずに、ルート リストがリセットされます。このようなトランクの例として、他の Unified CM クラスタおよびアプリケーション向けのトランクが含まれます。

表 2-64 は、他の Unified CM クラスタ向けのクラスタ間トランクの簡単なルート リストを示しています。

表 2-64　他の Unified CM クラスタ向けのクラスタ間トランクのルート リスト

ルート リスト	メンバー	説明
[RL_UCM_EMEA]	[UCM_EMEA]	1 つのメンバーのみ（リモート Unified CM クラスタ向けの実際のトランク）。先頭の RL により、トランクと命名のコリジョンが発生しないことが保証されます。内部ではルート リストはデバイスとして扱われ、ルート リストの名前は SIP トランクなどの名前と同じにすることはできません。

Unified CM にプロビジョニングされているそれぞれの非 PSTN SIP トランクに対しては、簡単な類似のルート リストを作成する必要があります。

エンドポイントのプロビジョニング

新しいエンドポイントをプロビジョニングする場合には、次の最小限のタスクが必要です。

- デバイスの設定
- 回線の設定
- ユーザが制御するデバイスへデバイスを追加する
- プレゼンスに対する回線の関連付けの設定

デバイスの設定

Unified CM に新しいエンドポイントを追加する場合は、このドキュメントで説明している設計では、表 2-65 に要約されている設定が必要です。ここに記載されていない設定はデフォルトのままにしておくか、または、デバイス特有の要件に従って設定する必要があります。

表 2-65　エンドポイントのデバイス設定

設定	値	説明
[デバイス情報（Device Information）]		
[デバイスプール（Device Pool）]	[RTPPhoneVideo]	エンドポイントに対するサイト固有のデバイス プール（表 2-53 を参照してください）。この場合には、ビデオ会議メディア リソースへのアクセス権を持つサイト RTP 内のエンドポイントに対するデバイス プールになります。
[コーリングサーチスペース（Calling Search Space）]	[USEmergency]	多国籍環境でのイマージェンシー ルーティングへのアクセスは、デバイス レベルで実現されます（多国間環境における緊急コールの考慮事項を参照してください）。US などの 1 つの国（ダイヤル ドメイン）をサポートする必要がある場合は、この CSS は <なし（None）> のままにすることもできます。
[AARコーリングサーチスペース（AAR Calling Search Space）]	[PSTNReroute]	すべての場所で同じ（自動代替ルーティングのセクションを参照してください）。
[メディアリソースグループリスト（Media Resource Group List）]	<なし>	デバイス プール レベルの設定を使用します。

表 2-65　エンドポイントのデバイス設定（続き）

設定	値	説明
[AAR_Group]	デフォルト	すべての場所で同じ（自動代替ルーティングのセクションを参照してください）。
[オーナー（Owner）]	「ユーザ」の選択	デバイスが、ユーザが関連付けされていない電話（ロビーにある電話など）である場合は、[匿名（公共/共有スペース）（Anonymous（Public/Shared Space））] を選択し、[オーナーのユーザID（Owner User ID）] は選択しません。
[オーナーのユーザID（Owner User ID）]	この電話の所有者のユーザ ID を選択します。	
[CTIからのデバイスの制御を許可（Allow Control of Device from CTI）]	オン	
[番号表示トランスフォーメーション（Number Presentation Transformation）]		
[この電話からのコールの発信者ID（Caller ID For Calls From This Phone）]	[デバイスプールの発呼側トランスフォーメーションCSSを使用（この電話からのコールの発信者ID）（Use Device Pool Calling Party Transformation CSS）（Caller ID For Calls From This Phone）] を選択します	
[リモート番号（Remote Number）]	[デバイスプールの発呼側トランスフォーメーションCSSを使用（この電話からのコールの発信者ID）（Use Device Pool Calling Party Transformation CSS（Device Mobility Related Information））] を選択します	
[プロトコル固有情報（Protocol Specific Information）]		
[SIPプロファイル（SIP Profile）]	[FQDN]	表 2-56を参照してください

回線の設定

各エンドポイントで、少なくとも最初の回線をプロビジョニングする必要があります。表 2-66 は、このドキュメントに記載されている設計固有の回線設定について説明しています。

表 2-66　回線の設定

設定	値	説明
[電話番号情報（Directory Number Information）]		
[電話番号（Directory Number）]	[\+14085554146]	この DN がプロビジョニングされているユーザの電話番号と一致する、完全な +E.164 の電話番号。先頭の + はスラッシュ（\）でエスケープする必要があります。非 DID がプロビジョニングされている場合、電話番号は（81405001 などのように）ESN に設定されます。
[ルートパターン（Route Pattern）]	[DN]	非 DID がプロビジョニングされている場合、この部分は ESN になります。

表 2-66　回線の設定（続き）

設定	値	説明
[呼び出し表示（Alerting Name）]	[Aristotle Boyle]	この番号に関連付けられているユーザのフルネーム。番号がユーザに関連付けられていない場合は、（Bldg. 31 Lobby などのように）わかりやすい名前をプロビジョニングします。
[CTIからのデバイスの制御を許可（Allow Control of Device from CTI）]	オン	
[電話番号の設定（Directory Number Settings）]		
[コーリングサーチスペース（Calling Search Space）]	[SJCInternational]	この回線からのコールに対する実際のサービス クラスを定義している CSS。CSS はサイトおよびサービス クラス固有のものです（他の CSS についてはサービス クラスとコーリング サーチ スペース（CSS）を参照してください）。
[BLFプレゼンスグループ（BLF Presence Group）]	標準のプレゼンス グループ	すべての回線について同じ
[+E.164代替番号（+E.164 Alternate Number）]		
[番号マスク（Number Mask）]	マスクを空のままにしておく	マスクを空にしておくと、上記で設定された電話番号と同じ +E.164 代替番号が作成されます。非 DID がプロビジョニングされている場合は、非 DID には定義により PSTN アドレスが存在しないため、+E.164 代替番号が追加されます。
[ローカルルートパーティションに追加（Add to Local Route Partition）]	オフ	電話番号にはすでに +E.164 の番号が存在するため、+E.164 代替番号はローカル ルート パーティションには追加されません。
[ILSを介してグローバルにアドバタイズ（Advertise Globally via ILS）]	オフ	+E.164 代替番号は ILS を介してアドバタイズされません。代わりに、各 DID 範囲に対するサマリ ルートがアドバタイズされます（表 2-70 を参照してください）。+E.164 代替番号を作成する唯一の理由は、この +E.164 代替番号を、この電話番号に関連付けられている URI の GDPR PSTN フェールオーバー番号としてアドバタイズできることです。
[エンタープライズ代替番号、+E.164代替番号、およびURIダイヤリングのPSTNフェールオーバー（PSTN Failover for Enterprise Alternate Number, +E.164 Alternate Number, and URI Dialing）]		
[アドバタイズされたフェールオーバー番号（Advertised Failover Number）]	[+E.164番号（Advertised Failover Number）]	+E.164 番号は GDPR PSTN としてアドバタイズされます。非 DID がプロビジョニングされている場合は、<なし（None）> に設定します。
[AAR設定（AAR Settings）]		
[ボイスメール（Voicemail）]	オフ	非 DID がプロビジョニングされている場合は、このオプションをオンにします。
[AAR接続先マスク（AAR Destination Mask）]	+14085554XXX	この DID 範囲マスクにより、AAR に対する代わりの PSTN 通知先が電話番号と同じであることが保証されます。非 DID がプロビジョニングされている場合は、このマスクを空のままにします。
[AARグループ（AAR Group）]	[デフォルト（Default）]	すべての場所で同じ

表 2-66　回線の設定（続き）

設定	値	説明
[コール転送とコールピックアップの設定（Call Forward and Call Pickup Settings）]		
[コーリングサーチスペースのアクティベーションポリシー（Calling Search Space Activation Policy）]	[システムデフォルトの使用（Use System Default）]	
[不在転送（Forward All）]	[ボイスメール（Voicemail）] をオフに設定する [コーリングサーチスペース（Calling Search Space）]：SJCInternational	より限定的な CSS に設定される可能性があります。
[未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）] 以外のすべての転送の設定	[ボイスメール（Voicemail）] をオフに設定する [コーリングサーチスペース（Calling Search Space）]：SJCInternational	より限定的な CSS に設定される可能性があります。
[未登録内線の不在転送（Forward Unregistered Internal）] および [未登録外線の不在転送（Forward Unregistered External）]	[通知先（Destination）]：+14085554146 [コーリングサーチスペース（Calling Search Space）]：PSTNReroute	エンドポイントが未登録の場合、未登録転送は PSTN を介して代替ルートを実装します。これは、PSTN を介して代替ルートが確立できるローカル PSTN へのアクセスを持つ、リモート サイトのエンドポイントでのみ有効です。 非 DID がプロビジョニングされている場合、または PSTN がリルートする DN が有効ではない場合は、[ボイスメール（Voicemail）] をオンにして、CSS を SJCInternational、またはボイスメール パイロットに到達可能な他の CSS に設定します。
[デバイスの回線1（Line 1 on Device）]		
[表示（発信者ID）（Display (Caller ID)）]	[Aristotle Boyle]	この番号に関連付けられているユーザのフルネーム。番号がユーザに関連付けられていない場合は、（Bldg. 31 Lobby などのように）わかりやすい名前をプロビジョニングします。
[回線のテキストラベル（Line Text Label）]	4146	電話の回線ボタンの隣に、電話番号の最後の 4 桁が表示されるようになります。この設定は、回線テキスト ラベルをサポートしているデバイス上の回線にのみ存在します。
[外線電話番号マスク（External Phone Number Mask）]	+14085554XXX	外線電話番号のマスクは、プロビジョニングされているダイヤル プランの中では参照されず、任意に設定することができます。外線電話番号のマスクが、電話表示における最初の回線のテキストを決定する電話の場合は、マスクを、意味のあるラベルを作成するものに設定することができます。

ユーザが制御するデバイスへデバイスを追加する

ユーザに関連付けられているデバイスでは、Unified CM Administration の [デバイス情報（Device Information）] セクションにおいて各ユーザの [エンドユーザの設定（End User Configuration）] でデバイスをプロビジョニングした後で、デバイスがユーザに関連付けられていることを確認します。これを実行するための推奨される方法は、[デバイスの割り当て（Device Association）] を選択し、ユーザの電話番号と一致する電話番号を持つデバイスを検索することです。

プレゼンスに対する回線の関連付けの設定

ユーザのプレゼンス状態を決定するために、プレゼンスに明示的に関連付けられている（DN およびデバイスごとの）ライン アピアランスのみが考慮されます。ユーザの電話番号のすべてのライン アピアランスがプレゼンスに対して考慮されることを確認するには、Unified CM Administration の [デバイス情報（Device Information）] のセクションで各ユーザの [エンドユーザの設定（End User Configuration）] で、[プレゼンスのラインアピアランス関連付け（Line Appearance Association for Presence）] を選択し、すべてのライン アピアランスを関連付けます。

ユーザのプライマリ内線の確認

LDAP から同期されているユーザのディレクトリ URI が電話番号へ反映されていることを確認するには、Unified CM Administration で各ユーザの [エンドユーザの設定（End User Configuration）] の [電話番号の割り当て（Directory Number Associations）] セクションにおいて、[プライマリ内線（Primary Extension）] を選択します。

Jabber プロビジョニング

Service Discovery により、Jabber が自動的に設定を確立することができます。Jabber クライアントは Unified CM User Discovery Service（UDS）を介して自身の設定を取得します。これは推奨される設定で、以前の手動による設定よりも優先されます。

サービスは UC サービスを介して設定されます。サービス プロファイルは、どの UC サービスを使用するかを指定します。各ユーザは、1 つのサービス プロファイルに関連付けられています。

表 2-67 は、Jabber クライアントで使用することができる UC サービスを示しています。これらのサービスは [ユーザ（User）] > [ユーザ設定（User Settings）] > [UCサービス（UC service）] で設定されます。

表 2-67　　UC サービス

UC サービスのタイプ	コメント
[IM and Presence]	各 IM and Presence ノードに対して IM and Presence サービスを作成します。
[ディレクトリ（Directory）]	アクティブなディレクトリ サーバについてそれぞれディレクトリ サービスを作成します。LDAP ディレクトリと統合する場合は、[連絡先の解決にUDSを使用する（Use UDS for Contact Resolution）] を選択しないでください。連絡先の解決に UDS を使用すると、Unified CM のユーザの拡張性が低減します。
[CTI]	CTI Manager サービスを実行している各 Unified CM に対して CTI サービスを作成します。これは、デスク電話の制御モードで使用されます。Unified CM のすべてのコール処理ノードで、CTI の負荷を均衡にします。

表 2-67　UC サービス（続き）

UC サービスのタイプ	コメント
[ボイスメール（Voicemail）]	各 Unity Connection ノードに対してボイスメール サービスを作成します。
[会議（Conferencing）]	Jabber は Cisco WebEx Meetings Server または Cisco WebEx Meeting Center に統合することができます。この設計では、Cisco WebEx Meetings Server との統合を対象としています。

UC サービスをサービス プロファイルに関連付けます。次に、サービス プロファイルを各ユーザに関連付けます。複数の Unified CM 呼処理サブスクライバを備えている展開では、Unified CM のすべての呼処理サブスクライバに対して CTI の負荷を均等に分散させて、CTI の拡張性制限が、CTI Manager サービスを実行している単一の Unified CM の呼処理サブスクライバを超えないようにします。Jabber クライアントを、CTI Manager サービスを実行しているもう 1 つの Unified CM の呼処理に関連付けるには、関連する CTI UC サービスの設定を使用してもう 1 つのサービス プロファイルを設定します。

（Cisco Collaboration Edge を使用せずに）内部のエンタープライズ ネットワークに接続しているユーザに対しては、UDS または LDAP を介してディレクトリ検索 Contact Sources を提供することができます。LDAP では、Windows デスクトップ向けの拡張ディレクトリ統合（EDI）と、Mac、iOS、および Android 向けの基本ディレクトリ統合（BDI）を使用できます。BDI と EDI は共存することが可能です。Contact Source またはディレクトリは、jabber-config.xml ファイルまたは UC サービスを介して設定することができます（UC サービスが優先されます）。この場合には、Unified CM TFTP サーバへアップロードされている jabber-config.xml ファイルを設定することが推奨されます。jabber-config.xml ファイルは、Jabber クライアント用の URI ダイヤルを有効にする場合にも使用します。例 2-5 は、jabber-config.xml ファイルによる Jabber クライアント用の URI ダイヤルの有効化について示しています。これは最小限の推奨事項です。これ以外の設定オプションを追加することもできます。

例 2-5　jabber-config.xml ファイルによる URI ダイヤルの有効化

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
    <Policies>
        <EnableSIPURIDialling>true</EnableSIPURIDialling>
    </Policies>
</config>
```

詳細については、次のマニュアルを参照してください。

- *Configuration and Administration of IM and Presence on Cisco Unified Communications Manager*

  http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html

- *Deployment and Installation Guide for Cisco Jabber*

  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/10_5/CJAB_BK_D6497E98_00_deployment-installation-guide-ciscojabber.html

マルチクラスタ展開向けの ILS 設定

複数のクラスタ上にクラスタ間検索サービス（ILS）を設定した場合、ILS は、ILS ネットワーク内のリモート クラスタの現在のステータスで Unified CM を更新します。

ILS のクラスタ検出サービスを使用すると、管理者が各クラスタ間の接続を手動で設定しなくても Unified CM はリモート クラスタの詳細を知ることができます。

ILS クラスタ検出サービスにより、マルチクラスタ環境の Jabber クライアントに対して UDS ベースのサービス検出を実現できます。また、ILS はグローバル ダイヤル プラン レプリケーションのベースとなるもので、これにより Unified CM クラスタ間の英数字 URI と数字の通知先の両方について、到達性の情報のやりとりを可能にします。

複数の Unified CM クラスタの ILS ネットワークを作成するには、次のタスクを実行します。

- ネットワーク内の各 Unified CM クラスタに対して一意の クラスタ ID を割り当てる
- ネットワーク内の最初の ILS ハブ クラスタで ILS をアクティブにする
- ネットワーク内の残りの ILS クラスタで ILS をアクティブにする
- UDS 証明書要件の検討事項

ネットワーク内の各 Unified CM クラスタに対して一意の クラスタ ID を割り当てる

Unified CM クラスタのエンタープライズ パラメータに定義されているクラスタ ID は一意である必要があります。詳細については、表 2-4を参照してください。

ネットワーク内の最初の ILS ハブ クラスタで ILS をアクティブにする

ILS ネットワークの構築は、最初の Unified CM クラスタ上で ILS をアクティブにすることから始めます。アクティブにするには、最初に Unified CM Administration の [ILS設定（ILS Configuration）] メニューで、役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更します。

表 2-68 は、最初の Unified CM クラスタで ILS をアクティブにするときに適用される設定を示しています。

表 2-68　最初の Unified CM クラスタでの ILS のアクティベーション

設定	値	コメント
[役割（Role）]	[ハブクラスタ（Hub Cluster）]	役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更して、ILS をアクティブにします。
[リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]	オン	URI および数字の到達性情報が、リモート クラスタとやりとりされることを確認します。

表 2-68　最初の Unified CM クラスタでの ILS のアクティベーション（続き）

設定	値	コメント
[アドバタイズされたルート文字列（Advertised Route String）]	us.route	アドバタイズされたルート文字は、この Unified CM クラスタにアドバタイズされるすべての URI および数字の到達性情報に関連付けられているロケーション属性です。このクラスタによってアドバタイズされるいずれかの通知先に到達しようとするリモート クラスタは、学習した SIP ルート文字列をリモート クラスタ上でプロビジョニングされた SIP ルート パターンに照合して、この通知先へのルートを確立しようとします。
[クラスタ同期間隔（Synchronize Clusters Every）]	2	同期間隔を適度に小さく設定すると、リモート クラスタによって短期間で変更が取得されることが保証されます。GDPR は差分更新のアルゴリズムを使用しており、これは最後の更新後に何らかの変更が生じた場合に、差分の情報のみをやりとりするため、間隔を短期間にすることのオーバーヘッドは制限定されます。
[ILS認証（ILS Authentication）]		
[パスワードの使用（Use Password）]	オン	パスワード ベースの認証が選択されます。
[パスワード（Password）]	<some password>	安全なパスワードを選択します。このパスワードは、ILS ネットワークに属しているすべての Unified CM クラスタ間で共有します。

Unified CM Administration で、役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更することによって ILS をアクティブにすると、[ILSクラスタ登録（ILS Cluster Registration）] ポップアップが表示され、登録サーバを入力するよう要求されます。最初の Unified CM クラスタで ILS をアクティブにする場合、登録サーバの情報は使用できないため、ポップアップの入力は空白のままにしておきます。

ネットワーク内の残りの ILS クラスタで ILS をアクティブにする

ILS ネットワークへ Unified CM クラスタを追加するには、最初の Unified CM クラスタで ILS をアクティブにするのと同じプロセスが必要です。つまり、Unified CM Administration の [ILS設定（ILS Configuration）] メニューで、[スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ役割を変更します。

表 2-69 は、残りの Unified CM クラスタ上で ILS をアクティブにするときに適用される設定を示しています。

表 2-69　残りの Unified CM クラスタでの ILS のアクティベーション

設定	値	コメント
[役割（Role）]	[ハブクラスタ（Hub Cluster）]	役割を [スタンドアロンクラスタ（Standalone Cluster）] から [ハブクラスタ（Hub Cluster）] へ変更して、ILS をアクティブにします。
[リモートクラスタとのグローバルダイヤルプランのレプリケーションデータの交換（Exchange Global Dial Plan Replication Data with Remote Clusters）]	オン	URI および数字の到達性情報が、リモート クラスタとやりとりされることを確認します。
[アドバタイズされたルート文字列（Advertised Route String）]	emea.route	これらのルート文字列に基づいて決定論的ルーティングを可能にするには、各クラスタに対する SIP ルート文字列が一意になるようにします。 この例は、EMEA の通知先として機能する Unified CM クラスタを示しています。
[クラスタ同期間隔（Synchronize Clusters Every）]	2	整合性を保証するために、すべてのクラスタで同じ同期間隔を使用するようにします。
[ILS認証（ILS Authentication）]		
[パスワードの使用（Use Password）]	オン	パスワード ベースの認証が選択されます。
[パスワード（Password）]	<some password>	安全なパスワードを選択します。このパスワードは、ILS ネットワークに属しているすべての Unified CM クラスタ間で共有します。

UDS 証明書要件の検討事項

UDS ベースの検出を可能にするために、それぞれの Unified CM クラスタ上の UDS プロセスは、リモート Unified CM クラスタ上で実行中の UDS プロセスとの接続を確立して、リモート クラスタの UDS ノードについて情報を取得しようとします。このサーバ間の通信に対して、Unified CM クラスタのパブリッシャ間で TLS 通信が確立され、TLS の接続の設定時にリモートピアの証明書が検証されます。この検証が失敗しないようにするために、すべての Unified CM クラスタの Unified CM のパブリッシャ ノードの Tomcat 証明書をやりとりする必要があります。

また、このサーバ間の通信を使用する理由の 1 つは、外部 CA で Tomcat 証明書を発行するときに、X.509 の拡張キーに **TLS Web クライアント認証**を含める必要があるためです（表 2-3 を参照してください）。

Unified CM クラスタのパブリッシャ証明書をやりとりするには、次のタスクを実行します。

- Cisco Unified オペレーティング システムの管理の各 Unified CM クラスタで、[証明書の一括管理（Bulk Certificate Management）] を使用してクラスタの Tomcat 証明書をセントラル SFTP サーバへエクスポートします。
- すべてのクラスタから Tomcat 証明書がエクスポートされた後で、クラスタの 1 つで Cisco Unified オペレーティング システムの管理において [統合（Consolidate）] オプションを使用して、すべての Tomcat 証明書を 1 つのファイルに統合します。
- Cisco Unified オペレーティング システムの管理の各 Unified CM クラスタで、[証明書の一括管理（Bulk Certificate Management）] を使用して、すべての Tomcat 証明書が統合されたファイルをインポートします。

このプロセスにより、Unified CM クラスタのすべてのパブリッシャの Tomcat 証明書が、Tomcat 信頼証明書としてすべての Unified CM クラスタのローカルな証明書ストアに確実にインポートされ、クラスタ間の UDS 通信の一部として生じる証明書の検証が失敗しないようになります。

GDPR の設定（マルチクラスタのみ）

ILS ネットワークでグローバル ダイヤル プラン レプリケーション（GDPR）を有効にすると、ILS ネットワーク内のリモート クラスタで、次のようなグローバル ダイヤル プラン データを共有します。

- ディレクトリ URI
- +E.164 および ESN パターン
- PSTN フェールオーバー番号

GDPR では、ILS ネットワーク全体を対象としてディレクトリ URI のクラスタ間ダイヤルや代替番号などのグローバル ダイヤル プランを作成することができます。GDPR を使用すると、各クラスタに対して個別にダイヤル プラン コンポーネントを設定する必要がなく、ILS ネットワーク全体にグローバル ダイヤル プランをすばやく設定できます。

GDPR の設定には、前のセクションで説明した ILS のアクティベーションの他に、次の手順が必要です。

- URI のアドバタイズ
- アドバタイズされたパターンの設定
- 学習番号およびパターンに対するパーティションの設定
- クラスタ間トランクの設定
- SIP ルート パターンの設定

URI のアドバタイズ

このドキュメントでは、ユーザの URI は、社内ディレクトリの電子メール属性から、各ユーザに同期されているディレクトリ URI に基づいて（表 2-45 を参照）、および各ユーザに設定されているプライマリ内線に基づいて自動的にプロビジョニングされると仮定しています。デフォルトでは、[ILSを介してグローバルにアドバタイズ（Advertise Globally via ILS）] オプションは、パーティション ディレクトリ URI で自動的に作成された URI に対して設定されています。また、自動的に作成された URI だけでなく、プロビジョニングしたすべての URI について [ILSを介してグローバルにアドバタイズ（Advertise Globally via ILS）] オプションを設定するようにします。

アドバタイズされたパターンの設定

リモート クラスタ上でルート プランを小規模に保持するために、この設計では、各クラスタにホストされている +.164 および ESN 範囲に対してサマリー パターンのみがアドバタイズされます。たとえば、サイト RTP、RCD、および SJC にホストしているクラスタについては、表 2-70 で示されているパターンは、GDPR アドバタイズ パターンとして設定する必要があります。この例で使用されている DID 範囲および ESN 範囲の詳細については、表 2-10 および 表 2-11 を参照してください。

表 2-70　GDPR を介してアドバタイズされるパターン

パターン	パターン タイプ	PSTN フェールオーバー設定	コメント
+14085554XXX	[+E.164番号（Advertised Failover Number）]	[パターンをPSTNフェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト SJC の DID 範囲
81404XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTNフェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTNフェールオーバー削除桁数（PSTN Failover Strip Digits）]:4 [PSTNフェールオーバー付加番号（PSTN Failover Prepend Digits）]:+1408555	SJC DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81405XXX	[エンタープライズ番号（Enterprise Number）]	[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]	SJC 非 DID の ESN 範囲 PSTN フェールオーバーは不可
+19195551XXX	[+E.164番号（Advertised Failover Number）]	[パターンをPSTNフェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト RTP の DID 範囲
81911XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTNフェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTNフェールオーバー削除桁数（PSTN Failover Strip Digits）]:4 [PSTNフェールオーバー付加番号（PSTN Failover Prepend Digits）]:+1919555	RTP DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81912XXX	[エンタープライズ番号（Enterprise Number）]	[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]	SJC 非 DID の ESN 範囲 PSTN フェールオーバーは不可
+19725555XXX	[+E.164番号（Advertised Failover Number）]	[パターンをPSTNフェールオーバー番号として使用する（Use Pattern as PSTN Failover Number）]	サイト RCD の DID 範囲

表 2-70　GDPR を介してアドバタイズされるパターン（続き）

パターン	パターン タイプ	PSTN フェールオーバー設定	コメント
81975XXX	[エンタープライズ番号（Enterprise Number）]	[パターンに削除桁数と付加番号を適用し、PSTNフェールオーバーに使用する（Apply Strip Digits and Prepend Digits to Pattern and Use for PSTN Failover）] [PSTNフェールオーバー削除桁数（PSTN Failover Strip Digits）]：4 [PSTNフェールオーバー付加番号（PSTN Failover Prepend Digits）]：+1972555	RCD DID の ESN 範囲 ESN から PSTN フェールオーバー番号へ変換するための削除桁数とプレフィックス。
81976XXX	[エンタープライズ番号（Enterprise Number）]	[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]	RCD 非 DID の ESN 範囲 PSTN フェールオーバーは不可
8099XXXX	[エンタープライズ番号（Enterprise Number）]	[PSTNフェールオーバーを使用しない（Don't use PSTN Failover）]	このクラスタの会議用の ESN 範囲（表 2-11 を参照）

各サイトに対して +E.164 範囲と ESN 範囲の両方をアドバタイズすることにより、この情報を学習するリモート クラスタ上のクラスタ間ダイヤリング手順として両方の形式を使用することができます。

学習番号およびパターンに対するパーティションの設定

リモート クラスタから学習した番号パターン（+E.164 および ESN）は、事前定義のパーティションのローカル ルート プランに追加されます。Unified CM Administration の [学習番号とパターンのパーティション（Partitions for Learned Numbers and Patterns）] メニューでは、学習した情報のそれぞれのタイプについて、異なるパーティションを定義することができます。この設計では、1 つのパーティション、onNetRemote のすべてのリモート数値パターンを学習するために、この区別および簡単な設定 GDPR を行う必要はありません（表 2-13 を参照してください）。

表 2-71 は、GDPR パーティションの設定をまとめています。

表 2-71　GDPR パーティションの設定

設定	値	コメント
[エンタープライズ代替番号のパーティション（Partition for Enterprise Alternate Numbers）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオフにする	
[+E.164代替番号のパーティション（Partition for +E.164 Alternate Numbers）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオンにする	+E.164 のオンネット クラスタ間コールで番号間のタイムアウトを回避するために、緊急としてマークされる。

表 2-71　GDPR パーティションの設定（続き）

設定	値	コメント
[エンタープライズパターンのパーティション（Partition for Enterprise Patterns）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオフにする [可変長パターンを緊急とする（Mark Variable Length Patterns as Urgent）] をオンにする	
[+E.164パターンのパーティション（Partition for +E.164 Patterns）]	onNetRemote [学習番号を緊急とする（Mark Learned Numbers as Urgent）] をオンにする [可変長パターンを緊急とする（Mark Variable Length Patterns as Urgent）] をオンにする	+E.164 のオンネット クラスタ間コールで番号間のタイムアウトを回避するために、緊急としてマークされる。

クラスタ間トランクの設定

GDPR 交換では、すべての URI および数値の到達性情報が Unified CM クラスタ間で交換され、SIP ルート文字列にロケーション属性として関連付けられることを保証するだけです。クラスタ間のセッションは、SIP トランクを確立する必要があります。この設計では、すべての Unified CM クラスタ間において、最大 3 つの Unified CM クラスタを備えたフルメッシュ SIP トランクを仮定しています。最大 3 つの Unified CM クラスタにより、SIP トランクのフルメッシュのトポロジが管理可能であることが保証されます。4 つ以上の Unified CM クラスタが必要な場合は、Unified CM Session Management Edition（SME）を追加し、SME をハブとして、その他すべての Unified CM クラスタをスポークスまたはリーフ クラスタとするハブアンドスポーク トポロジになるように簡素化することが推奨されます。

標準の SIP クラスタ間トランクは GDPR ルーティングとして使用されます。表 2-61 に示されている設定と同様に、SIP トランク ST_UCM_EMEA は、GDPR 用にプロビジョニングされたクラスタ間トランクの例です。

SIP ルート パターンの設定

SIP ルート パターンは、GDPR を介して学習した SIP ルート文字列と SIP トランク トポロジを関連付けます。GDPR のルート文字列が、学習した URI 又は数値パターンが見つかった「場所」を教えてくれると考えると、この通知先に到達する方法を教えるには、これらのルート文字列上でルート パターン マッチングが必要になります。

GDPR の完全な到達性を実現するには、GDPR を介してアドバタイズされる各 SIP ルート文字列が、プロビジョニングされている SIP ルート パターンに従ってルートできることを確実にする必要があります。表 2-72 は、2 つの Unified CM 間で完全なクラスタ間 GDPR ルーティングを実現するためにプロビジョニングする必要があるトランク、ルート、グループ、ルート リスト、および SIP ルート パターンについて概要を示しています。

表 2-72　2 つの Unified CM クラスタを備えた GDPR ルーティング

コンポーネント	US クラスタ	EMEA クラスタ	コメント
SIP トランク	[ST_UCM_EMEA]	ST_UCM_US	他の Unified CM クラスタに向けた、各クラスタ上の SIP トランク（表 2-61 を参照）
上記の SIP トランクをメンバーとするルート グループ	[UCM_EMEA]	UCM_US	クラスタ間トランクに対する専用のルート グループ（表 2-63 を参照）
上記のルート グループをメンバーとするルート リスト	[RL_UCM_EMEA]	RL_UCM_US	クラスタ間トランクに対する専用の非 LRG ルート リスト（表 2-64 を参照）
SIP ルート文字列	us.route	emea.route	Unified CM クラスタによってアドバタイズされた SIP ルート文字列
上記のルート リストをポイントする SIP ルート パターン	パーティション onNetRemote の emea.route	パーティション onNetRemote の us.route	他の Unified CM クラスタによってアドバタイズされた SIP ルート文字列上での、プロビジョニングされた SIP ルート パターン マッチ

GDPR コール フローの例

このセクションでは、上記の設定例で EMEA クラスタに登録されている "international" サービス クラスのエンドポイントで +14085554001 がダイヤルされた場合に、コールがどのようにルートされるかについて説明しています。

1. ダイヤルされた番号（+14085554001）は、発信側デバイスの CSS XXXInternational を使用して、EMEA クラスタ上のダイヤル プランに対して照合されます。ここで XXX は、EMEA クラスタ上でプロビジョニングされているサイトのサイト コードを表します。実際のサイト特定のダイヤル正規化は、ここでは関係ありません。

   CSS XXXInternational には少なくとも次のパーティションが含まれていることが重要なポイントです（表 2-18 を参照。XXX はサイトのコードを、XX はダイヤル ドメイン識別子を表します）。

   - DN
   - Directory URI
   - URI
   - ESN
   - onNetRemote
   - XXXIntra
   - XXtoE164
   - XXPSTNNational
   - PSTNInternational
   - B2B_URI
   - USEmergency

これらのパーティション ダイヤル番号（+14085554001）は、次の 3 つのものと一致します。

- SIP ルート文字列が us.route である US クラスタから学習したパーティション onNetRemote の +14085554XXX（表 2-70 を参照）
- \+!パーティション PSTNInternational の \+!（表 2-29 を参照）
- パーティション PSTNInternational の \+!#（表 2-29 を参照）

2. パーティション onNetRemote の +14085554XXX は緊急パターンとしてルートに挿入され（表 2-71 を参照）、この段階ではこのパターンがベスト マッチであるため、番号の収集はすぐに停止し、このベスト マッチに基づいてルートされます。
3. パーティション onNetRemote の +14085554XXX は GDPR の学習パターンで、SIP ルート文字列 us.route に関連付けられます。したがって、us.route は EMEA クラスタ上に設定された SIP ルート パターンに対して、発信側デバイスの CSS XXXInternational を使用して照合されます。

   唯一のマッチは、パーティション onNetRemote における SIP ルート パターンです。
4. EMEA クラスタのコールは SIP トランク ST_UCM_EMEA に拡張され、マッチした SIP ルート パターン us.route がポイントしているルート リスト RL_UCM_EMEA への参照、および RG_UCM_EMEA への参照は解除されます（表 2-72 を参照してください）。
5. US クラスタでは、SIP トランク ST_UCM_EMEA の着信側 CSS ICTInbound（表 2-61 を参照）を使用して、着信コールが通知先 +14085554001 へルートされます。
6. CSS ICTInbound には次のパーティションがあります。
   - DN
   - ESN
   - URI
   - Directory URI

   これらのパーティションの唯一の（潜在的な）マッチは、パーティション DN における +E.164 電話番号 \+14085554001（緊急としてマークされている）です。この電話番号が存在する場合は、コールは、関連付けられているすべてのデバイスに拡張されます。

リモートでダイヤルされた ESN 通知先のルーティングは同じフローに従いますが、ここでは CSS ICTInbound を使用した US クラスタ上の最後のルックアップで、パーティション ESN の ESN を見つけることだけが異なります。

IM and Presence クラスタ間展開

フルメッシュのプレゼンス トポロジを作成するには、それぞれの Cisco IM and Presence クラスタと、同じドメイン内の他のそれぞれの Cisco IM and Presence クラスタとの間に、個別のピア関係が設定されている必要があります。このクラスタ間ピアに設定されているアドレスは、リモート Unified CM クラスタ IM and Presence のパブリッシャ ノードの IP アドレスです。

各 Cisco IM and Presence クラスタ間のインターフェイスには、AXL/SOAP インターフェイスとシグナリング プロトコル インターフェイス（SIP または XMPP）の 2 つが使用されます。IM and Presence クラスタのパブリッシャのみのサーバ間の AXL/SOAP インターフェイスはホーム クラスタ アソシエーションの同期を処理しますが、これは完全なユーザ同期ではありません。シグナリング プロトコル インターフェイス（SIP または XMPP）はフルメッシュで、展開内のすべてのサーバを対象としています。これは、サブスクリプション トラフィックと通知トラフィックを処理します。また、同じドメイン内のリモートの Cisco IM and Presence クラスタにユーザが存在することが検出された場合、SIP インターフェイスが URI のホスト部分を書き換えた後でユーザを転送します。

Cisco IM and Presence がクラスタ間環境に展開されている場合、プレゼンス ユーザを決定する必要があります。プレゼンス ユーザ プロファイルは、マルチクラスタ プレゼンスの展開の規模とパフォーマンス、およびサポート可能なユーザ数の決定に役立ちます。プレゼンス ユーザ プロファイルによって、一般的なユーザの連絡先（バディ）の数、およびそれらの連絡先の多くがローカル クラスタのユーザか、リモート クラスタのユーザかが確定します。

Survivable Remote Site Telephony（SRST）展開

リモート サイトへの WAN が失敗した場合に呼処理が存続するようにするために、各リモート サイトで SRST を設定します。SRST では WAN が失敗しても、リモート サイトまたは PSTN 内で電話のコールを作成することができます。

展開

SRST に対応させる各リモート サイトに 1 つの Cisco Integrated Services Router（ISR）を展開します。

プロビジョニング

SRST を設定するには、Unified CM と SRST ルータの両方で設定を行う必要があります。

Unified CM での設定

- 各リモート サイトに対して SRST 参照先を設定し、リモート電話のデバイス プール内の SRST 参照先に関連付けます。
- +E.164 番号および AAR CSS を使用するには、リモート電話の DN で [不在転送未登録（Call Forwarding Unregistered）（CFUR）] を設定します。WAN が失敗した場合、コールはこの情報を使用し、PSTN を介してルートされます。

SRST ルータでの設定

- 各リモート ブランチ ルータで SRST を設定します。ここでは、SIP 電話の使用が推奨されるため、**voice register global** および **voice register pool** コマンドを使用します。**voice service voip/sip** コマンドを使用してソース インターフェイスの IP アドレスをバインドし、レジスタの容量を有効にします。リモート ブランチの電話に DHCP を設定します。DHCP サーバは、SRST ルータ、または他のネットワーク サービス リソース上に設定することができます。
- WAN が失敗した場合、SIP phone は自身の +E.164 内線番号で登録します。4 桁の内線番号を使用して他のローカル ユーザへ通話できるようにするには、音声レジスタ プールの設定で着信プロファイルとして参照される音声変換プロファイルを設定します。この音声変換プロファイルは、着信番号を 4 桁から +E.164 の完全な番号へ変換します。
- POTS ダイヤルピアを設定して、WAN が停止している場合の PSTN へのローカル アクセスを可能にします。サービス プロバイダの PSTN ダイヤル要件に準拠するために、変換音声プロファイルを設定します。ダイヤルピア設定の詳細については、Cisco Unified Border Element を展開するの方法について説明しているセクションを参照してください。

例 2-6 の SRST 設定は、前の段落で説明したいくつかの概念を説明するための、部分的なものです。SRST の完全な設定について記載しているわけではありません。たとえば、メイン サイトの Cisco Unity Connection サーバへ到達するための設定については、コア アプリケーションの章で説明しています。

例 2-6　SRST 設定（一部）

```
voice service voip
 allow-connections sip to sip
sip
  bind control source-interface GigabitEthernet0/0.241
  bind media source-interface GigabitEthernet0/0.241
  registrar server
!
voice register global
 mode srst
 max-dn 100
 max-pool 100
!
voice register pool  1
 translation-profile incoming 4-digit-rtp
 id network 10.0.94.0 mask 255.255.255.0
!
voice translation-rule 1
 rule 1 /\(^1...\)$/ /+1919555\1/
!
voice translation-profile 4-digit-rtp
 translate called 1
!
```

SRST での設定の詳細については、次のサイトで入手可能な『*Cisco Unified SCCP and SIP SRST System Administrator Guide*』を参照してください。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/admin/sccp_sip_srst/configuration/guide/SCCP_and_SIP_SRST_Admin_Guide.html

エクステンション モビリティ

Cisco Extension Mobility では、Cisco Unified IP Phone の設定（ライン アピアランス、サービス、短縮ダイヤルなど）に他の Cisco Unified IP Phone から一時的にアクセスすることができます。

1 つまたは 2 つの Unified CM コール処理ノードは、Extension Mobility の要求をアクティブに処理することができます。Extension Mobility に対して 2 つ目の Unified CM コール処理ノードを追加すると、レジリエンスおよびキャパシティが増加するという利点があります。このシナリオでは、2 つの Unified CM ノードへ要求を送信するために 1 つのロード バランサが必要です。Cisco IOS Server Load Balancing などを使用することができます。

Extension Mobility Cross Cluster（EMCC）を使用すると、社内のクラスタ間でエクステンション モビリティのログインを実行することができます。この機能については、このガイドでは説明していません。EMCC の詳細については、『*Cisco Collaboration System 10.x SRND*』および EMCC 製品のドキュメントを参照してください。

エクステンション モビリティの展開

エクステンション モビリティを展開するには、次のタスクを実行します。

- 1 つまたは 2 つの Unified CM 呼処理サーバで Cisco Extension Mobility サービスがアクティブになっていることを確認します。
- エクステンション モビリティ向けの IP Phone サービスを追加します。非セキュアな URL の他に、HTTPS を使用したセキュアな IP Phone サービスの URL を設定できます。非セキュア URL は次のとおりです。

  http://<*IPAddress*>:8080/emapp/ EMAppServlet?device=#DEVICENAME#

  ユーザは、[エンタープライズ登録（Enterprise Subscription）] を選択してクラスタ内のすべての電話でサービスを使用できるようにするか、またはこれらの電話をこのサービスに登録し、選択した電話で使用できるようにするか、いずれかを選択することができます。
- エクステンション モビリティを使用する各ユーザについて、少なくとも 1 つのデバイス プロファイルを作成します。デバイス プロファイルは特定のユーザに関連付けられているため、デバイス プロファイルは通常、ユーザ デバイス プロファイルとして参照されます。あるユーザに対してデバイス プロファイルが作成されていない場合、ユーザはエクステンション モビリティにログインできません。
- デバイス プロファイルを、エクステンション モビリティのユーザに関連付けます。CTI が必要な場合は、CTI コントロールのデバイス プロファイルとなるプロファイルを関連付けます。
- ユーザのログインで使用できるそれぞれの電話について、エクステンション モビリティを有効にします。Cisco DX シリーズエンドポイントで、（電話によってリセットされる）マルチユーザも有効にします。TC ソフトウェアを使用している Cisco TelePresence エンドポイント（Cisco TelePresence EX や SX シリーズのエンドポイントなど）で、TelePresence のエンドポイントが Cisco TelePresence Management Suite（TMS）でプロビジョニングされていないことを確認します。プロビジョニングされている場合は、エンドポイントでサインイン ボタンが使用できません。
- DN の設定で、対象ユーザの関連付けを回線へ設定します。これにより、電話回線が使用中の場合でも、DN で対象ユーザのプレゼンス情報を送信することができます。次に例を示します。

  ユーザ B が Jabber を使用しており、ユーザ B がユーザ A を監視しています。ユーザ A はエクステンション モビリティを使用して電話にログインしており、自身に関連付けられている DN のユーザ デバイス プロファイルを持っています。ユーザ A がオフフック状態になると、このプレゼンス情報はユーザ B の Jabber クライアントでレポートされます。

エクステンション モビリティの詳細については、次のサイトで入手可能な『*Features and Services Guide for Cisco Unified Communications Manager*』を参照してください。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmfeat/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100.html

ビジー回線フィールド（BLF）のプレゼンス

BLF プレゼンス機能により、ユーザ（ウォッチャ）は、ある電話番号または SIP URI における他のユーザのリアルタイムのステータスを、ウォッチャのデバイスから監視することができます。ウォッチャは、次のオプションを使用してユーザのステータスを監視することができます。

- BLF/スピードダイヤル ボタン
- ディレクトリ ウィンドウの不在着信、発信履歴、または着信履歴のリスト
- 共有ディレクトリ（社内ディレクトリなど）

BLF プレゼンスは Cisco Unified IM and Presence をベースにしているわけではありません。

BLF プレゼンスの展開

- **コール リストの BLF** エンタープライズ パラメータを有効にします（表 2-4 を参照してください）。
- BLF プレゼンスに対してクラスタ全体のサービス パラメータを設定します。
- BLF プレゼンス グループの認証を使用するには、BLF プレゼンス グループおよび権限を設定します。
- Cisco Unified Communications Manager Administration で、電話番号、SIP トランク、SIP を実行している電話、SCCP を実行している電話、エンド ユーザ、およびアプリケーション ユーザ（SIP トランクを介して BLF プレゼンス要求を送信しているアプリケーション ユーザ）に対して BLF プレゼンス グループを適用します。
- SIP トランクから BLF プレゼンス要求を可能にするには、[SIPトランクセキュリティプロファイルの設定（SIP Trunk Security Profile Configuration）] ウィンドウの [プレゼンスの SUBSCRIBEの許可（Accept Presence Subscription）] オプションを選択します（表 2-59 を参照してください）。
- SUBSCRIBE コーリング サーチ スペースを設定し、必要に応じて電話、トランク、またはエンド ユーザにコーリング サーチ スペースを適用します。
- 電話の BLF/スピードダイヤル ボタンでは、BLF/スピードダイヤル ボタンのボタン テンプレートをカスタマイズしたり、電話へ直接追加したりできます。

コンピュータ テレフォニー インテグレーション（CTI）の展開

- CTI Manager サービスを必要とする Unified CM 呼処理ノード上で、CTI Manager サービスをアクティブにします。
- 冗長性を実現するために、CTI のアプリケーション管理全体で、CTI Manager サービスを実行しているプライマリおよびバックアップの Unified CM ノードを選択します。
- TAPI を使用するアプリケーションについて、TAPI クライアント ソフトウェアをダウンロードします。
- 可能な場合は、CTI に対応している特定のエンドポイントについて、CCM 登録および CTI Manager 監視および制御について同じ Unified CM 呼処理ノードを設定します。

- CTI Manager を実行しているすべての Unified CM ノードで CTI の負荷が分散されており、CTI の容量制限を超えていないことを確認します。たとえば、Jabber クライアントで 2 つの Unified CM 呼処理ペアが必要な場合、登録を 2 つのペアで分散させます。また、Jabber クライアントがデスク電話モードでの機能で設定されている場合は、2 つのペアで CTI Manager の接続性を分散させます。これは、複数のサービス プロファイルに複数の CTI プロファイルを関連付けることによって実現されます。CTI Manager サービスを実行している各 Unified CM で監視および制御されているデスク電話モードの Jabber クライアントの数が、CTI の容量制限を超えていないことを確認します。

会議

改訂日：2015 年 1 月 22 日

この章では、企業展開におけるビデオおよび音声会議のコンポーネントと導入方法について説明します。また、会議のアーキテクチャについて説明し、会議の導入プロセスに含まれる主なタスクについて概要を示します。

会議の導入プロセスの主なタスクはそれぞれ、そのタスクに必要な手順をリストする「*概要*」セクションから始まり、そのタスクの重要な「*導入上の考慮事項*」を扱うセクションが続きます。その後、「*概要*」セクションでリストされた導入タスクの詳細を示すセクションが続きます。

この章の変更点

この章では、Cisco Collaboration System Release（CSR）10.6 に関する内容が大幅に改定されました。特に、スケジュール済み会議の推奨される導入は、直接管理型 TelePresence Server から TelePresence Conductor によって管理される TelePresence Server に変更されました。ご使用のコラボレーション ソリューションへの会議の導入を試す前に、この章全体を読むことをお勧めします。

コア コンポーネント

コア アーキテクチャには、以下の主要な会議要素が含まれます。

- 音声およびビデオ会議リソース用の Cisco TelePresence Server
- 音声およびビデオ会議リソース管理用の Cisco TelePresence Conductor
- 会議のプロビジョニング、モニタリング、およびスケジューリング用の Cisco TelePresence Management Suite（TMS）
- スケジュール済み音声および Web 会議、ハイブリッド ビデオおよび Web 会議用の Cisco WebEx Software as a Service（SaaS）

主な利点

- 会議の参加者にとって簡略化された最適なユーザ エクスペリエンス
- 無期限、スケジュール済み、インスタントのいずれかまたはすべての会議の 1 つ以上のリソースの導入をサポートする柔軟性と拡張性のあるアーキテクチャ
- 着信コールに対する TelePresence Server での会議リソースの動的な最適化
- ビデオ ネットワークでの復元性

会議タイプ

会議ソリューションでは、表 3-1 および表 3-2 にリストされている会議タイプおよび会議機能をサポートします。

表 3-1　　会議の種類

会議タイプ	説明
[インスタント会議（Instant conferences）]	Unified CM でホストされたポイントツーポイント コールから、会議ブリッジにホストされた三者コールへのエスカレートは手動で行います（アドホック会議とも呼ばれます）。インスタント会議は事前にスケジュールまたは調整されることはありません。
[無期限の会議（Permanent conferences）]	事前のスケジュールなしで会議を行えるようにする、事前定義されたアドレス。会議ホストはその他のユーザとアドレスを共有します。それらのユーザは、いつでもそのアドレスにコールインできます（ミートミー会議、静的会議、またはランデブー会議とも呼ばれます）。この章で扱う無期限の会議は Cisco Personal Collaboration Meeting Rooms を使用します。
[スケジュール済み会議（Scheduled conferences）]	開始および終了時間のある（オプションで一連の参加者を事前定義する）、Cisco TMS を介して、または Cisco TMS を使用した統合、あるいはその両方を使用して予約する会議。
[Cisco Personal Collaboration Meeting Rooms（CMR）]	会議名、レイアウト、PIN などの項目を管理できるポータルを使用して Cisco TMS からプロビジョニングされた無期限の会議。
[Cisco CMR Hybrid]（旧称 WebEx Enabled TelePresence）	スケジュール済み会議に似ていますが、TelePresence および WebEx の参加者が同じ会議に参加し、音声、ビデオ、およびコンテンツを共有できるようにする Cisco WebEx Meeting Center へのリンクを使用します。
[個人向けマルチパーティ（Personal Multiparty）]	個人向けマルチパーティには、インスタント、無期限、スケジュール済み、および CMR の会議を提供するユーザベースのライセンス アプローチが含まれます。これは、名前付きホストで任意の数の参加者がいる、最大解像度 1080p の会議に使用されます。個人向けマルチパーティ会議では、TelePresence Conductor のバックグラウンドで TelePresence Server を使用する必要があります。

表 3-2　　代替ソリューション

ソリューションの種類	説明
Cisco WebEx Meetings Server	クラウドベースの Web および音声会議が適していない場合に、オンプレミス WebEx Meetings Server ソリューションを使用できます。この製品は、現時点では、TelePresence とのハイブリッド会議を提供していませんが、スタンドアロンの音声、ビデオ、およびコラボレーション Web 会議のプラットフォームを提供します。
Cisco CMR Cloud	Cisco CMR Cloud は、オンプレミス会議リソースまたは管理インフラストラクチャの必要性を打ち消す代替会議の導入モデルです。1 つのコールで、各種の標準規格に準拠したビデオ（TelePresence を含む）、音声、および WebEx の参加者をサポートします。すべてはクラウドでホストされます。

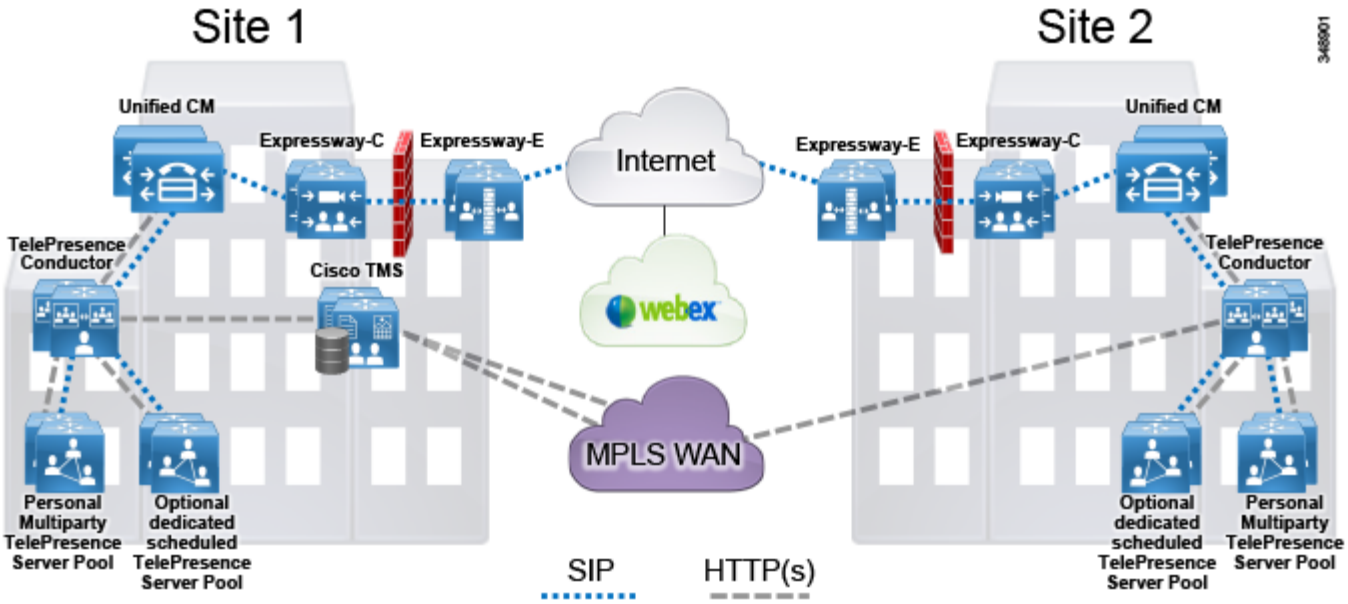
アーキテクチャ

TelePresence Conductor は、すべてのタイプの会議の会議ブリッジを管理します。SIP トランクを使用して、TelePresence Conductor とのブリッジに接続し、TelePresence Conductor を Unified CM と接続します（図 3-1）。

HTTP 上でアプリケーション プログラミング インターフェイス（API）を介して会議ブリッジを制御するために Unified CM が使用するすべての XML リモート プロシージャ コール（RPC）接続も、TelePresence Conductor を通過します。また、Cisco TMS は、プロビジョニングおよびスケジュール済み会議の管理のためにも、TelePresence Conductor にリンクする XML-RPC 接続を使用します（図 3-1）。

図 3-1 に示すアーキテクチャでは、SIP が排他的に使用されています。H.323 エンドポイントを使用する会議では、Cisco Video Communication Server（VCS）または Cisco Expressway-C によるインターワーキングが必要になります。

図 3-1　　アーキテクチャの概要



TelePresence Conductor の役割

TelePresence Conductor は、すべてのタイプの会議用に TelePresence Server を管理します。TelePresence Conductor は特定の会議をホストするために使用する TelePresence Server またはブリッジ プールを選択します。また、定義したプール内の TelePresence Server 全体で会議にかかる負荷のバランスを取ります。Unified CM は、ネットワーク内の個々の TelePresence Server を認識せず、TelePresence Conductor とのみ通信します。

会議に TelePresence Conductor を使用すると、以下のようないくつかの利点があります。

- 会議の TelePresence Server のリソースを共有することによる効率の向上
- ActiveControl やリソースの動的最適化などの拡張された TelePresence Server 機能によるユーザ エクスペリエンスの向上
- プロビジョニングされた CMR による導入オプションの簡略化
- すべてのタイプの会議に対応する単一導入モデル

場合によっては、TelePresence Conductor 会議テンプレートで [リソースの最適化（Optimize resources）] 設定を有効にすると、TelePresence Conductor が TelePresence Server リソースを動的に最適化します。これにより、参加者の最大リソース使用率は、会議参加中にアドバタイズされた最大受信帯域幅に基づくようになります。会議コールによって使用されるリソースの量は削減され、実行される同時接続により多く対応できるようになります。詳細については、『TelePresence Server release notes』を参照してください。

Cisco TMS の役割

スケジュール済み会議では、Cisco TMS が会議スケジュール機能および会議制御機能を実行します。

Cisco TelePresence Management Suite Provisioning Extension（TMSPE）は、個人向け Collaboration Meeting Rooms（CMR）の管理者による自動化された一括プロビジョニング、および個々のユーザが自分の個人向け CMR の定義と管理をするためのユーザ ポータルをサポートします。

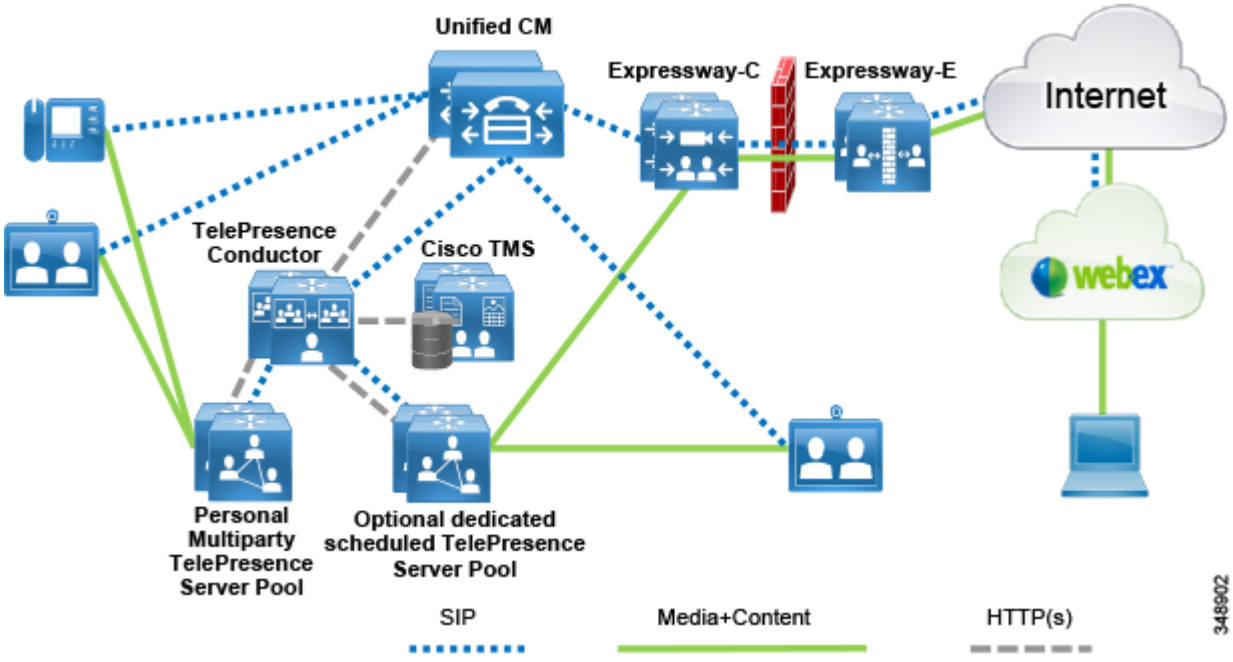
TelePresence Server の役割

TelePresence Server は、リモート管理モードで動作する会議ブリッジであり、TelePresence Conductor でプールにグループ化されます。TelePresence Conductor は、会議用のプールに優先順位を付けるサービス設定を適用します。ブリッジ プールは、スケジュールされた会議と事前スケジュールなしの会議の間で共有することも、いずれかのタイプの会議の専用にすることもできます。

展開の概要

標準的な展開では、複数の Unified CM ノードがコール制御に使用されます。TelePresence Conductor は、会議リソースを提供するために、TelePresence Server を管理する SIP トランクを使用して Unified CM に接続されます（図 3-2）。TelePresence Server はコールをブリッジするために使用され、Cisco TMS は会議管理ファシリティおよびスケジューリングを提供します。

図 3-2　　標準的な展開



標準的な展開では、コール制御やエンドポイント管理のための Unified CM と会議管理のための Cisco TMS を併用して、いくつかの TelePresence Server が TelePresence Conductor の背後に配置されます。CMR Hybrid サービスと同様、スケジュールされない会議とスケジュール済み会議の両方に同じ会議インフラストラクチャを使用できます。WebEx は、スケジュール済みの音声およびビデオ Web 会議を提供します。これらの要素は一緒に、ローカル エンタープライズに音声およびビデオ会議を提供します。

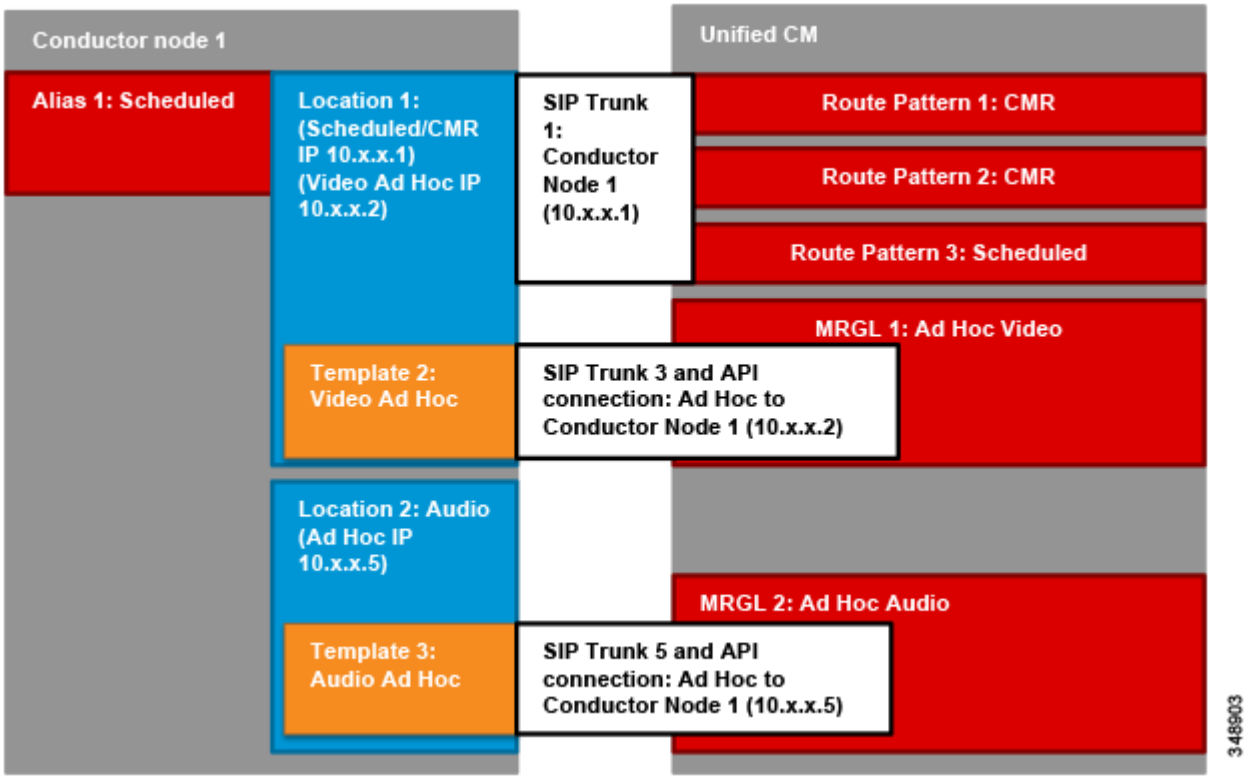
要件と推奨事項

- 早期オファーは、CMR Hybrid コールといくつかのサードパーティ サービス（Microsoft Lync など）を必要とします。
- TelePresence コールを伝達する Unified CM に接続されたすべての SIP トランクで、早期オファー メッセージングを推奨します。
- すべての TelePresence Server は、リモート管理モードで設定し、すべての会議タイプに対応する会議リソースとして TelePresence Conductor の背後に配置する必要があります。
- エスカレートされた会議の Multiway™ 方式は、推奨されていません。
- TelePresence Server 上の音声会議は、参加トーンも終了トーンもサポートしていません。

会議のコール フロー

Unified CM で、接続されたエンドポイント間の音声およびビデオ コールのデバイス登録およびルーティングを行います。無期限、インスタント、およびスケジュール済みの会議コールは、SIP トランク上で実行されます。XML-RPC 接続は、Unified CM パブリッシャで設定し、Unified CM コール処理サブスクライバ ノードと TelePresence Conductor ノードの間を HTTP 上で接続します。

図 3-3　Unified CM および TelePresence Conductor SIP トランク



CMR およびスケジュール済みの会議コールは、同じトランク上で Unified CM からルーティングします。一方、インスタント会議コールは、会議を作成した Unified CM から TelePresence Conductor テンプレートに直接ルーティングします。そのため、各タイプに対して 1 つずつ、複数のトランクがインスタント会議に存在する可能性があります。各トランクには、関連付けられた XML-RPC 接続があります。発信 Unified CM がインスタント会議を制御します。そのため、SIP API トランク ペアが、ローカル TelePresence Conductor へのインスタント会議をサポートする各 Unified CM クラスタからのインスタント会議タイプごとに必要になります。

Unified CM によって管理されるインスタント コール フローは、スケジュール済み会議など、その他の方法で作成された会議への参加者を追加するために使用できません。その他のコール フローを使用して、インスタント会議への参加者を追加することはできません。インスタント コール エスカレーション方式は、その方法で作成されたインスタント会議でのみサポートされます。その他の方法で生成された会議をインスタント メカニズムで拡張することはできません。これにより、チェーン会議の可能性を回避できます。

（注）　Unified CM は、インスタント会議を、TelePresence Conductor 上の CMR やスケジュール済み会議とは異なる IP アドレスに対して提供します。複数の Unified CM クラスタが、TelePresence Conductor 上の同じ IP アドレスにアクセスできます。ただし、このマニュアルでは、1 つの TelePresence Conductor クラスタが各 Unified CM クラスタに専用であることを想定しています。

インスタント会議

インスタント会議は、TelePresence Conductor で設定します。そのため、会議は単一の TelePresence Server 上に静的に定義されることはありません。TelePresence Conductor は、プール内の使用可能な TelePresence Server 全体で会議についてロードバランスします。これにより、会議の復元性が向上します。インスタント会議は、Unified CM と各 TelePresence Conductor ノードの間の XML-RPC 接続に関連付けられた SIP トランクを必要とします。Unified CM は、これらの SIP トランクの IP アドレスにインスタント会議の参加者をルーティングします。

Collaboration Meeting Rooms を使用した無期限の会議

無期限の会議は、個人向け Collaboration Meeting Rooms（CMR）を使用して導入されます。個人向け CMR は、Conductor Provisioning API と連携して Cisco TMSPE で作成された無期限タイプの会議を提供します。ユーザは会議エイリアスをダイヤルして会議をいつでも開始できます。

個々のエンドユーザは、管理者によってプロビジョニングされたグループ レベルのテンプレートに基づいて、Cisco TMSPE ユーザ ポータルから自分の CMR を作成します。ユーザ ポータルから作成されたそれぞれの CMR には、TelePresence Conductor 上に対応する会議バンドル エンティティ（ConfBundle）が存在します。これは、Conductor Provisioning API によって作成および管理され、1 人以上のユーザの会議を作成するために必要なデータが含まれます。このデータには、会議テンプレート情報、一連の会議エイリアス、一連の自動ダイヤルの参加者、および会議名が含まれます。ConfBundle は、Web UI では [Collaboration Meeting Rooms] としてレポートされます。Cisco TMSPE を使用して作成された CMR は、TelePresence Conductor Web UI から変更できません。逆に、TelePresence Conductor を使用して作成された会議テンプレートおよびエイリアスは、Cisco TMSPE から変更できません。CMR 会議は、Unified CM と各 TelePresence Conductor ノードの間の SIP トランクを必要とします。Unified CM は、CMR 会議の参加者をこれらの SIP トランクの IP アドレスに ルーティングします。

設定情報

- Cisco TMSPE の設定の詳細については、『*Cisco TelePresence Management Suite Provisioning Extension with Cisco Unified CM Deployment Guide*』を参照してください。以下から入手できます。

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-provisioning-extension/model.html

- Conductor Provisioning API の詳細については、『*Cisco TelePresence Conductor API Guide*』を参照してください。以下から入手できます。

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-programming-reference-guides-list.html

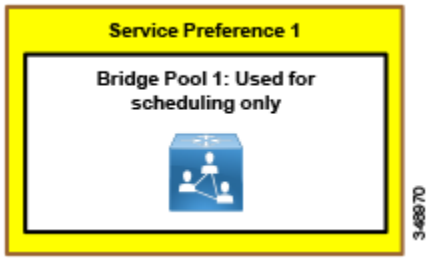
スケジュール済み会議

このソリューションは、TelePresence Conductor による会議のスケジュールをサポートします。スケジュール設定は、Cisco TMS で実行します。スケジュール済み会議は、Unified CM と各 TelePresence Conductor ノードの間の SIP トランクを必要とします。Unified CM は、スケジュール済み会議の参加者をこれらの SIP トランクの IP アドレスにルーティングします。これらのトランクは、CMR 会議に使用されるトランクと同じです。

TelePresence Conductor を使用する場合、TelePresence Server リソースをスケジュールするには 2 種類の導入方法があります。すなわち、会議リソースをスケジュール済み会議の専用にする方法と、スケジュール済み会議とスケジュールされない会議の両方で共有する方法を採用できます。利点および欠点については、表 3-3 を参照してください。

- 専用 TelePresence Server：スケジュール済み会議専用の 1 台以上の TelePresence Server を設置します。各 TelePresence Server は独立したブリッジ プールおよびサービス設定で配置されます（図 3-4）。オプションで、2 つ目のブリッジとプールの組み合わせをバックアップとして使用することもできます。

図 3-4　　専用のスケジューリング TelePresence Server



- 共有 TelePresence Server：スケジュール済み会議に加えて、スケジュールされない会議にも TelePresence Server を使用できるようにします（図 3-5）。この場合、スケジュール済み会議のリソースの可用性は、必要なリソースがスケジュールされない会議によってすでに使用されている可能性があるため保証できません。すべての TelePresence Server のサイズが類似していれば、それらを単一のブリッジ プールに構成することもできます。

図 3-5　　共有スケジューリング TelePresence Server

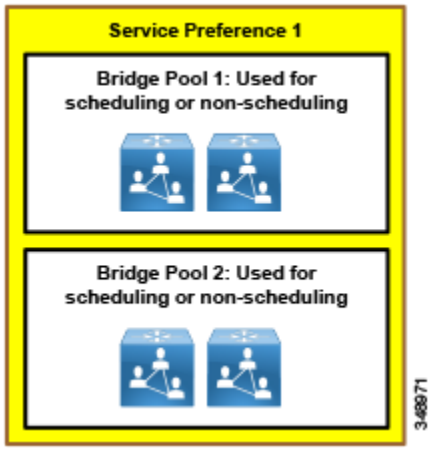


表 3-3　TelePresence Server リソースでの専用と共有の対比

リソースの種類	展開の詳細	利点	欠点
専用	サービス設定：スケジュール済み会議専用の TelePresence Server プール。 プール内の 1 台の TelePresence Server が配置される単一プール。プールは TelePresence Conductor サービス設定でスケジュールに使用されるとマークが付けられます。プールは、容量情報要求で TMS にレポートされます。 サービス設定では、オプションで、ハイ アベイラビリティのためにスケジュールされないブリッジ プールを指定できます。これには、追加の専用 TelePresence Server リソースが含まれます（詳細については、「会議のハイ アベイラビリティ」(P.3-12)を参照してください）。	会議リソースをスケジュール済み会議専用にすることによって、スケジュールされない会議によってリソースが使用されるリスクはなくなります。また、十分なリソースがプロビジョニングされていれば、リソースの可用性が損なわれてスケジュール済み会議に不具合が生じるリスクもなくなります。	TelePresence Server がスケジュール用に専有されてしまいます。スケジュールされない会議には、異なる TelePresence Server を使用する必要があります。 ユーザが特定の期間にスケジュールされない会議をより多く行う場合、会議リソースの使用効率が低下します。使用パターンの変動に対処するために、より多くのリソースが必要になります。 使用可能なリソースを使用できるスケジュールされない会議がないため、最適化されたリソースの利点が打ち消されてしまいます。 カスケードされる会議は発生しません。リソースを無駄に使用しないように、カスケードを無効にする必要があります。
共有	サービス設定：スケジュール済み会議とスケジュールされない会議で共有される TelePresence Server。 スケジュール済み会議とスケジュールされない会議で共有される 1 つ以上のプール。 1 つ以上のサービス設定。各サービス設定には、TelePresence Conductor 内でスケジュールが有効にされたすべてのブリッジ プールがあり、複数の TelePresence Server 会議ブリッジを含めることができます。サービス設定では、オプションで、ハイ アベイラビリティのためにスケジュールされないブリッジ プールを指定できます。これには、追加の専用または共有 TelePresence Server リソースが含まれます（詳細については、「会議のハイ アベイラビリティ」(P.3-12)を参照してください）。	より効率的なリソース使用。ユーザが使用するスケジュール済みリソースが増減する場合でも、使用されない専用リソースが発生するなどの、アイドル状態で残されるリソース数への影響はありません。 カスケードされた会議が使用できます（有効にされている場合）。 TelePresence Server リソースの的を絞った管理が可能です。 スケジュール済み会議のリソースが最適化されて使用可能になったリソースは、スケジュールされない会議が使用できます。 時間をかけて使用パターンのモニタリングを行うことによって、最適なプール設定を識別できます。	スケジュールされない会議がすべてのリソースを使用してしまう可能性があるため、会議リソースをスケジュール済み会議で使用できるかは必ずしも保証されません。高い使用率でも機能するように十分なリソースを提供することによって、このリスクを低減できます。

ヒント　インスタント会議のみ、CMR 会議のみ、スケジュール済み会議のみ、または 3 種類の会議すべてをホストするように TelePresence Server を TelePresence Conductor で設定できます。単一の TelePresence Server プールを使用することにより、全体の会議参加者の最大数をプロビジョニングできるため、必要な TelePresence Server の数を最小限に抑えることができます。

Multiway

Cisco では、この展開で Multiway（インスタント エスカレーションの Cisco VCS 方式）を使用することをお勧めしません。Multiway は、Cisco VCS のみの展開で使用する必要があります。その代わりに、Unified CM の展開では、このマニュアルで説明されているように会議ボタンのエスカレーション方式を使用する必要があります。両方のタイプのインスタント会議の同時使用はサポートされていません。

サードパーティ エンドポイント

他の機器プロバイダー製のエンドポイントは、標準 SIP を使用して、インスタント、スケジュール済み、および CMR 会議に参加できます。インスタント会議を開始できるのは、会議ボタンをサポートする Unified CM に登録されたエンドポイントだけです。SIP への H.323 コールをインターワーキングさせるために Cisco Expressway または Cisco VCS を使用できます。これにより、H.323 エンドポイントは会議に参加できるようになります。

設定情報

Cisco TMS を使用して会議をスケジュールする方法のガイダンスについては、コア アプリケーションの章のセクション Cisco TelePresence Management Suite（TMS）による会議スケジュールを参照してください。

Cisco WebEx Software as a Service（SaaS）

Cisco WebEx Software as a Service（SaaS）は、音声およびビデオ Web 会議をリッチ コンテンツ コラボレーションで提供するクラウド ホスト型ソリューションです。スケジュール済み音声会議をホストする場合に、このサービスを使用することをお勧めします。次のセクションで説明するように、CMR ハイブリッド会議を作成するためにも使用されます。

Cisco CMR Hybrid

Cisco WebEx ユーザと TelePresence ユーザは、スケジュール済み会議またはユーザの個人向け Collaboration Meeting Rooms（CMR）に共同して参加できます。Cisco WebEx と TelePresence Server の間のコールの音声部分では、SIP と PSTN ベース音声の両方がサポートされます（WebEx 参加者と WebEx 会議の間の音声接続は、PSTN 音声、SIP 音声、またはコンピュータ テレフォニーのいずれかになります）。

Cisco WebEx Meetings Server

一部の導入では、クラウドベースのコラボレーション サービスが適していない場合があります。このようなお客様の場合、代わりにオンプレミス ソリューションの Cisco WebEx Meetings Server を使用することをお勧めします。このサーバは、WebEx の Software as a Service バージョンのように TelePresence とは統合されませんが、その代わりにスタンドアロンの音声、ビデオ、およびコラボレーション Web 会議サービスとして機能します。インストール手順については、以下にある WebEx Meetings Server 製品のマニュアルを参照してください。

http://www.cisco.com/c/en/us/support/conferencing/webex-meetings-server/products-installation-guides-list.html

Collaboration Meeting Rooms（CMR）Cloud

Cisco CMR Cloud は、オンプレミス会議リソースまたは管理インフラストラクチャの必要性を打ち消す代替会議の導入モデルです。CMR Cloud は、Cisco WebEx Meeting Center サブスクリプションのアドオン オプションとして提供される使いやすいクラウド ホスト型ミーティング ルーム ソリューションで、Cisco WebEx Cloud を通して提供されます。このソリューションによって、各種の標準規格に準拠したビデオ エンドポイントを最大 25 台、ビデオ対応 WebEx Meeting Center ユーザを最大 500 ユーザ、および音声のみの WebEx Meeting Center ユーザを最大 500 ユーザ、つまり 1 つの会議で合計 1,025 の参加者をサポートするように拡張できる、クラウドでの会議が可能になります。このガイドでは、CMR Cloud の導入については扱っていません。CMR Cloud の導入の詳細については、『Cisco Collaboration Meeting Rooms（CMR）Cloud Enterprise Deployment Guide』を参照してください。以下から入手できます。

http://www.cisco.com/c/en/us/support/conferencing/webex-meeting-center/products-installation-and-configuration-guides-list.html

会議のハイ アベイラビリティ

会議ソリューションについていくつかのレベルで、ハイ アベイラビリティを考慮する必要があります。また、ハイ アベイラビリティは、考慮するサービスに応じて異なる方法で実現されます。

スケジュール済み会議とスケジュールされない会議の両方とも、ハイ アベイラビリティには、Unified CM、TelePresence Server、および TelePresence Conductor が関係します。

TelePresence Server のハイ アベイラビリティ

TelePresence Server で障害が発生した場合には、TelePresence Conductor のサービス設定内に使用可能なリソースがある限り、会議は別の TelePresence Server で行うことができます。会議番号は同一のまま残るため、エンド ユーザが関係する範囲では、シームレスに行われます。

TelePresence Conductor のハイ アベイラビリティ

フルキャパシティの標準 TelePresence Conductor は、最大 3 つの Conductor ノードのクラスタの一部にすることができます。各ノードは、その他のノードすべてに対してラウンド トリップ遅延が 30 ミリ秒以内である必要があります。コールは、クラスタ内のどのノード経由でもフローできます。あるノードが使用できなくなった場合、残りの TelePresence Conductor ノードを使用して、会議に参加できます。

（注）　TelePresence Conductor には、このマニュアルでは扱われないモデルが他に 2 つあります。TelePresence Conductor Select はクラスタ内の 2 つの Conductor ノードをサポートしますが、TelePresence Conductor Essentials はクラスタリングをサポートしません。

TelePresence Conductor クラスタは、冗長性を確保するために使用されます。プライマリ Conductor に障害が発生した場合に、現在および将来の会議を管理するためにセカンダリまたはターシャリの Conductor が使用できます。この冗長性は、インスタントおよび無期限の会議ではシームレスに機能します。ただし、スケジュール済み会議の場合、この冗長性は自動的には機能せず、セカンダリまたはターシャリの TelePresence Conductor にフェールオーバーするには手動による介入が必要になります。これは、Cisco TMS が 1 つの TelePresence Conductor ノードしか認識しないためです。そのクラスタ ノードに障害が発生した場合、そのノードが復旧するか、Cisco TMS がクラスタ内の別の TelePresence Conductor ノードと通信するように更新されるまで、Cisco TMS のスケジューリングは使用できなくなります。

Cisco TMS は、TelePresence Conductor に設定された各エイリアスを、TelePresence Server リソースの別個のセットと見なします。エイリアスにコールをスケジュールするために使用できるリソースがない場合、次の優先順位にあるエイリアスが検討されます。複数の TelePresence Conductor が設定されている場合（TelePresence Conductor クラスタごとに 1 つ）、スケジュール済み会議に対してそれらが Cisco TMS によって検討されます。Cisco TMS は、TelePresence Conductor の IP ゾーン設定および予約時にスケジュールされたエンドポイントを使用して、その予約でどの TelePresence Conductor を優先すべきかを判別します。

TMS ハイ アベイラビリティ

Unified CM および Cisco TMS のハイ アベイラビリティ（TMSPE も含む）については、「Cisco TelePresence Management Suite（TMS）による会議スケジュール」（P.5-37）のセクションで説明します。

このマニュアルでは、音声会議は WebEx クラウドを使用するようにスケジュールされており、そのため通常のテレフォニーおよび Web の接続性を超えた復元力に関する考慮事項はないことを想定しています。Cisco WebEx Meetings Server が代わりに使用されている場合、サーバについてのハイ アベイラビリティを考慮する必要がありますが、このアプローチについてはこのマニュアルでは扱われません。

会議のセキュリティ

このソリューションでは、メディアおよびシグナリングの暗号化は使用されません。その代わり、すべての会議で Unified CM と TelePresence Conductor の間にセキュリティで保護されない SIP トランクが実装されています。この例外となるのは、TelePresence Conductor と TelePresence Server の間の API 通信を暗号化しなければならないというソリューションの要件です。この要件を満たすため、暗号化機能キーを TelePresence Server にインストールする必要があり、この場合、HTTPS を使用する必要があります。また、これは、有効な認証局の署名付き証明書を使用して暗号化されたメディアおよびシグナリングを有効にするという Cisco Expressway と WebEx クラウドの間の通信の要件ともなります。

PIN やパスワードを使用して会議へのアクセスを制限するため、別レベルのセキュリティを追加できます。すべての参加者に、接続が許可される前に PIN の入力を要求するように、すべてのスケジュール済み会議または CMR 会議で PIN を設定できます。CMR Hybrid では、会議の TelePresence 部分を保護するために PIN を使用できます。また、会議の WebEx 部分に対して、パスワードを追加または自動生成できます。

会議ソリューションの拡張

まず、ライセンスを追加して、使用可能な TelePresence Server の数を増やすことによって、または TelePresence Server がサポートできる接続数を増やすことによって、会議ソリューションを拡張できます。

TelePresence Server の合計数は、TelePresence Conductor の容量によって制限されます。フルキャパシティの各 TelePresence Conductor（または各クラスタ）は、最大 30 台の TelePresence Server または 2,400 個の同時会議コールを管理できます。クラスタリングによって、TelePresence Server の最大数またはサポート可能な同時コールの最大数は増加しません。

単一 TelePresence Conductor の容量を超えるほど展開が大きくなった場合、新しい独立したクラスタを作成して、そこに TelePresence Server の追加を継続することができます。

各地域の Unified CM に対して、独立した TelePresence Conductor クラスタを使用します。たとえば、3 つの Unified CM が存在する場合、地域ごとに 1 つずつ、3 つの TelePresence Conductor クラスタを配置する必要があります。

会議の導入プロセス

会議ソリューションを導入するには、以下の主要なタスクをリストの順に実行します。

1. 会議の導入を計画する
2. TelePresence Server を導入する
3. TelePresence Conductor を導入する
4. スケジュール済み会議とスケジュールされない会議用に Unified CM を有効にする
5. 会議用の TelePresence Management Suite の有効化
6. Cisco Collaboration Meeting Rooms の導入
7. WebEx および Collaboration Meeting Rooms（CMR）Hybrid の導入

1. 会議の導入を計画する

会議ソリューションを導入する前に、以下の項目について計画します。

要件

- IP アドレスをプロビジョニングします。各 TelePresence Conductor ノードには、それ自体の IP アドレスが必要です。導入する会議サービスに応じて、最大 64 個の追加の IP アドレスを設定できます。
- すべての TelePresence Server で暗号化キーを発注してインストールします。
- CMR Hybrid には、必要なものがすべて所定の場所に配置されるように、前もって理解しておく必要がある多くの要件があります。たとえば、オプション キーは、Cisco TMS 用に発注されている必要があります。Cisco Expressway-E には、適切な認証局から公的に署名された証明書が必要です。CMR Hybrid が機能できるようにするため、Cisco Expressway-E は WebEx ルート証明書を信頼する必要があります。

製品モデル

Cisco では、TelePresence Conductor と TelePresence Server の複数の異なるモデルを用意しています。導入環境に最も適したオプションを選択できるように、それらのモデルの相違を理解しておくことが重要です。

TelePresence Conductor には 3 種類のモデルがあります。1 つのクラスタで最大 2,400 個の同時コールおよび最大 3 つの Conductor ノードをサポートするため、企業導入用のフルキャパシティのバージョンを使用します。

すべての TelePresence Server は、TelePresence Conductor の背後でスケジュール済み会議にもスケジュールされない会議にも使用できます。仮想マシン上の TelePresence Server は、いくつかの容量で使用できます。大きな容量が必要な場合、MSE 8000 シャーシベース MSE 8710 ブレードを使用できます。MSE 8710 は、1 つのクラスタ内で最大 4 つのブレードをサポートします。つまり、MSE 8710 の容量は 4 倍まで増加します。クラスタは、単一デバイスであるかのように動作します。

これらのデバイスのいずれかを、リモート管理モードで実行し、TelePresence Conductor と連携できるように設定できます。

ライセンシング

さまざまな製品にライセンスをインストールする必要があります。

- Cisco TMS では、CMR Hybrid 用に WebEx 統合キーがインストールされている必要があります。
- このガイドでは、Personal Multiparty Advanced を使用して、TelePresence Server のライセンスを受けます。
- TelePresence Conductor のフルバージョンには、必要なライセンスがインストールされています。

Personal Multiparty は、2 つのバリエーション（Basic と Advanced）があるユーザベースのライセンシング モデルです。このガイドでは、Advanced オプションのみを考慮します。各ライセンスは、最大 1080p ビデオ品質で任意の数の参加者が参加できる会議スペースへの権限をユーザに付与します。Personal Multiparty Advanced を発注すると、2 つの Conductor フル ライセンスが含まれています。TelePresence Conductor クラスタは、個人向けマルチパーティ会議をプロビジョニングするために使用されます。Personal Multiparty ライセンスで使用するために、TelePresence Server を専用にする必要があります。Personal Multiparty でライセンス付与された TelePresence Server では、画面ライセンスを購入する必要ありません（Personal Multiparty ライセンシングを介して受けたライセンスをデバイスに適用する必要はあります）。

2. TelePresence Server を導入する

このセクションでは、TelePresence Conductor を使用するために、TelePresence Server を導入し、準備するために必要な主なタスクについて説明します。これらの TelePresence Server は、スケジュール済み会議とスケジュールされない会議に使用できます。

概要

TelePresence Server の導入タスク：

1. 暗号化機能キーをインストールします。
2. 使用する TelePresence Conductor の新規 API アクセス ユーザを作成します。
3. HTTPS および 暗号化 SIP（TLS）サービスを有効にし、H.323 サービスを無効にします。
4. SIP 設定を [直接コール（Call Direct）] に、また TLS を使用するように設定し、H.323 ゲートキーパー登録を無効にします。
5. リモート管理モードのオプションがあれば、サーバをリモート管理モードに設定し、リブートします。

導入上の考慮事項

メディア トラフィックが TelePresence Server と会議の各参加者との間をフローするので、TelePresence Server の物理的な場所を考慮することが重要です。参加者に最高のエクスペリエンスを提供するために、TelePresence Server が導入される各地域で、TelePresence Server のロケーションを集中配置します。

TelePresence Server をリモート管理モードに設定します。これは、より高度な API を有効にし、すべてのオペレーションでその API を使用するのに必要なシステム全体の設定です。リモート管理モードは、仮想マシン上の Cisco TelePresence Server で使用できる唯一のモードです。TelePresence Server をその他の環境で使用する場合は、リモート管理モード またはローカル管理モード（TelePresence Conductor には使用できません）のいずれかを使用できます。

注意　リモート管理モードでは、特定の機能は TelePresence Server インターフェイスから使用できません。また、会議の管理およびエンドポイントの事前設定は TelePresence Conductor レベルで実行されます。動作モードを変更するには、TelePresence Server をリブートする必要があります。また、TelePresence Server でローカル管理モードに設定されたすべての会議は、そのユニットがリブートされると失われます。

TelePresence Conductor は、XML-RPC API を介して TelePresence Server を管理します。また、TelePresence Conductor は、SIP シグナリングを Back-to-Back User Agent（B2BUA）を介して TelePresence Server にルーティングします。

TelePresence Server には、通信に安全な接続を使用する機能があります。これらのセキュリティ機能は、暗号化機能キーで有効にされます。暗号化機能キーは、TelePresence Conductor が TelePresence Server と通信するのに必要です。暗号化されない通信はサポートされません。

インスタント、無期限、およびスケジュール済みの会議

図 3-6　　インスタント会議のコール フロー

図 3-7　　無期限またはスケジュール済み会議のコール フロー

TelePresence Server の導入タスク

最初に、暗号化機能キーをすべての TelePresence Server に適用します。これにより、HTTPS と TLS および暗号化されたメディアを使用して、暗号化されたシグナリングを使用することができます。次に、TelePresence Server で HTTPS および暗号化された SIP（TLS）サービスを有効にして設定します。

TelePresence Conductor が TelePresence Server と通信できるようにするには、TelePresence Conductor が API 認証に使用する TelePresence Server に API アクセス ユーザ アカウントを作成します。

TelePresence Server 上のすべての H.323 設定を無効にし、発信トランスポートに TLS を使用する SIP 設定で直接コール モードを有効にします。TelePresence Conductor は SIP のみを使用するため、これが必要になります。

TelePresence Server をリモート管理モードに設定します。これにより、TelePresence Conductor はサーバと通信できるようになります。このタスクは、常にリモート管理モードで実行される仮想マシン上の Cisco TelePresence Server には関係ありません。

要約

上記のタスクを完了すると、TelePresence Server は TelePresence Conductor を追加する準備が整います。

3. TelePresence Conductor を導入する

このセクションでは、スケジュール済み会議とスケジュールされない会議用に TelePresence Conductor を導入するために必要な主なタスクについて説明します。

概要

TelePresence Conductor でのインスタント会議とスケジュール済み会議に共通する導入タスク：

1. API ユーザを TelePresence Conductor に作成します。
2. 共有個人向けマルチパーティのブリッジ プールを作成し、TelePresence Server をそのブリッジ プールに追加します。専用モデルの場合、複数のブリッジ プールを作成し、ブリッジ プールごとに 1 つの TelePresence Server を追加します。
3. 個人向けマルチパーティのサービス設定を作成し、ブリッジ プールをそのサービス設定に追加します。
4. 各会議タイプごとに 1 つの IP アドレスを TelePresence Conductor に割り当てます。
   - インスタント音声個人向けマルチパーティ会議
   - インスタント ビデオ個人向けマルチパーティ会議
   - CMR およびスケジュール済み個人向けマルチパーティ会議

   クラスタ内の各 TelePresence Conductor ノードでこのプロセスを繰り返します。各ノードに、IP アドレスの固有のセットが必要になります。

TelePresence Conductor でのインスタント会議の導入タスク：

5. インスタント会議用に TelePresence Conductor を設定するには、各会議タイプのテンプレートを作成します。
   - インスタント音声個人向けマルチパーティ テンプレート
   - インスタント ビデオ個人向けマルチパーティ テンプレート

   ビデオ テンプレートでは、[リソースの最適化（Optimize resources）] を [はい（yes）] に設定します。
6. 各インスタント会議のテンプレートに固有のロケーションを作成します。1 つのロケーションに 1 つのテンプレートしか割り当てることはできません。
   - インスタント音声個人向けマルチパーティ ロケーション
   - インスタント ビデオ、CMR、およびスケジュール済み個人向けマルチパーティ ロケーション
7. 関連するインスタント テンプレートを関連するロケーションに割り当てます。また、アドホック IP アドレスをそれぞれに割り当てます。各アドホック IP アドレスは、SIP および API を介して TelePresence Conductor と通信するために Unified CM によって使用されます。

TelePresence Conductor でのスケジュール済み会議の導入タスク：

8. 以前に作成したインスタント ビデオ、CMR、およびスケジュール済み個人向けマルチパーティのロケーションを編集します。タイプを [両方（Both）] に変更し、ランデブー IP アドレスを割り当てます。ランデブー IP アドレスは、SIP を介して TelePresence Conductor と通信するために Unified CM によって使用されます。

   Unified CM コール処理サブスクライバ ノードの IP アドレスを使用して、最大 3 つのトランク IP アドレスをインスタント ビデオ、CMR、およびスケジュール済み個人向けマルチパーティのロケーションに追加します。

9. 以前に作成したブリッジ プールを編集し、個人向けマルチパーティのロケーションを共有個人向けマルチパーティのブリッジ プールに割り当てます。複数のプールが存在する場合、同じロケーションをすべてのプールに追加します。

10. スケジュール済み会議用に TelePresence Conductor を設定するには、以下のテンプレートを作成します。

    – スケジュール済み個人向けマルチパーティ 720p HD ビデオ テンプレート

    サービス設定をテンプレートに割り当てます。テンプレートで、[リソースの最適化（Optimize resources）] を [はい（yes）] に設定し、[スケジュール済み会議（Scheduled conference）] を [はい（yes）] に設定します。

11. テンプレートをスケジュールするための固有の着信エイリアスが Cisco TMS の設定中に作成されます。サービス設定を編集し、ブリッジ プールで [スケジュールに使用するプール（Pools to use for scheduling）] オプション ボタンが選択されていることを確認します。これは、容量を TelePresence Conductor にレポートする必要のあるブリッジ プールでのみ設定する必要があります。

導入上の考慮事項

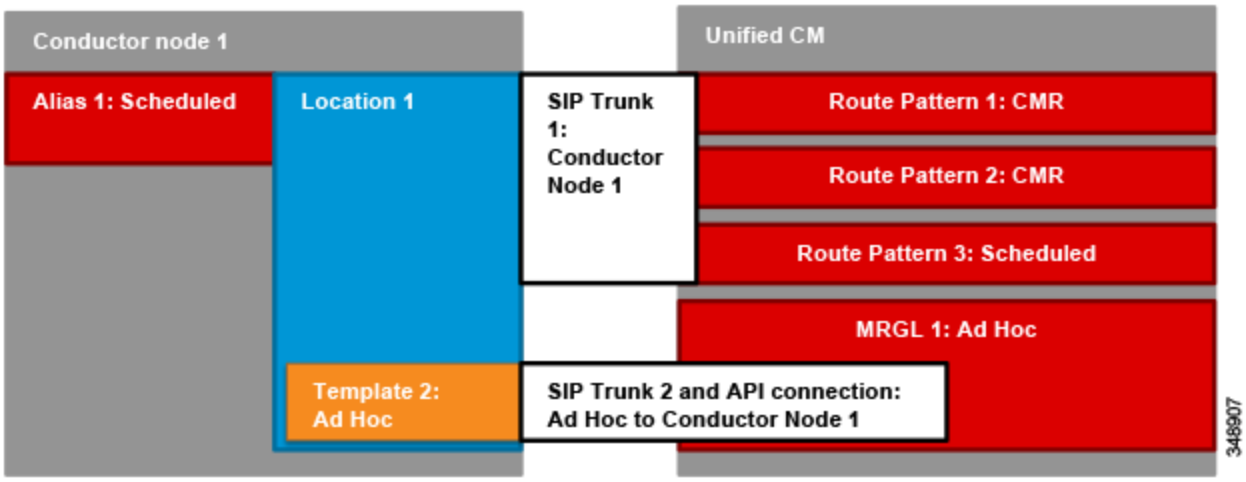
（注）　TelePresence Conductor を設定する前に、すべてのアラームをクリアして、製品が機能できるようにします。

インスタント、CMR、およびスケジュール済みの会議を有効にするには、システム管理者が TelePresence Conductor と Unified CM の設定を完了する必要があります。これらの 2 つの製品は、会議作成ロジックの責任を共有します。TelePresence Conductor は TelePresence Server への排他的接続を維持しますが、Unified CM に関する限り MCU と同様に機能します。また、Unified CM からの要求に基づいて、会議の開催を決定します。

TelePresence Conductor は、図 3-1 に示されているように、各地域の Unified CM クラスタにその地域のすべての TelePresence Server を管理する関連付けられた TelePresence Conductor クラスタが存在するように、地域に集中配置的な方法で展開する必要があります。

TelePresence Conductor は、Back-to-Back User Agent（B2BUA）を使用して、導入する必要があります。Unified CM は、TelePresence Conductor が TelePresence Server と通信する方法と同様に、XML-RPC API および SIP トランクを使用して TelePresence Conductor と通信します。（図 3-8）。

図 3-8　　Unified CM と TelePresence Conductor の間の API および SIP トランク接続



インスタントおよびスケジュール済み会議

図 3-9　　インスタント会議用の TelePresence Conductor の内部設定フロー

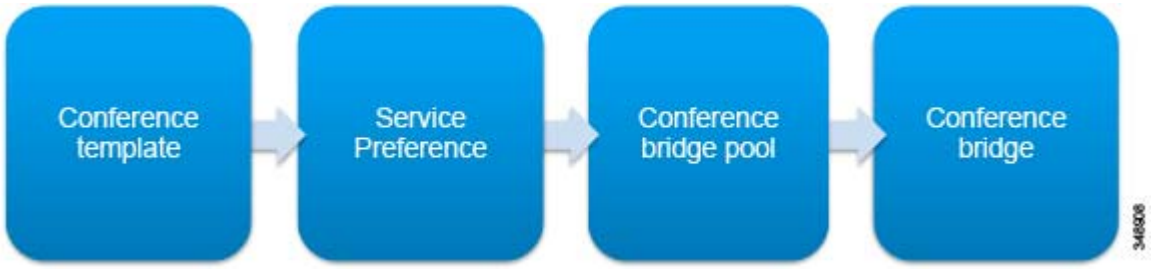
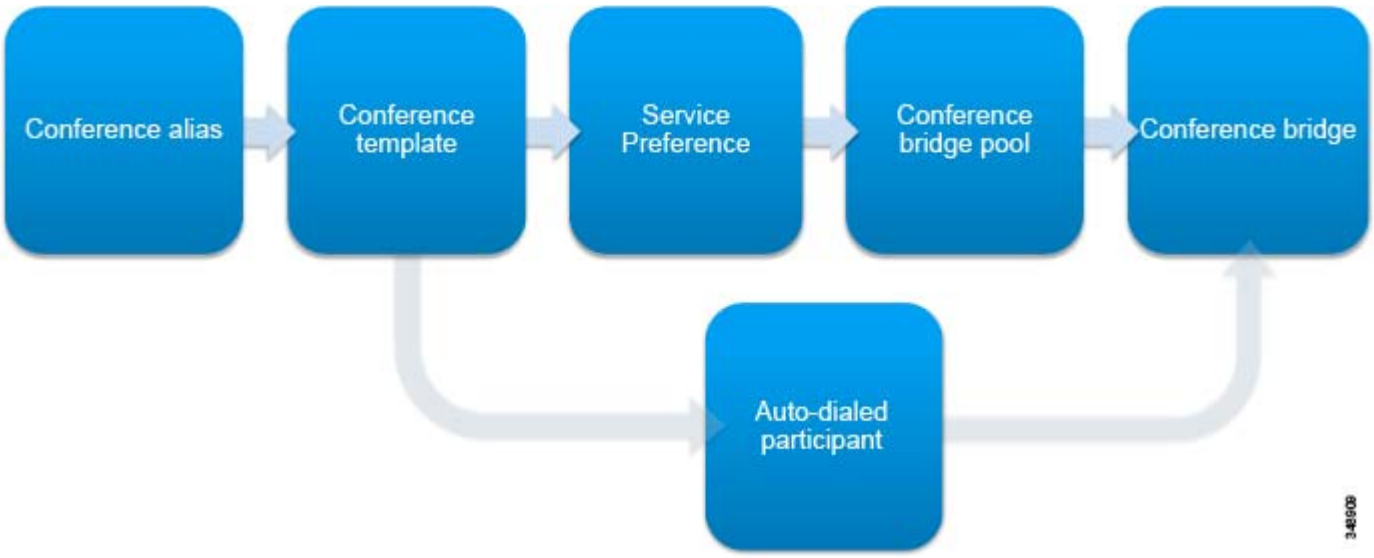


図 3-10　スケジュール済み会議用の TelePresence Conductor の内部設定フロー

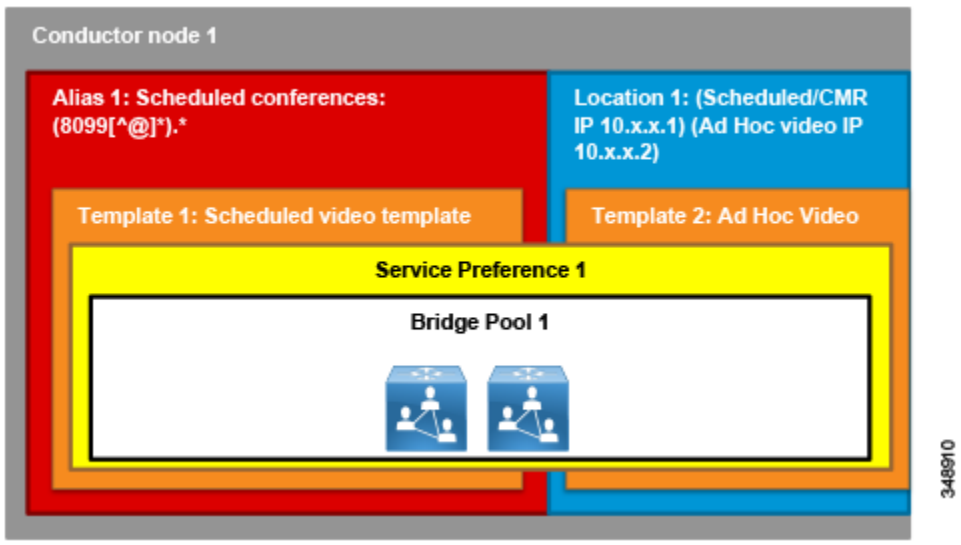


TelePresence Conductor でのインスタント会議とスケジュール済み会議に共通する導入タスク

設定を開始する前に、TelePresence Conductor 内のすべてのアラームを解決します。未解決のアラームがあると、TelePresence Conductor は機能しません。また、root および管理者のパスワードを変更し、Unified CM が TelePresence Conductor API にアクセスするための認証に使用する API ユーザを作成します。

図 3-11 に、TelePresence Server プールを使用するスケジュール済みおよびインスタント会議のために TelePresence Conductor 内でどの要素を設定する必要があるかを詳細に示します。

図 3-11　TelePresence Conductor の設定



展開内の各 TelePresence Server は、TelePresence Conductor のブリッジ プールに割り当てる必要があります。TelePresence Server は、1 つのブリッジ プールにしか属することができません。ブリッジ プールは、TelePresence Server の物理的な場所を反映する必要があります。また、ブリッジ プールに複数の TelePresence Server が含まれている場合、それらすべてを類似したサイズにする必要があります。各 TelePresence Conductor は、1 つの地域専用になります。そのため、このマニュアルでは、すべての TelePresence Server は同じ物理的な場所に存在することを想定しています。物理的な場所が複数存在する場合、Unified CM によるコール アドミッション制御を維持するために、それぞれに対してロケーションとプールを設定する必要があります。前述のとおり、専用スケジューリング モデルを使用する場合、ブリッジ プールにはスケジューリング専用の TelePresence Server が 1 つだけ存在します。一方、共有モデルの場合、ブリッジ プールに複数の TelePresence Server が存在できます。

サービス設定は、TelePresence Conductor を介して設定されたブリッジ プールに優先順位が付けられたリストで、会議リソースが限られている場合に使用するプールの順番を定義します。管理者は、特定の会議に対して TelePresence Conductor がその会議をホストするために使用を試みるプールの優先順位を決定できます。最初のブリッジ プールに、会議をホストするために使用できる TelePresence Server がなかった場合（たとえば、会議の要件を満たすために使用できるリソースが不足している）、TelePresence Conductor はリストの 2 番目のブリッジ プールをチェックします。図 3-11 に示されているスケジュール済み会議およびインスタント会議は、すべて同じサービス設定を使用します。そのため、同じブリッジ プールが使用されます。それぞれが異なるサービス設定を使用する（つまり、異なるブリッジ プールを使用する）ことも、複数のブリッジ プールを 1 つのサービス設定に定義することも可能です。

サービス設定には、1 ～ 30 個の会議ブリッジ プールを含めることができます。また、任意の数のサービス設定で 1 つの会議ブリッジ プールを使用することができます。

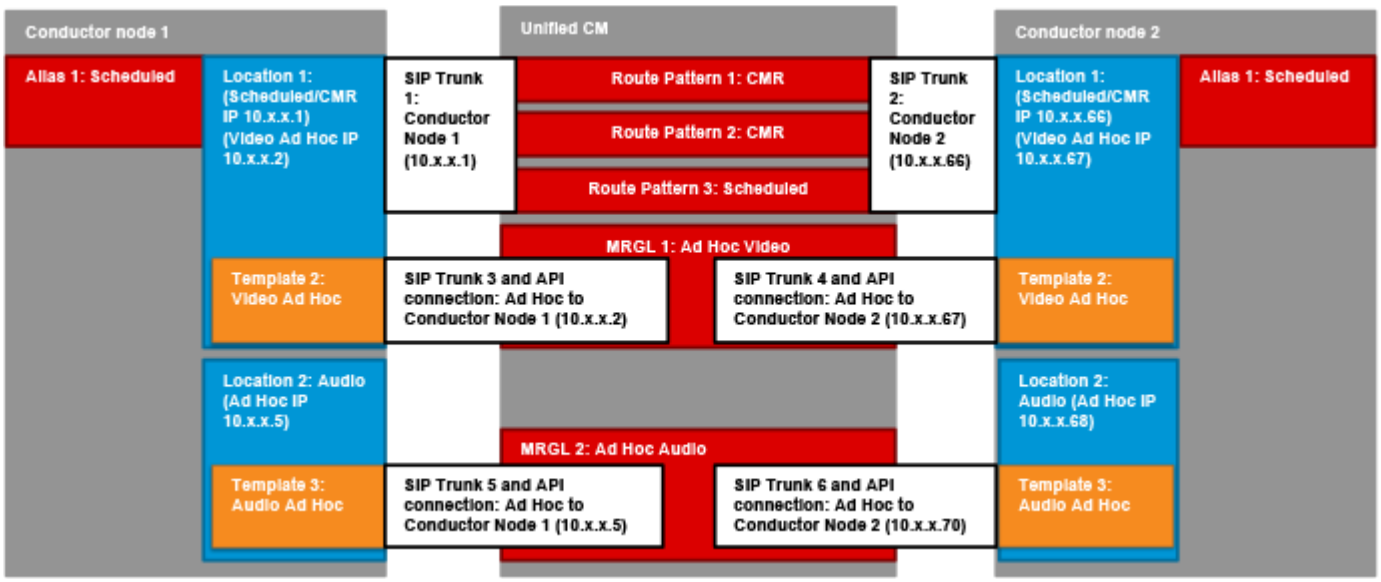
プールと同様、TelePresence Conductor サービス設定で設定されたすべての TelePresence Server は、メディアが常に同じ物理的な場所に送信されるように、同じ物理的な場所に存在している必要があります。そのようにして、帯域幅の使用量が把握できるようにします。

Unified CM と TelePresence Conductor の間の各 SIP トランクは、固有の IP アドレスを使用する必要があります。IP アドレスは、TelePresence Conductor 内のロケーションで設定された IP アドレスに対応している必要があります。ロケーションは、インスタントまたは CMR/スケジュール済み、あるいは両方の会議タイプに専用にすることもできます。両方の会議タイプがそのロケーションに対して有効にされている場合、そのロケーションには 2 つの IP アドレスが必要です（図 3-12）。

さまざまな異なる会議タイプおよびロケーションに対応するため、TelePresence Conductor には最大 64 個の IP アドレスを設定できます。

（注） 各 TelePresence Conductor ノードに、IP アドレスの固有のセットが必要になります。

図 3-12　TelePresence Conductor のロケーションおよび Unified CM IP アドレス

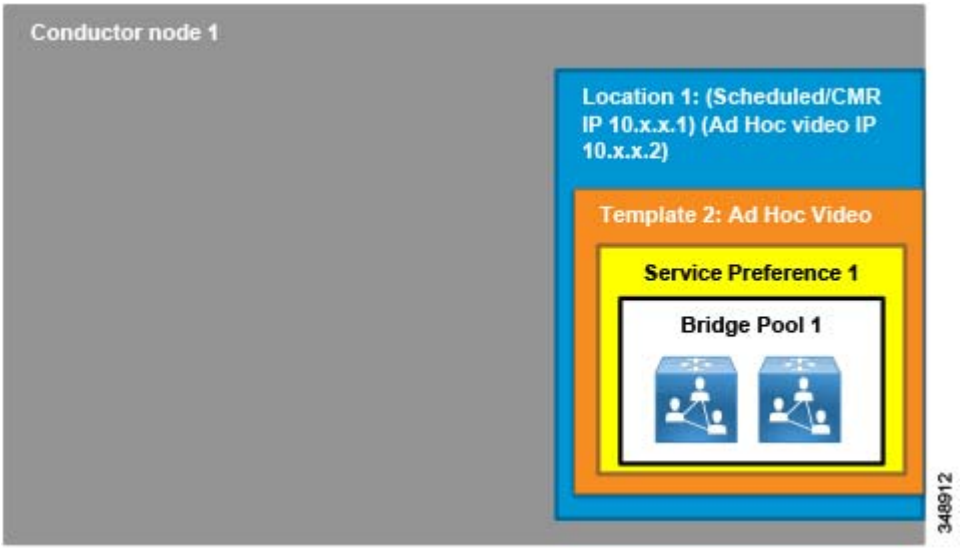


TelePresence Conductor でのインスタント会議の導入タスク

IP アドレスを TelePresence Conductor に追加し、TelePresence Server をブリッジ プールに割り当てて、ブリッジ プールをサービス設定に追加したら、インスタント会議の最初のテンプレートを作成できます。参加者によって適切なリソースが使用されるように、各テンプレートに関連する品質設定を設定する必要があります。たとえば、音声テンプレートをモノラル音声のみ（ビデオもコンテンツもなし）に設定する必要があります。

図 3-13 には、インスタント ビデオ会議を有効にするために、設定する必要がある要素が示されています。図 3-12 に示されているように、インスタント サービスの各タイプ（ビデオおよび音声）には、固有のロケーションとテンプレートが必要になります。

図 3-13　TelePresence Conductor ビデオ画面ライセンスのロケーションとインスタント テンプレート



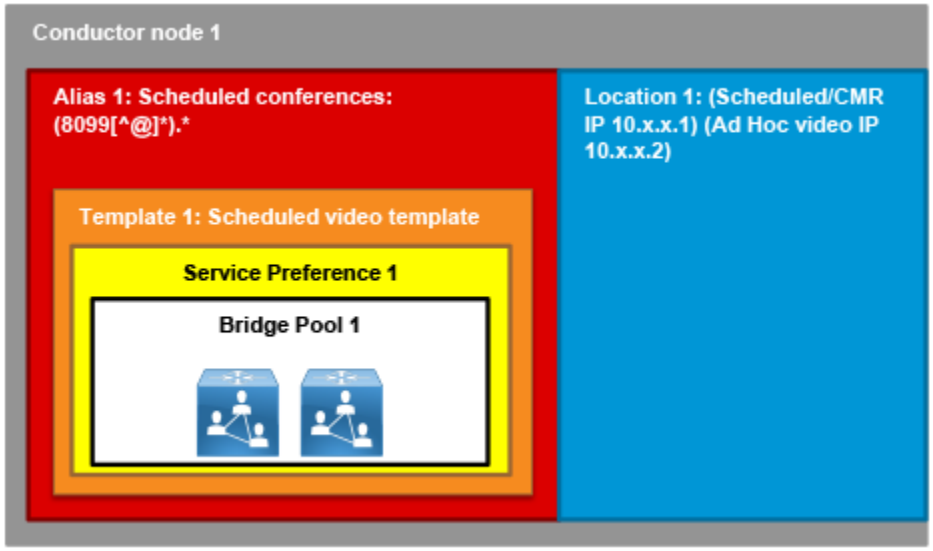
各インスタント会議のテンプレートに固有のロケーションを作成します。1 つのロケーションが、インスタント テンプレートとスケジュール済み/CMR 会議の両方に使用されることがあります。インスタント会議の場合、最も重要なロケーション設定パラメータは、インスタント会議テンプレートとインスタント会議専用の IP アドレスの 2 つです。Unified CM は、この IP アドレスを使用して、インスタント会議を作成するため要求を TelePresence Conductor に送信します。そして、TelePresence Conductor は、テンプレートを使用して、作成された会議の最大品質を決定します。

TelePresence Conductor でのスケジュール済み会議の導入タスク

スケジュール済み会議は、スケジュールできるように設定されたテンプレートを介して有効にされます。複数のテンプレートを設定することがあります。たとえば、マルチ画面システム用に設定された 2 番目のテンプレートを作成する必要がある場合があります。参加者によって適切なリソースが使用されるように、これらのテンプレートのそれぞれに関連する品質設定を設定する必要があります。

図 3-14 に、スケジュール済み会議を有効にするために、設定する必要がある要素を示します。

図 3-14　TelePresence Conductor スケジュール済みテンプレート



TelePresence Conductor は、会議エイリアスを使用して、ロケーションへの着信コール用に関連する会議テンプレートを選択します。エイリアスは正規表現を使用し、着信番号に基づいてマッチングできます。着信番号範囲は、TelePresence Conductor ランデブー IP アドレス（後続の手順で設定）を使用して SIP トランクに割り当てられる Unified CM ルート パターンによって制限されます。Unified CM は SIP トランクに広範な数値を指定できますが、TelePresence Conductor エイリアスは、この範囲をより小さなセグメントに分けるために使用されることがあります。分けられたセグメントのそれぞれは異なるテンプレートに使用されることもあります。これは、各エイリアスの数値範囲の部分のみに一致する正規表現を使用することによって、実行されます。

個人向けマルチパーティ会議用に TelePresence Conductor 内にロケーションを作成します。1 つの設定されたロケーションが、インスタント テンプレートとスケジュール済み会議の両方に使用されることがあります。スケジュール済み会議の場合、最も重要なロケーション設定パラメータは、[ランデブー IP アドレス（Rendezvous IP address）] です。Unified CM は、この IP アドレスを使用して、コール シグナリングを CMR およびスケジュール済みコール用の TelePresence Conductor に送信します。TelePresence Conductor からの発信ダイヤリングを容易にするため、これらのコールを受信する Unified CM コール処理サブスクライバ ノードの IP アドレスを使用して、最大 3 つのトランク IP アドレスをロケーションに追加します。

適切な SIP トランクへの発信コールをルーティングするには、関連するロケーションを CMR およびスケジュール済み会議に使用されるブリッジ プールに割り当てます。

要約

上記の導入タスクを完了すると、TelePresence Conductor は Unified CM に追加する準備が整います。

4. スケジュール済み会議とスケジュールされない会議用に Unified CM を有効にする

このセクションでは、スケジュール済み会議とスケジュールされない会議用に Unified CM を有効にするために必要な主なタスクについて説明します。

概要

インスタント会議用に Unified CM を有効にする導入タスク：

1. **Standard SIP Profile for TelePresence Conductor** という名前で新規 SIP プロファイルを作成します。
2. 3 つの SIP トランクを作成し、それぞれの SIP トランクを、インスタント会議のそれぞれのタイプの TelePresence Conductor ロケーションに設定された関連する IP アドレスを指すように設定します。
   - インスタント音声個人向けマルチパーティ SIP トランク
   - インスタント ビデオ個人向けマルチパーティ SIP トランク

   この手順は、各 TelePresence Conductor ノードに対して繰り返す必要があります。たとえば、3 つの TelePresence Conductor ノードがある場合、2 つの SIP トランクが設定された 3 つのセット（それぞれの TelePresence Conductor ノード対して 2 つで 1 セット）が存在している必要があります。
3. 2 つの会議ブリッジを作成し、SIP トランク（タスク 2 で設定済み）をそれぞれに追加します。各会議ブリッジには、関連するトランクが含まれている必要があります。
   - インスタント音声個人向けマルチパーティ会議ブリッジ
   - インスタント ビデオ個人向けマルチパーティ会議ブリッジ

   API を使用するために TelePresence Conductor で作成したユーザ名とパスワードを指定して各会議ブリッジを設定します。

   この手順は、各 TelePresence Conductor ノードに対して繰り返す必要があります。たとえば、3 つの TelePresence Conductor ノードがある場合、2 つの 会議ブリッジが設定された 3 つのセット（それぞれの TelePresence Conductor ノード対して 2 つで 1 セット）が存在している必要があります。
4. 2 つのメディア リソース グループ（MRG）を作成します。
   - インスタント音声個人向けマルチパーティ MRG
   - インスタント ビデオ個人向けマルチパーティ MRG

   マッチング タイプのすべての会議ブリッジ（TelePresence Conductor ノードごとに 1 つ）を関連する MRG に追加します。3 つの TelePresence Conductor ノードを使用している場合、各 MRG には 3 つの会議ブリッジが必要です。それぞれは、各ノード上の関連する IP アドレスの同じインスタント テンプレートを指します。
5. 2 つのメディア リソース グループ リスト（MRGL）を作成し、1 つの MRG をそれぞれに追加します。
   - インスタント音声個人向けマルチパーティ MRGL
   - インスタント ビデオ個人向けマルチパーティ MRGL

   エンドポイントによるインスタント会議の使用を許可するには、適切な MRGL をデバイス プールまたはデバイス自体に割り当てます。

CMR およびスケジュール済み会議用に Unified CM を有効にする導入タスク：

6. SIP トランクを作成し、その SIP トランクが、TelePresence Conductor ロケーションの [ランデブー IP アドレス（Rendezvous IP address）] フィールドに設定された関連する IP アドレスを指すように設定します。

   CMR およびスケジュール済み個人向けマルチパーティ会議（ST_CONDUCTOR_PM_CMR_SCHED1-1）

   この手順は、各 TelePresence Conductor ノードに対して繰り返す必要があります。たとえば、3 つの TelePresence Conductor ノードがある場合、設定された 3 つの SIP トランク（それぞれの TelePresence Conductor に対して 1 つ）存在している必要があります。

7. ルート グループを作成します。

   CMR およびスケジュール済み個人向けマルチパーティのルート グループ（MULTIPARTY_CMR_SCHED）

   すべての SIP トランクをルート グループに追加します。3 つの TelePresence Conductor ノードを使用している場合、ルート グループには 3 つの SIP トランクが必要です。それぞれは、各 TelePresence Conductor ノード上の関連する IP アドレスを指します。

8. ルート リストを作成し、ルート グループをそれに追加します。

   CMR およびスケジュール済み個人向けマルチパーティのルート リスト（RL_PM_CMR_SCHED）

9. 以前に作成した TelePresence Conductor で設定されたスケジュール済みエイリアス（8099[12]XXX）に一致するルート パターンを作成します。CMR を設定する場合、さらに追加のルート パターンが必要になります。それらについては、「6. Cisco Collaboration Meeting Rooms の導入」（P.3-41）のセクションで説明します。

導入上の考慮事項

Unified CM は、コールをルーティングする方法を決定し、設定に基づいて会議に使用する TelePresence Conductor テンプレートを選択するロジックの最初のポイントになります。Unified CM でのインスタント会議の設定手順と CMR/スケジュール済み会議の設定手順は異なります。これは、それぞれのタイプの会議に参加するためのメカニズムが異なるためです。

（注）　インスタント会議を開始するために使用するエンドポイントには、会議ボタンが必要になります。会議ボタンがないエンドポイントもインスタント会議に参加することはできますが、会議ボタンがあるエンドポイントに、会議に追加してもらう必要があります。

インスタントおよび無期限の会議

図 3-15　　インスタント会議用の Unified CM の内部設定フロー

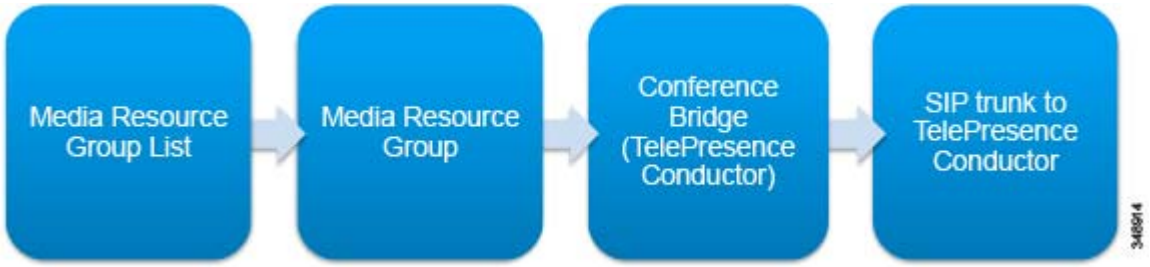
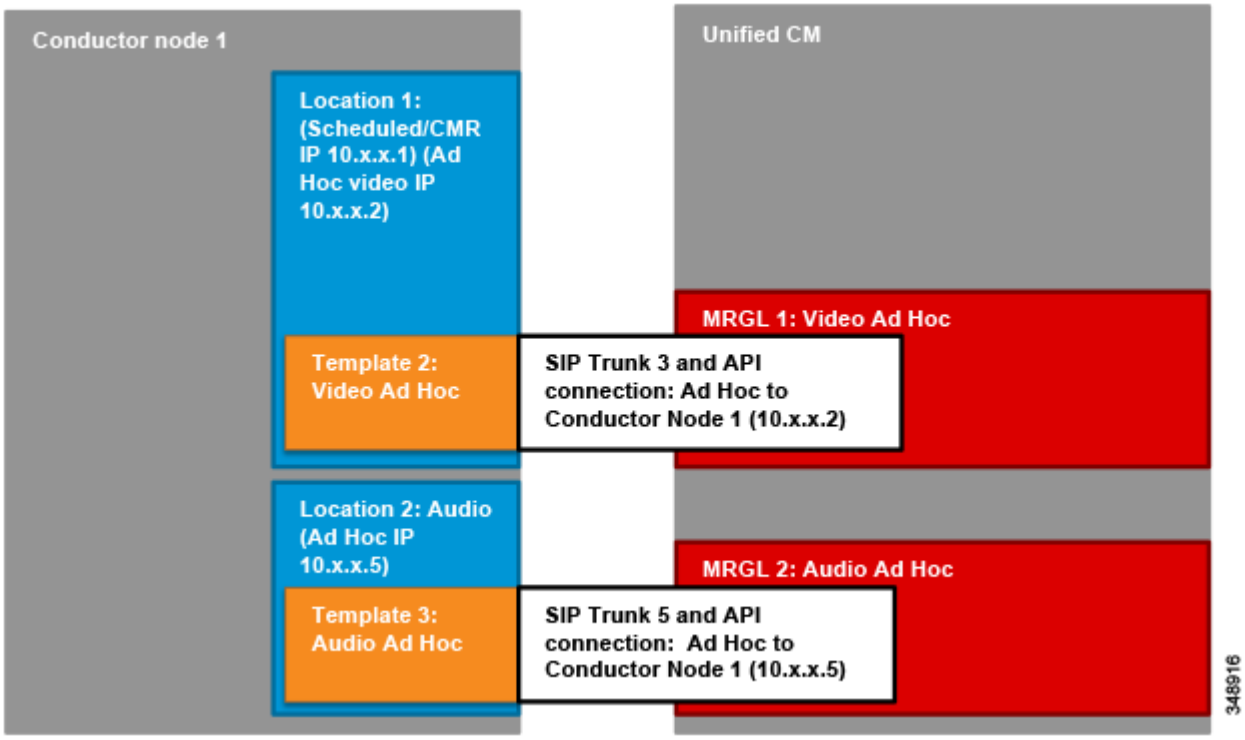


図 3-16　　CMR およびスケジュール済み会議用の Unified CM の内部設定フロー

インスタント会議用に Unified CM を有効にする導入タスク

Unified CM 会議と TelePresence Conductor 設定の関係を理解することが重要です。この展開の場合、TelePresence Conductor では 2 つのロケーションが設定され、それぞれでインスタント会議用にアドホック IP アドレスが追加されました。これらの IP アドレスのいずれかに送信されるすべてのコールは、そのロケーションで設定された会議テンプレートを使用します。コールを正しくルーティングするには、Unified CM のどの SIP トランクが、TelePresence Conductor 内で設定されたどの IP アドレスを指す必要があるかを理解することが重要になります。

図 3-17　Unified CM と TelePresence Conductor のインスタント関係



それぞれのタイプのインスタント会議は、TelePresence Conductor と通信するために Unified CM で設定された固有の SIP トランクと会議ブリッジを必要とします。各 SIP トランクは、1 つのインスタント会議にしか使用できません。CMR やスケジュール済み会議には独自の SIP トランクが必要になります。各 TelePresence Conductor ノードも、SIP トランクと会議ブリッジの固有のセットを必要とします。

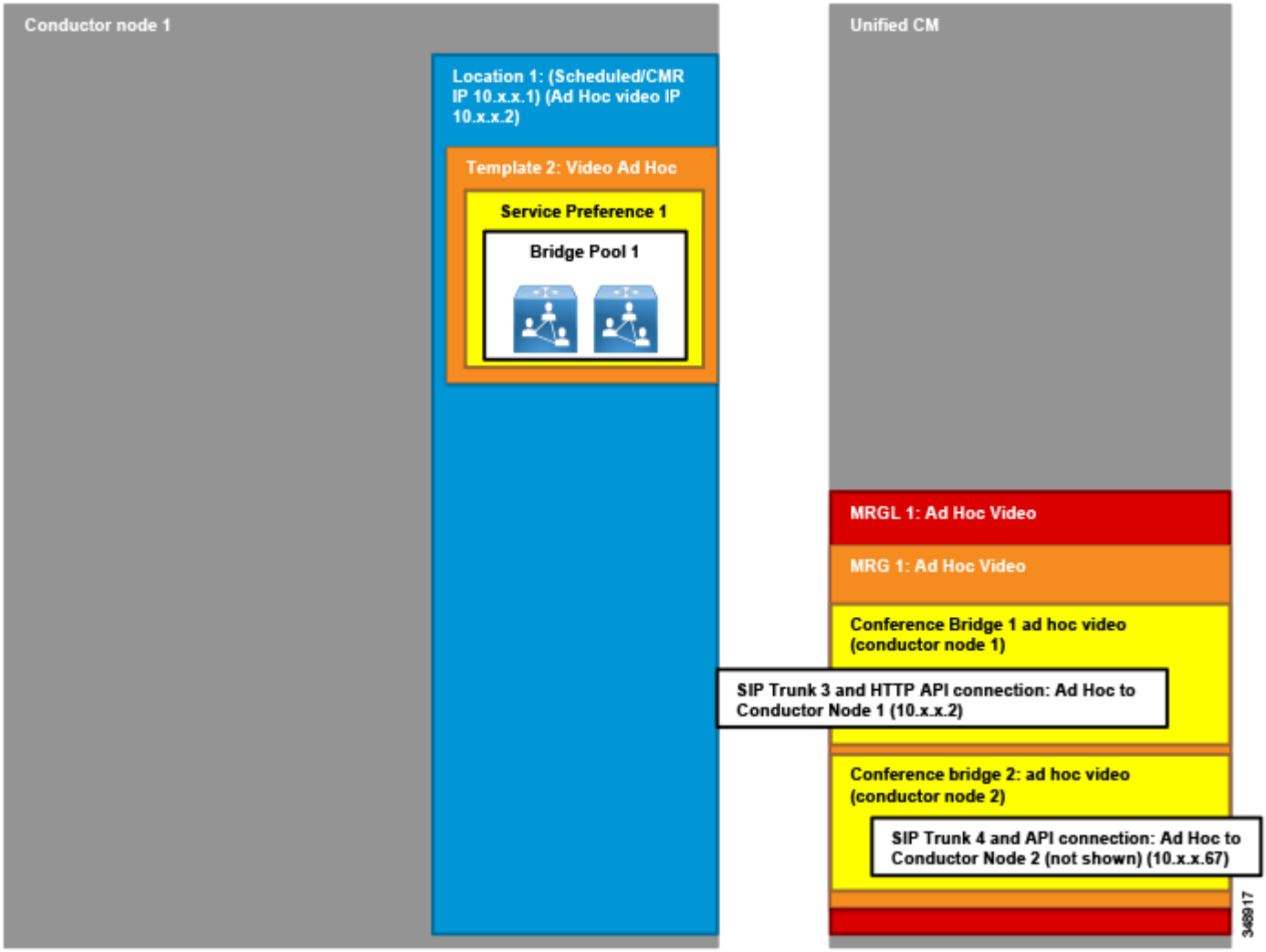
TelePresence Conductor への SIP トランクは、すべてのシナリオ内でコールをサポートするためにカスタマイズされた SIP プロファイルを必要とします。SIP プロファイルを作成するには、**Standard SIP Profile for TelePresence Conferencing** をコピーして、そのコピーに **Standard SIP Profile for TelePresence Conductor** という名前を付け、表 3-4 に示されているように設定を変更します。

表 3-4　SIP プロファイルの設定

設定	値	コメント
[インバイトのタイムアウト値(秒)(Timer Invite Expires (seconds))]	30	トランクのタイマーは、TelePresence Conductor のタイマーと同じ時間で有効期限が切れます。
[音声コールとビデオコールに対する早期オファーサポート(Early Offer support for voice and video calls)]	[ベストエフォート(MTPの挿入なし)(Best Effort (no MTP inserted))]	これは、すべての Unified CM トランクに対して推奨される設定です。ベスト エフォートの早期オファー トランクでは、早期オファーを作成するために MTP を使用しません。コールに使用するデバイスに応じて、早期オファーか遅延オファーのいずれかを使用して発信 SIP トランク コールを開始します。この設計では、発信コールは常に早期オファーを使用します。

SIP トランクは、Unified CM に SIP トラフィックをルーティングする場所を伝達します。インスタント会議の場合、SIP トランクは Unified CM に API 要求の宛先も伝達し、それらは会議ブリッジ設定で使用されます。TelePresence Conductor に接続された SIP トランクは、セキュリティで保護されるように設定できますが、このガイドでは、セキュリティで保護されないように設定されることが想定されています。

図 3-18　　Unified CM インスタント構成



会議ブリッジ設定によって、2 つの重要な情報（TelePresence Conductor と通信するための API クレデンシャルとその通信の宛先アドレス）が Unified CM に通知されます。ユーザ名とパスワードは、TelePresence Conductor を指すそれぞれの会議ブリッジで同じものを使用できます。これらのクレデンシャルは、TelePresence Conductor 設定で設定されたクレデンシャルに一致している必要があります。会議ブリッジで設定された SIP トランクは、HTTP API トラフィックの送信先を Unified CM に示します。各 SIP トランクは、表 3-5 に示す設定で設定します。

表 3-5　　インスタント会議用の SIP トランク設定

設定	値	コメント
[名前(Name)]	[ST_CONDUCTOR_ADHOC_AUDIO1-1]	プレフィックス「ST_」を付けて、同じテーブル内に格納された他のデバイスと名前がコリジョンしないようにします。 名前の残りの部分で、会議タイプとトランクが指す TelePresence Conductor ノードを識別します。
[説明(Description)]		わかりやすい説明。
[デバイスプール(Device Pool)]	[Trunks_and_Apps]	中央トランクの共通デバイス プール
[メディアリソースグループリスト(Media Resource Group List)]	<なし>	デバイス プールで定義された MRGL を使用します
[AARグループ(AAR Group)]	[デフォルト(Default)]	すべての場所で同じ
[発呼側名にUTF-8を転送(Transmit UTF-8 for Calling Party Name)]	オン	この設定によって、ASCII 呼び出し表示を、UTF-8 文字をサポートするデバイスに転送できます。
[PSTNアクセス(PSTN Access)]	オフ	
[すべてのアクティブな Unified CM ノードで実行(Run on All Active Unified CM Nodes)]	オン	この設定は、すべての SIP トランクに推奨されます。この設定によって、SIP への発信コールは、Unified CM コール処理サブスクライバ間のクラスタ内制御シグナリングを必要としなくなります。
着信コール		
[コーリングサーチスペース(Calling Search Space)]	[TelePresenceConferencing]	コール制御の章で定義されているとおり
[AARコーリングサーチスペース(AAR Calling Search Space)]	[PSTNReroute]	
アウトバンド コール		
[デバイスプールの着信側トランスフォーメーションCSSを使用(Use Device Pool Called Party Transformation CSS)]	オン	
[デバイスプールの発呼側トランスフォーメーションCSSを使用(Use Device Pool Calling Party Transformation CSS)]	オン	
SIP 情報		
[接続先(Destination)]	10.X.X.2	TelePresence Conductor 音声アドホック IP アドレス

表 3-5　インスタント会議用の SIP トランク設定（続き）

設定	値	コメント
[SIPトランクセキュリティプロファイル（SIP Trunk Security Profile）]	[非セキュアSIPトランクプロファイル（Non Secure SIP Trunk Profile）]	デフォルトの SIP トランク セキュリティ プロファイル
[SIP プロファイル（SIP Profile）]	TelePresence Conductor 用 標準 SIP プロファイル	上記で作成した SIP プロファイルを使用します

すべての会議ブリッジを設定したら、それらをメディア リソース グループ（MRG）に追加できます。各メディア リソース グループは、インスタント会議のいずれかのタイプを表し、各 TelePresence Conductor ノードの会議ブリッジが 1 つ含まれている必要があります。これにより、1 つの TelePresence ノードと通信できなくなった場合に、コールを別のノードにルーティングできるようになります。

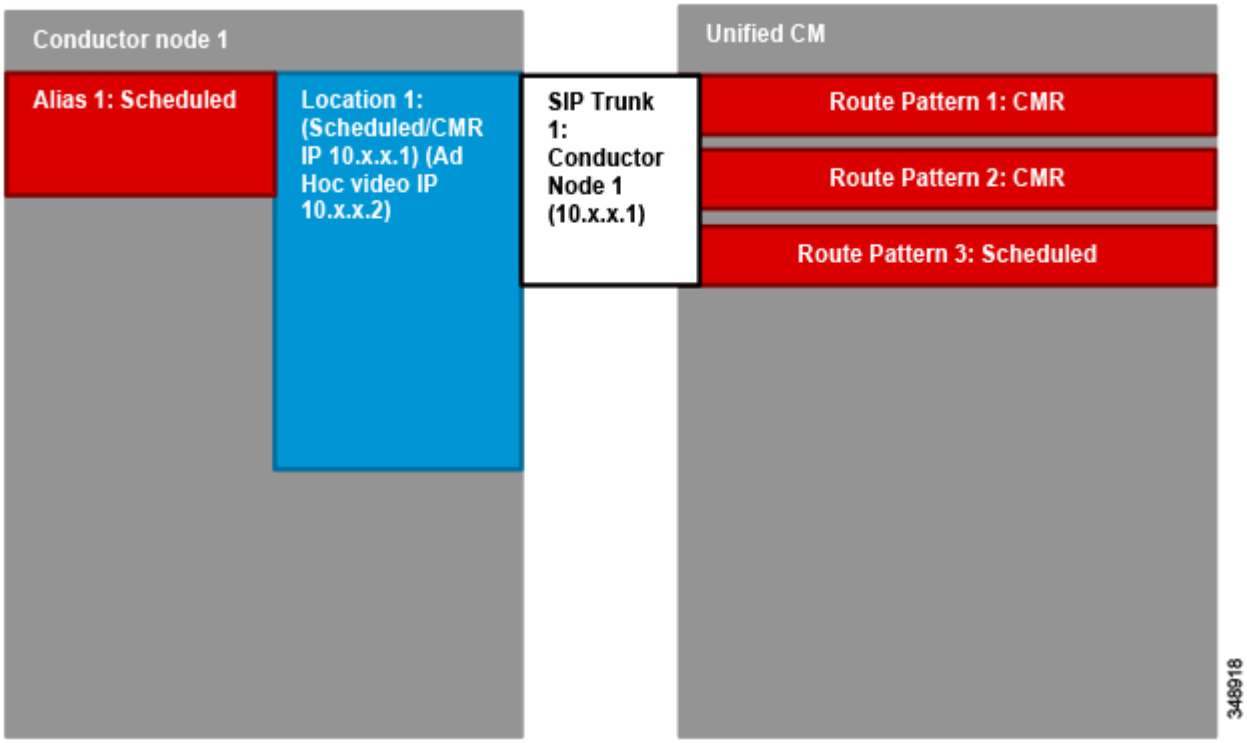
各メディア リソース グループは、独自のメディア リソース グループ リスト（MRGL）に追加できます。メディア リソース グループ リストは、Unified CM 内のデバイスまたはデバイス プールに割り当てることができます。また、会議ボタンを使用して、ポイントツーポイント コールから会議コールにそれらのデバイスをエスカレートするときに使用できます。

全体で、2 つの MRGL を設定できます。1 つは、インスタント音声個人向けマルチパーティ会議用で、もう 1 つは、インスタント ビデオ個人向けマルチパーティ会議用です。これら 2 つの MRGL は、それぞれ TelePresence Conductor 内で設定された異なるロケーションを指し、そのロケーション内で設定されたインスタント テンプレートを参照している必要があります。

CMR およびスケジュール済み会議用に Unified CM を有効にする導入タスク

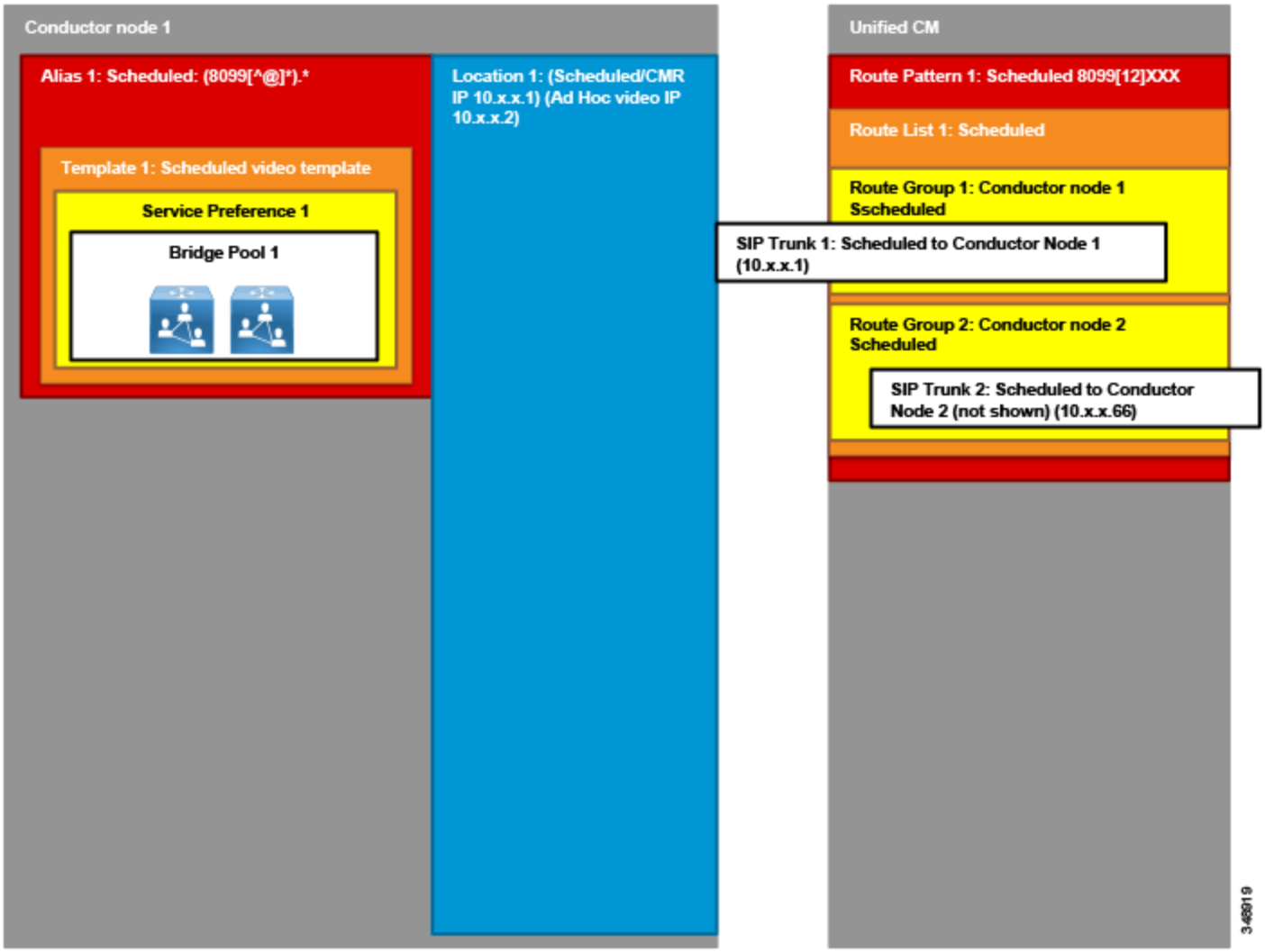
CMR およびスケジュール済み会議は、インスタント会議と類似した方法で Unified CM で設定しますが、メディア リソースではなく、ダイヤル プランを設定する必要があります。

図 3-19　Unified CM と TelePresence Conductor CMR およびスケジュール済みの関係



最初に、展開用に作成した TelePresence Conductor のロケーションに設定された関連する IP アドレスを使用して TelePresence Conductor に接続するように SIP トランクを設定します。各 TelePresence Conductor ノードに固有の SIP トランクが必要になります。CMR とスケジュール済み会議に対して、表 3-5 に示す設定でインスタント会議用に作成した同じ SIP プロファイルを使用します。

図 3-20　Unified CM CMR およびスケジュール済み会議



すべての SIP トランクを設定した後、それら 1 つ 1 つにルート グループを作成します。

特定の会議タイプのルート グループを固有のルート リストに追加します。TelePresence Conductor ロケーションごとに 1 つのルート リストが必要です。コールがそのルートを指すルート パターンに一致する場合に、ルート リストが選択されます。

コールを関連する SIP トランクにルーティングし、その結果として TelePresence Conductor 内の関連するロケーションにルーティングするには、ルート リストのルート パターンを設定します。ルート パターンは、表 3-6 に示す、必要なテンプレート用に設定されたエイリアス範囲に一致する必要があります。

表 3-6　スケジュール済み会議ルート リストのルート パターン

パターン	パーティション	ゲートウェイまたはルート リスト	説明
8099[12]XXX	ESN	RL_PM_CMR_SCHED	スケジュール済み個人向けマルチパーティ エイリアス範囲に一致するパターン

要約

上記の導入タスクを完了すると、Unified CM は TelePresence Conductor と通信できるようになります。

5. 会議用の TelePresence Management Suite の有効化

このセクションでは、TelePresence Conductor を使用して会議をスケジュールするように Cisco TMS を設定するために必要な主なタスクについて説明します。

概要

スケジュール済み会議に関する Cisco TMS の導入タスク：

1. 各 TelePresence Conductor クラスタから 1 つの TelePresence Conductor を追加します。
2. TelePresence Conductor の背後に TelePresence Server を追加します。
3. TelePresence Conductor およびすべての追加した TelePresence Server の更新を実行します。
4. スケジュール済みエイリアスを Cisco TMS で作成します。
5. Cisco TMS によって生成された正規表現を使用して、会議エイリアスを TelePresence Conductor 内に作成します。このドキュメントの前の箇所で実行したスケジューリングに割り当てられた会議テンプレートを使用します。
6. Cisco TMS 内の TelePresence Conductor の更新を実行します。
7. Cisco TMS 内の TelePresence Conductor 設定を編集します。[予約の許可（Allow booking）] および [着信/送信SIP URIダイヤルの許可（Allow incoming and outgoing SIP URI Dialing）] を選択し、両方向の H.323 ダイヤルを無効にします。
8. Cisco TMS 内の TelePresence Conductor 拡張設定を編集し、Unified CM 内で設定されたルート パターン範囲を超えないように数量を設定します。
9. Cisco TMS 設定の会議設定を編集し、[ルーティングの優先MCUタイプ（Preferred MCU Type in Routing）] を [Cisco TelePresence Conductor] に設定します。

導入上の考慮事項

Cisco TMS は、会議展開内で以下のサービスを提供します。

- スケジューリングおよび会議制御機能（スケジュール済み会議用）の TelePresence Server 上での直接実行。
- TelePresence Conductor と連動する個人の Collaboration Meeting Rooms（CMR）のプロビジョニングおよびモニタリングの有効化（セクション6. Cisco Collaboration Meeting Rooms の導入を参照してください）。
- CMR Hybrid のリソースの管理と割り当て（これについては、後続のセクションで説明します）。

Cisco TMS でのスケジュールおよびスケジュール済み会議の会議制御を許可するには、1 つの TelePresence Conductor ノードを各 TelePresence Conductor クラスタから追加します。TelePresence Server も Cisco TMS に追加する必要があります。

Cisco TMS および TelePresence Conductor は、同様のエイリアスで設定する必要があります。また、これらは、スケジュールされたコールを配置する場所を決定するために Cisco TMS によって使用されます。カスケーディングが無効の場合（専用 TelePresence サーバ展開を使用している場合は無効ではありません）、会議は単一の TelePresence Server のサイズを超えることはできません。

スケジュール済み会議に関する Cisco TMS の導入タスク

各 TelePresence Conductor クラスタから 1 つの TelePresence Conductor を Cisco TMS に追加します。それらを適切なフォルダに追加し、TelePresence Conductor で設定された管理者アカウントを使用して適切な IP ゾーンに割り当てます。Cisco TMS に設定された各 TelePresence Conductor に対して、表 3-7 にリストされているようにパラメータを設定します。

表 3-7　TelePresence Conductor の Cisco TMS パラメータ設定

設定	値	コメント
[IPゾーン（IP Zone）]	地域 IP ゾーン	この設定は、Cisco TMS にデバイスの物理的な場所を知らせます
[ユーザ名（Username）]	[TMSadmin]	この設定は、TelePresence Conductor で設定されたユーザ名に一致している必要があります
[パスワード（Password）]	<パスワード>	
[使用タイプ（Usage Type）]	その他	

TelePresence Conductor を追加した後、前述の TelePresence Conductor と同様の方法で、各 TelePresence Server を Cisco TMS に追加します。すべての TelePresence Server を追加したら、TelePresence Conductor で更新を実行し、追加したすべての TelePresence Server でも更新します。

[TelePresence Conductor] タブで、スケジュールされたコールに使用する Cisco TMS のエイリアスを作成します。表 3-8 に示されているように、下の方の設定は、読み取り専用のため、[保存（Save）] をクリックした後にのみ表示されます。

表 3-8　TelePresence Conductor の Cisco TMS エイリアス設定

設定	値	コメント
[名前（Name）]	[スケジュール済み会議（Scheduled meeting）]	エイリアスに名前を指定します（たとえば、「スケジュール済み会議」）。
[エイリアスパターン（Alias Pattern）]	[8099%]	パターンは固定値にすることも、変数（% で示されます）を含めることもできます。エイリアス パターンは、Unified CM のルート パターンに一致している必要があります。 エイリアスの可変部分は、[システム（Systems）] > [ナビゲータ（Navigator）] > [TelePresence Conductorの選択（select the TelePresence Conductor）] > [拡張設定（Extended Settings）] で、TelePresence Conductor 用に設定された [数字IDベース（Numeric ID Base）] から Cisco TMS によって生成されることに注意してください。
[プライオリティ（Priority）]	[1]	エイリアスにプライオリティを指定します。最も低い数値を持つエイリアスが、最も高いプライオリティになります。Cisco TMS が会議を作成するときに、そのエイリアスが最初に使用されます。そのエイリアスに使用可能なリソースがない場合、次に高い数値を持つエイリアスが使用されます。 優先順位は 0 ～ 65535 の間の任意の数値に設定できます。
[説明（Description）]	[デフォルトのスケジュール済み会議（Default scheduled conference）]	このエイリアスの説明を入力します。
[マルチスクリーンを選択（Prefer for Multiscreen）]	[いいえ（No）]	イマーシブ TelePresence システムを含む会議にエイリアスを選択した場合、Cisco TMS はこのフィールドがチェックされているエイリアスを使用します。最も高いプライオリティを持つエイリアスが最初に選択されます。 すべてのイマーシブ エイリアスが使用されている場合は、会議にイマーシブ以外のエイリアスが使用されます。 チェックする場合は、このエイリアスが使用するように設定された TelePresence Conductor 会議テンプレートの [マルチスクリーンの許可（Allow multiscreen）] が [はい（Yes）] に設定されていることを確認してください。
[予約の許可（Allow booking）]	[はい（Yes）]	[いいえ（No）] が選択された場合、このエイリアスは Cisco TMS の予約では使用されません。 多数の予約が存在し、それらが多すぎて削除できない特定のエイリアスの使用を停止するときに、この設定を使用できます。この設定を使用して予約を無効にすると、最後の予約が実行された時点で、エイリアスは削除できるようになります。
[WebExでの予約の許可（Allow Booking with WebEx）]	[はい（Yes）]	[はい（Yes）] に設定すると、このエイリアスを Cisco Collaboration Meeting Rooms（CMR）Hybrid を含む予約で使用できます。

表 3-8　TelePresence Conductor の Cisco TMS エイリアス設定（続き）

設定	値	コメント
[会議ごとの最大参加者（Max Participants per Conference）]	該当なし	このエイリアスで会議を予約した場合、この数値よりも多い参加者が選択されると、会議を保存できなくなります。 この数値は理論上の最大値です。会議に参加できる実際の人数は、関連する TelePresence Conductor の会議テンプレートが設定される方法に応じて、少なくなる可能性があります。 このフィールドは、TelePresence Conductor に対応するエイリアスが存在する場合にのみ、有効になります。
[参加者ごとの最大画面（Max Screens per Participant）]	該当なし	このエイリアスの参加者ごとの画面の最大数。 このフィールドは、TelePresence Conductor に対応するエイリアスが存在する場合にのみ、有効になります。
[正規表現（Regular Expression）]	該当なし	TelePresence Conductor で設定する必要のあるエイリアスの正規表現。
[サービス設定（Service Preference）]	該当なし	このエイリアスがリンクされるサービス設定。 TelePresence Conductor に対応するエイリアスが存在しない場合、このフィールドには**何も**表示されません。

TelePresence Conductor で対応するエイリアスを作成します。最初に、Cisco TMS の [TelePresence Conductor] タブの下のエイリアス [正規表現（Regular Expression）] フィールドで生成された正規表現をコピーします。表 3-8 に示されている例では、生成されたエイリアスは **(8099[^@]*).*** になります。

TelePresence Conductor で、新しい会議エイリアスを作成し、表 3-9 に示されているように設定します。

表 3-9　TelePresence Conductor エイリアス

設定	値	コメント
[名前（Name）]	[デフォルトのスケジュール済み会議（Default scheduled meeting）]	エイリアスに名前を指定します（たとえば、「スケジュール済み会議」）。
[着信エイリアス（Incoming alias）]	(8099[^@]*).*	Cisco TMS からコピーした正規表現を貼り付けます。
[会議名（Conference name）]	\1	着信エイリアスから会議名に変更する方法を定義する正規表現の置換文字列（たとえば、「\1」）を入力します。 静的値をここに入力すると、同じエイリアスの同時使用は許可されなくなります。エイリアス パターンに動的な部分が含まれている場合、ここに入力する正規表現の文字列にその部分が反映されているか確認します。 このフィールドで定義される TelePresence Conductor の会議名は、Cisco TMS の会議タイトルとは関係ないことに注意してください。

表 3-9　TelePresence Conductor エイリアス（続き）

設定	値	コメント
[プライオリティ（Priority）]	[1]	この会議エイリアスのプライオリティを入力します。ダイヤルされるエイリアスが複数の会議エイリアスに一致する場合に、このプライオリティが使用されます。このような場合、最も高いプライオリティ（0 に最も近い値）を持つ会議エイリアスが使用されます。
[会議テンプレート（Conference template）]	スケジュール済み個人向けマルチパーティ 720p HD ビデオ テンプレート	[TelePresence Conductor構成（TelePresence Conductor configuration）] セクションでスケジュールするために割り当てた会議テンプレートのいずれかを選択します。
[ロールタイプ（Role Type）]	[参加者（Participant）]	この設定は、この会議エイリアスを使用して会議にダイヤルする発信者に割り当てられる特権を決定します。選択可能なオプションは、選択されたテンプレートによって決定します。
[会議の作成の許可（Allow conference to be created）]	[いいえ（No）]	この設定は、この会議エイリアスをダイヤルする参加者が会議を作成できるかどうかを決定します。スケジュール済み会議は常に Cisco TMS によって作成されるので、この設定を有効にしないでください。

Cisco TMS 内で TelePresence Conductor を選択し、デバイスの [更新の実行（Force refresh）] を選択します。追加情報が、[TelePresence Conductor] タブ内の [サービス設定（Service Preferences）] の下にリストされます。

TelePresence Conductor は、サービス設定の総容量を Cisco TMS にレポートします。[容量調整（Capacity Adjustment）] 設定によって、この [サービス設定（Service Preferences）] で会議のスケジュールに使用できる総容量のパーセンテージを指定できます。

スケジュール専用に予約したブリッジ プールを使用する場合、この設定は変更しないでください。一方、インスタントおよび CMR 会議がスケジュールに使用されるブリッジ プールを共有する場合、パーセンテージを 100 % よりも少なく設定することによって、スケジュールされない会議のために容量を確保しておきます。

100 % よりも高いパーセンテージを設定することもできます。使用する容量よりも多くの容量をユーザが予約する傾向がある（たとえば、5 個しか使用されないのに 10 個の会議用ダイヤルインを予約する）場合、[容量調整（Capacity Adjustment）] を 120 % 以上に設定できます。

スケジュール済みコールに TelePresence Conductor を使用するには、Cisco TMS 内の TelePresence Conductor の設定を編集する必要があります。H.323 ダイヤルは両方向で無効、[予約の許可（Allow booking）] は有効、SIP ダイヤルは両方向で有効にする必要があります。

以前に Cisco TMS のエイリアスでワイルド カードが設定されていた場合、ワイルド カードの代わりに使用される数値範囲は、スケジュール済み会議の数値範囲が Unified CM で設定されている範囲に一致するように設定する必要があります。表 3-10 にリストされているように、Cisco TMS の TelePresence Conductor の [拡張設定（Extended Settings）] を編集します。数字 ID は、Unified CM から TelePresence Conductor へのトランクに設定されたルート パターンに一致している必要があります。

表 3-10　TelePresence Conductor の拡張設定

設定	値	コメント
[数字IDベース（Numeric ID Base）]	[1000]	エイリアスの変数部分を作成する際に Cisco TMS が使用する最初の数値。エイリアスの非変数部分とこの数値の組み合わせは、スケジュール済み会議にダイヤルする参加者によって使用されるダイヤル文字列になります（例：80991000）。
[数字IDステップ（Numeric ID Step）]	[1]	Cisco TMS は、エイリアスが重複しないように、この数値を [数字IDベース（Numeric ID Base）] に追加します。会議が終了すると、エイリアスは新しい会議で使用できるようになります。
[数字IDの桁数（Numeric ID Quantity）]	[1999]	Cisco TMS が [数字IDステップ（Numeric ID Step）] の増分を使用して [数字IDベース（Numeric ID Base）] から 数値を増やす回数。この数値は、最大値がスケジュールに割り当てられた範囲を超えないように設定する必要があります（80991000 ～ 80992999）。
[会議レイアウト（Conference Layout）]	デフォルト ビュー ファミリ	すべての会議のデフォルト レイアウトを設定します。
[ポートをスケジュール済み参加者の数に制限する（Limit Ports to Number of Scheduled Participants）]	オン	すべての会議に対して、ポートを音声およびビデオのスケジュール済み参加者の数（会議の予約時にスケジュールされた数）に制限します。この数値を超えて会議に参加することはできません。

スケジュールに TelePresence Conductor を使用するように Cisco TMS を設定することは重要です。それ以外の場合、スケジュールは失敗します。[管理ツール（Administrative Tools）] > [設定（Configuration）] > [会議設定（Conference Settings）] で、表 3-11 に示されているように設定を編集します。

表 3-11　Cisco TMS Conference 設定

設定	値	コメント
[ルーティングの優先 MCU タイプ（Preferred MCU Type in Routing）]	[Cisco TelePresence Conductor]	スケジュールする場合に、他のデバイスよりも TelePresence Server を優先します。

要約

上記の導入タスクを完了すると、Cisco TMS は、スケジュール済み会議のために TelePresence Conductor と通信するように設定されます。

6. Cisco Collaboration Meeting Rooms の導入

このセクションでは、Cisco Collaboration Meeting Rooms（CMR）を導入するために必要な主なタスクについて説明します。

概要

CMR のための Unified CM の導入タスク：

1. Unified CM と TelePresence Conductor の間に早期オファー SIP トランクを設定します。ここでは、以前に設定した SIP トランク ST_CONDUCTOR_PM_CMR_SCHED1-1 を使用します。
2. 関連トランクが含まれるルート リストを指定する CMR 数字エイリアスの新規ルート パターンを設定します。ここでは、以前に設定したルート リスト RL_PM_CMR_SCHED を使用します。
3. インポート済みグローバル ダイヤル プラン カタログ（例：ルート文字列 cmr.route）を作成し、一括管理ツール（BAT）を使用して CMR SIP URI をグローバル ダイヤル プラン カタログにインポートします。
4. タスク 2 で使用したルート リスト（RL_PM_CMR_SCHED）を指定する CMR URI のグローバル カタログのルート文字列で SIP ルート パターンを作成します。

CMR のための TelePresence Conductor の導入タスク：

5. 1 つ以上のブリッジ プールおよびサービス設定を設定します。共有スケジューリング モデルを使用する場合、スケジュールに使用される同じブリッジ プールのいずれかを使用します。または、専用モデルを使用する場合、スケジュールされない会議専用の新しいブリッジ プールを作成します。
6. TelePresence Conductor 内で読み取り/書き込みアクセス レベルと API アクセスを有効にした管理者アカウントを作成します。

CMR のための Cisco TMSPE の導入タスク：

7. Cisco TMSPE を Cisco TMS にインストールして、アクティブにします。
8. ユーザ グループ [エグゼクティブ（Executive）] と [マーケティング（Marketing）] を作成し、対応する AD グループに属するユーザを Active Directory からインポートします。
9. [TelePresence Conductor設定（TelePresence Conductor setting）] オプションを使用して、TelePresence Conductor ノードを 1 つだけ各クラスタから TMSPE に追加します。
10. 会議設定および会議エイリアスを定義する CMR テンプレートを作成し、必要に応じてデフォルト設定を変更します。
11. CMR を使用する権限を付与する CMR テンプレートを各ユーザ グループに割り当てます。

導入上の考慮事項

Cisco Collaboration Meeting Rooms（CMR）は、エンタープライズのデータセンターに配置される TelePresence インフラストラクチャに作成される無期限の会議に類似します。各 CMR には、ユーザが会議を開始するためにいつでも発信できるビデオ アドレスの固有のセットが存在します。これらのビデオ アドレスは、数字エイリアスまたは SIP URI の形式で指定できます。各 CMR は、個々のユーザに関連付けることができ、ユーザの Cisco TelePresence Management Suite Provisioning Extension（TMSPE）ポータルから作成することができます。

Cisco CMR は、参加者が位置している場所に関わりなく、TelePresence を使用して会議に参加する簡単な方法を提供します。すべてのユーザは、ラップトップ、テレプレゼンス会議室、デスクトップ エンドポイント、またはモバイルデバイスから同じ仮想会議室にダイヤルします。

CMR の導入には、Unified CM、TelePresence Conductor、および Cisco TMSPE の導入も必要です。以下のセクションでは、CMR の各コンポーネントの導入に関するプロセスの概要を説明します。

ヒント　CMR を開始する前に、会議エイリアスの形式（数字または SIP URI）を決定します。

CMR のための Unified CM の導入タスク

Unified CM の主な機能は、TelePresence Conductor へのコール ルーティング、および TelePresence Conductor からのコール ルーティングを処理する機能です。早期オファーで有効にされた SIP トランクを使用して、Unified CM を TelePresence Conductor に接続します（スケジュール済み会議用に以前に設定されたものと同じトランク（ST_CONDUCTOR_PM_CMR_SCHED1-1）を使用します）。ユーザが CMR 会議エイリアスにダイヤルすると、コールは SIP トランク経由で TelePresence Conductor に送信されます。同様に、TelePresence Conductor は、自動ダイヤル参加者用の SIP トランク経由で Unified CM にコールを送信できます。会議エイリアスには、2 つの形式（SIP URI と数字）があります。ダイヤル プラン設計には、CMR の数字エイリアスと SIP URI の両方のコール ルーティングを含める必要があります。ダイヤル プラン設計の詳細については、コール制御の章を参照してください。

Cisco Collaboration Meeting Rooms（CMR）は、個々のユーザに対して作成できます。CMR 数字エイリアスは、ユーザの DID 番号に基づかせることができます。表 3-12 には、コール制御の章のダイヤル プランのサンプルを使用した導入用の CMR 数字エイリアスの範囲が示されています。

表 3-12　CMR 数字エイリアスの範囲

サイト	+E.164 DID 範囲	CMR 数字エイリアスの範囲
SJC	+1 408 555 4XXX	8-004-4XXX
RTP	+1 919-555 1XXX	8-005-1XXX
RCD	+1 972 555 5XXX	8-006-5XXX

数字エイリアスでは、表 3-13 に示されているように、無期限の会議用の TelePresence Conductor ルート リストにルーティングする各サイトのルート パターンを設定します。

表 3-13　CMR 数字エイリアスのルート パターン設定

パターン	パーティション	ゲートウェイまたはルート リスト	説明
80044XXX	ESN	RL_PM_CMR_SCHED	SJC DID 範囲に一致するパターン
80051XXX	ESN	RL_PM_CMR_SCHED	RTP DID 範囲に一致するパターン
80065XXX	ESN	RL_PM_CMR_SCHED	RCD DID 範囲に一致するパターン

CMR 用の SIP URI では、ドメイン部分をエンド ユーザ ディレクトリ URI と同じにし、URI のユーザ部分を設定します（たとえば、*{username}*.cmr@ent-pa.com）。ディレクトリと CMR URI ダイヤルの両方に単一ドメインを使用すると、CMR が複数の Conductor システムまたはクラスタにホストされている場合に、ダイヤル プラン設計が簡略化されます。また、ユーザは、CMR を入力するために URI のユーザ部分しか入力する必要はありません。Unified CM は、ドメイン部分を自動的に追加してダイヤルを完成します。これは、ユーザ エクスペリエンスを大きく向上させます。

URI のコール ルーティングを設定するには、インポート済みグローバル ダイヤル プラン カタログ（例：ルート文字列 cmr.route）を作成します。次に、システム内のすべてのユーザの CMR SIP URI のリストを作成します（新規ユーザがシステムに追加されるたびに実行します）。また、一括管理ツール（BAT）を使用して URI をグローバル ダイヤル プラン カタログにインポートします。その後、表 3-14 に示されているように、無期限の会議用の TelePresence Conductor ルート リストにルーティングするグローバル カタログのルート文字列を使用して、ドメイン ルーティング SIP ルート パターンを設定します。

表 3-14　　CMR URI の SIP ルート パターン設定

パターン	パーティション	ゲートウェイまたはルート リスト
cmr.route	URI	RL_PM_CMR_SCHED

CMR のための TelePresence Conductor の導入タスク

TelePresence Conductor は、1 つ以上のブリッジ プールおよびサービス設定で設定する必要があります。Cisco TMSPE ポータルを使用して作成したすべての CMR は、この TelePresence Conductor にホストされます。TelePresence Conductor および Unified CM は、早期オファー SIP トランクを介して接続されます。共有リソース モデルを使用している場合、スケジュール済み会議用に TelePresence Conductor で以前に設定したブリッジ プールおよびサービス設定を CMR で再使用できます。それ以外の場合、CMR のインスタント会議用に TelePresence Conductor で以前に設定したブリッジ プールおよびサービス設定を使用します。また、TelePresence Conductor 内で読み取り/書き込みアクセス レベルと API アクセスを有効にした管理者アカウントを作成します。Cisco TMSPE は、CMR を作成するために、この管理者アカウントを使用して、TelePresence Conductor にアクセスします。

ヒント　TelePresence Conductor で設定されたエイリアスとテンプレートは、TMSPE では使用されません。その代わりに、エイリアスとテンプレートは TMSPE 内で設定します。

CMR のための Cisco TMSPE の導入タスク

Cisco TMSPE（Cisco TMS とともに使用）は、ユーザに CMR を作成するためのポータルを提供します。このためには、Cisco TMSPE を Cisco TMS にインストールし、アクティブにする必要があります。Cisco TMSPE を使用すると、管理者は、CMR を使用する権限を付与する 1 つ以上のユーザ グループ内にユーザを作成したりユーザをインポートしたりできます。たとえば、ユーザ グループは、ユーザがメンバーである Active Directory のグループに一致させることができます。または、ユーザ グループは、ユーザが存在する Active Directory の組織単位（OU）に一致させることもできます。Cisco TMSPE では、ユーザ グループ [エグゼクティブ（Executive）] と [マーケティング（Marketing）] を作成し、対応する AD グループに属するユーザを Active Directory からインポートします。表 3-15 に、ユーザをユーザ グループにインポートするための Active Directory の検索フィルタのリストを示します。TMSPE 内の TelePresence Conductor 設定オプションを使用して、管理者は CMR の導入に使用する TelePresence Conductor を指定できます。各 TelePresence Conductor クラスタに対して、管理者は、Conductor ノードの 1 つを指すレコードを 1 つだけ作成する必要があります。TelePresence Conductor 設定を構成するには、ここで TelePresence Conductor で作成された管理者アカウントを使用します。

表 3-15　　ユーザをユーザ グループにインポートするための検索フィルタ

ユーザ グループ	検索フィルタ
エグゼクティブ	(&(objectClass=user)(memberof=cn=executive, ou=enterprise, dc=ent-pa, dc=com))
マーケティング	(&(objectClass=user)(memberof=cn=marketing, ou=enterprise, dc=ent-pa, dc=com))

CMR テンプレートは、TelePresence Conductor の会議テンプレートおよび会議エイリアスに対応します。CMR テンプレートを使用して、管理者は会議属性（たとえば、会議品質、内容品質、会議 PIN など）、会議エイリアス（SIP URI と数字エイリアスのいずれかまたは両方）、および CMR 作成用の TelePresence Conductor を指定できます。1 つの CMR テンプレートを各ユーザ グループに割り当て、そのグループ内のユーザが Cisco TMSPE ポータルを使用して独自の CMR を設定できるようにします。

ユーザが CMR を作成すると、Cisco TMSPE は、そのユーザのグループに関連付けられた CMR テンプレートで定義された設定を適用します。また、プロビジョニング API コールを実行して、TelePresence Conductor に会議を作成します。これ以上、管理者が実行する必要のある操作はありません。

（注） Cisco TMSPE を使用して作成された CMR は、TelePresence Conductor Web インターフェイスからは変更できません。TelePresence Conductor を使用して作成された会議テンプレートおよびエイリアスは、Cisco TMSPE からは変更できません。

要約

上記の導入タスクを完了したら、ユーザは Cisco TMSPE ポータルにログインして、CMR の作成、および対応する SIP URI と数字エイリアスの生成ができます。ユーザは SIP URI または数字エイリアスをダイヤルして会議を開始できます。

7. WebEx および Collaboration Meeting Rooms（CMR）Hybrid の導入

このセクションでは、Cisco CMR Hybrid を有効にするために必要な主なタスクについて説明します。

概要

TelePresence Conductor for CMR Hybrid の導入タスク：

1. 以前に設定した TelePresence Conductor およびスケジュール済み会議のエイリアスを CMR Hybrid 会議に使用できます。

CMR Hybrid のための Unified CM の導入タスク：

2. WebEx サイトに一致し、Expressway-C ルート リストを指す SIP ルート パターンを設定します。

CMR Hybrid のための Expressway の導入タスク：

3. TLS 検証を使用し、暗号化を実行し、および TLS 検証名 **sip.webex.com** を使用する新規 DNS ゾーンを作成します。
4. WebEx ドメインを含むすべての URI に一致し、追加されたすべての文字を削除する検索ルールを作成します。

CMR Hybrid のための Cisco TMS の導入タスク：

5. WebEx 統合オプション キーをインストールします。
6. WebEx サイトを Cisco TMS に追加します。
7. CMR Hybrid の使用が有効にされたユーザの Cisco TMS ユーザ プロファイルに以下の属性を設定します。
   - WebEx ユーザ名
   - WebEx パスワード（シングルサインオンが有効にされていない場合）
   - アカウントを持っている WebEx サイト

CMR Hybrid のための Cisco TMSXE の導入タスク：

8. 関連するユーザ用に、Outlook への WebEx と TelePresence の統合プラグインをダウンロードしてインストールします。
9. webex@company.com などの WebEx Scheduling Mailbox を以下の設定値に設定します。
   - カレンダー アテンダントをオフにする。
   - AddNewRequestTentatively を [無効（Disabled）] に設定する。.
10. TMSXE が CMR Hybrid 予約について TMSXE 内の WebEx Scheduling Mailbox をモニタするようにそれらのメールボックスを設定します。

CMR Hybrid のための音声の導入タスク：

11. 導入要件に関する最適な音声接続タイプを選択し、関連する設定を有効にします。

CMR Hybrid のための WebEx サイト管理者の導入タスク：

12. Cisco TelePresence 統合（Meeting Center のみ）を有効にします。
13. 以下のその他の設定を行います。
    - Cisco TMS 予約サービスの URL
    - カレンダー上の Cisco TelePresence 会議のリスト
    - 会議ホストへの招待メールの送信
    - フリーダイヤル電話番号の参加者への表示
    - VoIP およびビデオ接続の [自動暗号化UDP/TCP SSL（Automatically encrypted UDP/TCP SSL）] への設定
    - 目的の音声接続に基づいた関連する音声設定の設定
14. Meeting Center TelePresence セッション タイプを、CMR Hybrid を使用するすべてのユーザに割り当てます。

導入上の考慮事項

Cisco CMR Hybrid は次の主要な機能を提供します。

- WebEx アプリケーションとテレプレゼンス デバイスの間の最大 720p 画面解像度での双方向ビデオ
- 統合音声とプレゼンテーション共有（会議に参加するすべてのユーザのアプリケーションおよびデスクトップ コンテンツの共有機能を含む）
- 会議のネットワークベースのレコーディング（コンテンツ共有、チャット、およびポーリングを含む）
- Cisco TelePresence Management Suite（Cisco TMS）を使用した統合会議スケジュール（これにより、ユーザは Cisco CMR Hybrid 会議のスケジュールを簡単に行えます）
- Cisco Expressway-E が提供するメディア暗号化によって実現される安全なコール制御および接続
- Cisco TelePresence Conductor によって提供される TelePresence Server の管理と会議リソースの割り当て
- サードパーティのテレプレゼンス デバイスとの相互運用性

Cisco TMS での Cisco CMR Hybrid 会議をスケジュールする各ユーザは、WebEx サイト上のホストアカウントを持っている必要があります。

ヒント　Cisco WebEx Meeting Center for CMR Hybrid 導入環境の最小バージョンとして WBS29 を使用することをお勧めします。

SIP 音声または PSTN 音声のいずれかを使用して、CMR Hybrid を導入できます。これは、Microsoft Outlook への統合、Cisco Smart Scheduler、または Cisco WebEx Scheduling Mailbox のいずれかを使用してスケジュールできます。

TelePresence Conductor for CMR Hybrid の導入タスク

以前に設定した TelePresence Conductor およびスケジュール済み会議のエイリアスを CMR Hybrid 会議に使用できます。

CMR Hybrid のための Unified CM の導入タスク

スケジュール済み会議のために Unified CM が Cisco Expressway および TelePresence Conductor と通信可能にするための以前の設定によって、CMR Hybrid との通信も可能になります。TelePresence Conductor から WebEx サイトへのコールが正しくルーティングされるように、追加の設定が 1 つ必要になります。それは、Expressway-C ルート リストにルーティングするための WebEx サイト（例：yoursite.example.com）に一致する SIP ルート パターンの設定です。

CMR Hybrid のための Expressway の導入タスク

Cisco Expressway-E では、特定のルート認証局によって署名され、WebEx クラウドの DST ルート CA 証明書とサーバ証明書を発行した CA の CA 証明書の両方を信頼するサーバ証明書が必要になります。サポートされるルート CA のリストについては、次のページで入手可能な『Cisco Collaboration Meeting Rooms（CMR）Hybrid Configuration Guide』を参照してください。

http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html

TLS 検証が有効にされ、TLS 検証名として **sip.webex.com** を使用する Expressway-E 上の新規 DNS ゾーンを設定します。WebEx ドメインに一致するこの DNS ゾーンを指すように検索ルールを設定します。

注意　コールのメディア部分が失敗する原因となる不具合があるため、スタティック NAT は Expressway-E では使用できません。スタティック NAT が必要な場合は、『*Cisco Collaboration Meeting Rooms (CMR) Hybrid Configuration Guide*』に示された推奨回避策を参照してください。

CMR Hybrid のための Cisco TMS の導入タスク

最初に、WebEx 統合オプション キーを Cisco TMS にインストールします。このキーがないと、CMR Hybrid 会議をスケジュールできません。WebEx サイトを Cisco TMS に追加し、このサイトへの接続を開始します。

Cisco TMS を使用して会議をスケジュールするには、信頼するようにサーバで設定したユーザ名とパスワードが必要になります。Active Directory のユーザは信頼されますが、Cisco TMS ユーザ プロファイルに格納された以下の情報が必要になります。

- WebEx ユーザ名
- WebEx パスワード（シングルサインオンが有効にされていない場合）
- アカウントを持っている WebEx サイト

CMR Hybrid のための Cisco TMSXE の導入タスク

すべてのクライアント タイプが Cisco TMSXE を使用して会議を予約できるようにするには、Cisco TMSXE を使用して CMR Hybrid 会議をスケジュールするための以下の 2 つのオプションを有効にします。

- Microsoft Outlook 用の WebEx 生産性向上ツール プラグイン

  ユーザは、Microsoft Outlook の [WebEx ミーティング オプション（WebEx Meeting Options）] パネルを使用して WebEx を会議に追加します。

- WebEx Scheduling Mailbox の使用

  ユーザは、特別な招待先（WebEx メールボックス）を含めることによって、WebEx を会議招待に電子メール クライアントから直接追加します。

TMSXE 予約サービスを通常として設定する必要があります。

WebEx および Outlook プラグインへの TelePresence 統合を使用して会議をスケジュールする会議の主催者は、TelePresence に関する WebEx 生産性向上ツールを WebEx サイトからダウンロードしてインストールする必要があります。

WebEx Scheduling Mailbox を有効にするには、会議が CMR Hybrid に対して有効にされるときに常にスケジューリング参加者として使用する Microsoft Exchange の新規ユーザ メールボックスを作成します。このメールボックスのカレンダー アテンダントをオフにし、新しい要求が仮の予定としてマークされないように AddNewRequestsTentatively 設定を無効にします。また、アカウントに関連付けられた AD ユーザも無効にします。

TMSXE が CMR Hybrid 予約についてモニタするアカウントを認識するように、WebEx Scheduling Mailbox として TMSXE で新規メールボックスを設定します。

CMR Hybrid のための音声の導入タスク

CMR Hybrid では、以下の音声接続オプションをサポートします。顧客の好みに応じて方式を選択します。

- SIP 音声：
  - SIP 音声を使用するように Cisco TMS で WebEx サイトを設定します。
  - WebEx サイトでハイブリッド モードを有効にします。
- PSTN 音声：
  - PSTN 音声を使用するように Cisco TMS で WebEx サイトを設定します。
  - WebEx サイトでハイブリッド モードを有効にします（オプション）。
  - PSTN コールが PSTN ゲートウェイをパススルーして WebEx に渡るように設定します。
- TSP 音声：
  - MACC ドメイン インデックスおよびオープン TSP 会議室 WebEx 設定を設定します。
  - TSP ダイヤル文字列を設定します。
  - 会議を開く方法を設定します。
  - 会議の主催者の TSP 音声を設定します。

CMR Hybrid のための WebEx サイト管理者の導入タスク

CMR Hybrid が機能するように WebEx サイトを設定します。主な設定は、以下のとおりです。

- Cisco WebEx OneTouch 会議の許可（Meeting Center のみ）
- Cisco TMS 予約サービスの URL
- カレンダー上の Cisco TelePresence 会議のリスト
- 会議ホストへの招待メールの送信
- フリーダイヤル電話番号の参加者への表示

- VoIP およびビデオ接続の [自動暗号化UDP/TCP SSL（Automatically encrypted UDP/TCP SSL）] への設定
- 目的の音声接続に基づいた関連する音声設定

設定を完了するには、Meeting Center TelePresence セッション タイプを WebEx サイトでホスト アカウントに割り当てる必要があります。これは、個々のユーザ用に [ユーザの編集（Edit User）] 画面を開くか、[ユーザリストの編集（Edit User List）] 画面から各ユーザの適切なセッション タイプを選択することによって実行できます。

要約

上記の導入タスクを完了すると、ユーザが TelePresence 会議および CMR Hybrid 会議を作成するための CMR Hybrid の準備が整います。

関連資料

- 『Cisco Personal Multiparty At-A-Glance』

  http://www.cisco.com/c/dam/en/us/solutions/collateral/collaboration/pervasive-conferencing/at-a-glance-c45-729835.pdf
- 『Cisco TelePresence Management Suite (TMS) and CMR Hybrid deployment guides』

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-and-configuration-guides-list.html
- 『Cisco TelePresence Conductor and Collaboration Meeting Rooms（CMR）Premises (optimized conferencing) deployment guides』

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-installation-and-configuration-guides-list.html
- 『Cisco TelePresence Conductor API guides』

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-conductor/products-programming-reference-guides-list.html
- 『Cisco TelePresence Server Release Notes』

  http://www.cisco.com/c/en/us/support/conferencing/telepresence-server/products-release-notes-list.html

コラボレーション エッジ

改訂日：2015 年 1 月 22 日

この章では、コラボレーション ネットワーク境界におけるサービスへのアクセスを定義する一連のサーバとゲートウェイを含むコラボレーション エッジ推奨アーキテクチャについて説明します。コラボレーション エッジ推奨アーキテクチャは、インターネットや PSTN などのパブリック ネットワークへのアクセスを提供します。

コラボレーション エッジの詳細なアーキテクチャの説明のあとに、インターネット アクセス用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法に関する展開の概要セクションが続きます。また、コラボレーション エッジのハイ アベイラビリティ、コラボレーション エッジのセキュリティ、およびコラボレーション エッジ ソリューションのスケーリングについても取り上げます。さらに、コラボレーション エッジの展開プロセスに関するセクションでは、Cisco Expressway、Cisco Unified Border Element、Cisco 音声ゲートウェイ、および Cisco ISDN ビデオ ゲートウェイの展開方法に関する詳細情報を提供します。

この章の変更点

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

表 4-1　　本リリースで追加または変更された情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
IP ベース ダイヤリング	「Business-to-Business（B2B）コールの IP ベース ダイヤリング」（P.4-20）	2015 年 1 月 22 日
宛先エンドポイントに最も近い Expressway の選択	「着信コールに関する留意点」（P.4-38）	2015 年 1 月 22 日
XMPP フェデレーション	「インスタント メッセージおよびプレゼンス フェデレーション」（P.4-8） 「Expressway-C と Expressway-E 経由の外部 XMPP フェデレーションの展開」（P.4-21）	2015 年 1 月 22 日

コア コンポーネント

コラボレーション エッジ アーキテクチャのコア コンポーネントを以下に示します。

- Cisco Expressway-C と Expressway-E：音声とビデオのインターネット接続とファイアウォール トラバーサル用
- Cisco Unified Border Element：IP トランク経由の音声 PSTN 接続用
- PSTN 音声ゲートウェイ：直接音声 PSTN 接続用
- ISDN ビデオ ゲートウェイ：直接ビデオ ISDN 接続用

主な利点

- 実装されているテクノロジーや使用されているパブリック ネットワークに関係なく、顧客やパートナーに接続します。
- 回復力のある、柔軟で拡張可能なアーキテクチャを提供します。
- ハードウェア クライアントとソフトウェア クライアントがパブリック ネットワーク（インターネットや PSTN）にアクセスできるようにします。
- Cisco Mobile クライアント、リモート クライアント、およびエンドポイントにコラボレーション サービスへのセキュアな VPN レス アクセスを提供します。

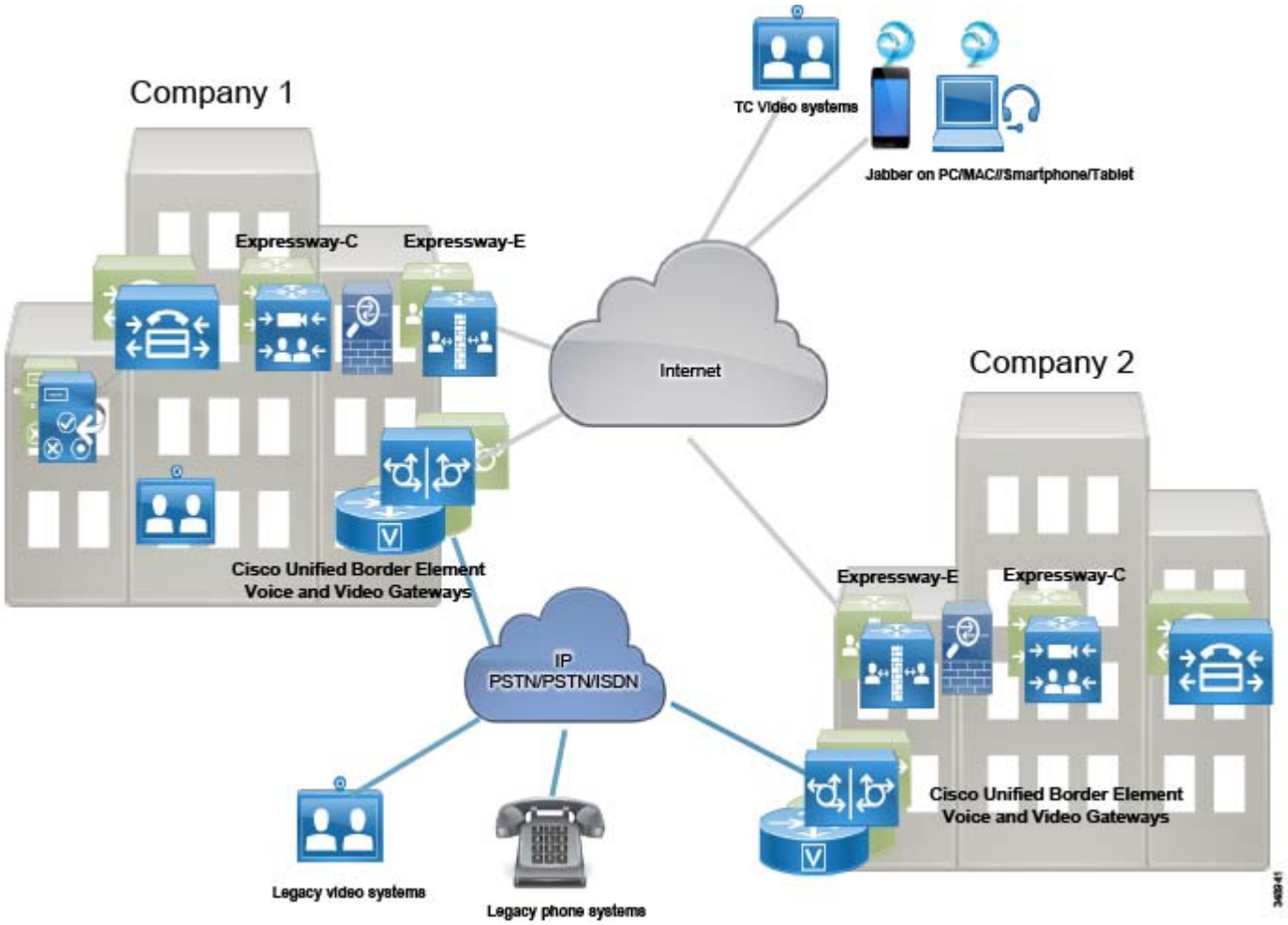
アーキテクチャ

コラボレーション エッジのアーキテクチャは、2 つの主要なネットワーク（インターネットと PSTN）とインターフェイス接続します。

インターネット接続は、VPN レス モバイルおよびリモート アクセス（MRA）と Business-to-Business（B2B）コミュニケーションを可能にします。これらのサービスを使用すれば、Jabber ユーザとハードウェア ビデオ エンドポイントは、組織のネットワーク境界の外側にある企業コラボレーション サービスに安全にアクセスして、外部組織との Business-to-Business（B2B）音声およびビデオ通信を実現できます。

Cisco Expressway-C と Expressway-E は、ファイアウォール境界を横断しなければならないほとんどのケースでペアとして展開する必要があります。Expressway-C を内部ネットワークに、Expressway-E を緩衝地帯（DMZ）に配置することによって、ファイアウォールの両側でファイアウォール トラバーサル機能を有効にします。加えて、Expressway-C と Expressway-E をそれぞれクラスタ化することができます（図 4-1 を参照）。ほとんどの場合、横断するファイアウォール境界はインターネット接続ですが、個人所有デバイス持ち込み（BYOD）接続用の別の企業 WiFi ネットワークの場合もあります。複数の Expressway-C と Expressway-E のペアを使用して地理的に分散した展開でこのアーキテクチャを使用した場合、Business-to-Business（B2B）コールは最も近いインターネット ブレークアウト ポイントに転送されます。ビデオ トラフィックは、インターネット ブレークアウトへの最短パスを通って社内ネットワークに到達します。同じ考え方が、最も近いインターネット入口点に転送される MRA ユーザ トラフィックにも適用されます。

図 4-1　　アーキテクチャの概要



PSTN 接続は、通信事業者ネットワークとの音声およびビデオ通信を可能にします。また、PSTN 接続は次のような方法で実現できます。

- 通信事業者への IP トランク経由。通常は音声専用サービス用。この接続は、サービス統合型ルータ（ISR）G2/G3 またはアグリゲーション サービス ルータ（ASR）上の Cisco Unified Border Element（CUBE）によって提供されます。Cisco Unified Border Element は、通信事業者のネットワークが企業ネットワークと通信するセントラル サイトに展開する必要があります。
- 音声ゲートウェイ経由。ゲートウェイには、シスコ サービス統合型ルータ（ISR）G2/G3 などのさまざまなルータ プラットフォーム上のアナログ インターフェイスと ISDN インターフェイスが含まれます。このマニュアルでは、ISDN 音声インターフェイスのみを取り上げます。音声ゲートウェイは、PSTN 接続が必要なサイトでローカルに展開する必要があります。
- PSTN へのレガシー H.320 ビデオ アクセスを可能にする Cisco TelePresence ISDN Gateway 3241 または MSE 8321 経由。TelePresence ISDN Gateway は、ISDN ビデオ接続が必要なすべての場所で一元管理する必要があります。TelePresence ISDN Gateway の特性とコストから、複数の場所を通して共有することができます。

ビデオ コール用のインターネット通信（Expressway）と音声専用コール用の IP PSTN 接続（CUBE）の展開に関連したコストを削減できます。ただし、次の点に注意してください。

- すべての会社がビデオ システムに対応したインターネット通信を利用できるわけではありません（Business-to-Business（B2B））。ビデオ通信専用に ISDN を使用しているパートナーや顧客が存在する場合は、ビデオ ゲートウェイもお勧めします。
- IP ネットワークの信頼性は徐々に向上していますが、ネットワークの接続性の問題でリモート サイトから集中型 IP PSTN サービスにアクセスできない場合があります。このようなサイトで日常業務の実行を PSTN 接続に大きく依存している場合は、集中型アクセス用のバックアップとして使用されるローカル PSTN 接続をお勧めします。

PSTN に関する推奨事項を以下に示します。

- PSTN を一元管理します。これにより、運用コストと経費が削減されます。
- 日常業務の実行を PSTN に大きく依存しているサイト専用のローカル PSTN 接続を設置します。このような場合は、ISDN チャネル数を削減する必要があります。これは、中央の PSTN アクセスが使用できない状況でしか ISDN チャネルが使用されないためです。これにより、ハードウェア コストが削減され、管理が簡素化され、資金の節約につながります。

上記の考察に基づくと、音声用に PSTN への IP トランク接続、ビデオ用にローカル PSTN ブレークアウトをバックアップとして使用したインターネットを使用することにより、大半の接続要件を満たすことになります。ただし、完全な接続性を提供するには、インターネットにアクセスできないパートナーや顧客に到達するための ISDN ビデオ ゲートウェイもお勧めします。

シスコ コラボレーション エッジには、ユーザが次のオプションにアクセスできるシナリオが含まれます。

- テレワーカやモバイル接続用のモバイルおよびリモート アクセス（MRA）
- 組織間の Business-to-Business（B2B）ビデオ通信
- 携帯電話用と固定電話へのアクセス用の PSTN
- 既存の H.320 ビデオ システムと通信するための ISDN ビデオ アクセス

これらのシナリオでは、社内のユーザまたはインターネット上のユーザが、PSTN 音声コール、ISDN ビデオ コール、および Business-to-Business（B2B）コミュニケーションに、それらが社内に存在するかのようにアクセスできます。ほとんどのケースで、保留、転送、会議などのサービスも使用できます。誰が誰に電話するかに関係なく、コラボレーション エッジ ソリューションは、モバイルおよびリモート アクセス、Business-to-Business（B2B）、PSTN 音声、およびビデオ サービス間の相互接続を可能にします。

インターネット アクセスに関する Expressway-C と Expressway-E の役割

インターネットを使用したコラボレーション サービスは、人気が高く、既存のレガシー ISDN ビデオ システムがどんどん置き換えられています。インターネット ベースのコラボレーション サービスに使用されている 2 つの主なプロトコルは SIP と H.323 です。

また、インターネットは、リモート ユーザとモバイル ユーザを、バーチャル プライベート ネットワーク（VPN）を使用せずに、音声、ビデオ、IM and Presence、およびコンテンツ共有サービスに接続するためにも使用されます。

モバイルおよびリモート アクセスだけでなく、Business-to-Business（B2B）サービスも、同じ Expressway-C と Expressway-E のソリューション ペアの一部として有効にできます。Expressway-C は社内ネットワーク内に展開されるのに対して、Expressway-E は DMZ 内に展開されます。

Expressway-C と Expressway-E のペアは次の機能を実行します。

- インターワーキング：音声、ビデオ、およびコンテンツ共有用の H.323 / SIP 間コールを相互接続する機能。
- 境界通信サービス：Expressway-C は社内ネットワーク内に配置されますが、Expressway-E はエンタープライズ DMZ 内に配置され、企業ネットワークとインターネット間の通信サービス専用の接続点を提供します。
- セキュリティ：モバイルおよびリモート アクセスと Business-to-Business（B2B）コミュニケーションの両方に認証と暗号化を提供する機能。

モバイルおよびリモート アクセス、および Business-to-Business（B2B）コールは Expressway-E と Expressway-C をフロースルーして、コール シグナリングとメディアの両方だけでなく、その他のコラボレーション データ フロー（XMPP や HTTP を含む）も処理されます。

モバイルおよびリモート アクセス

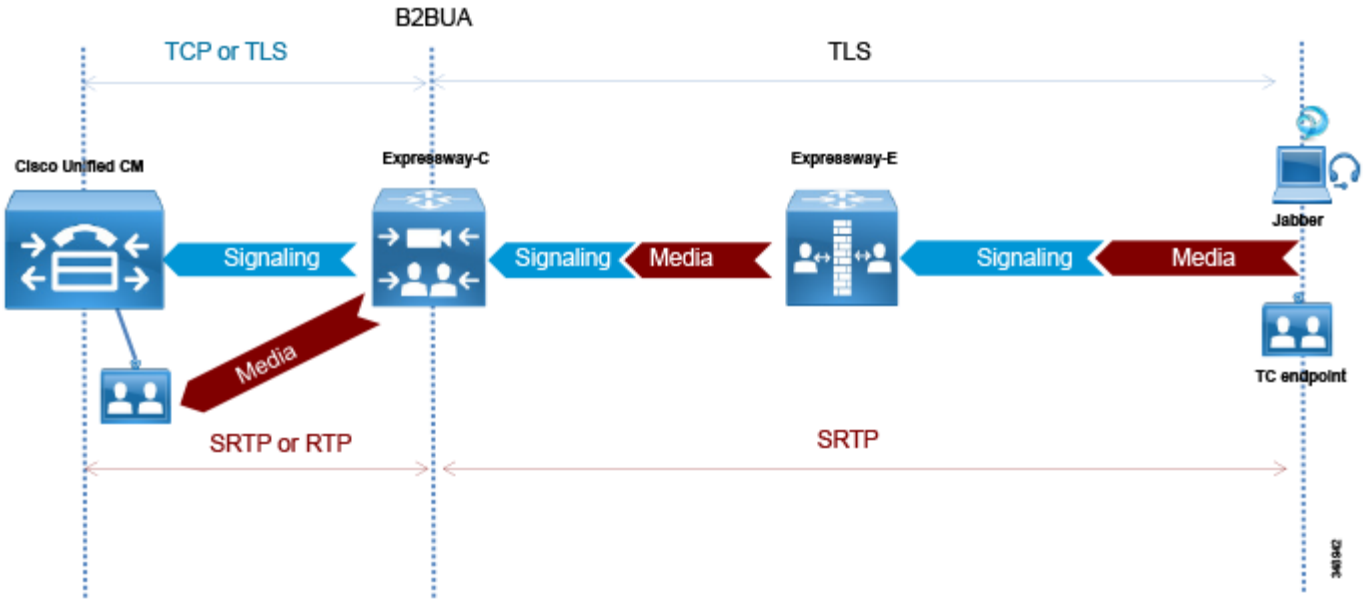
Cisco Expressway ソリューションのモバイルおよびリモート アクセス機能は、逆プロキシ ファイアウォール トラバーサル接続を提供します。これにより、リモート ユーザとそのデバイスが企業のコラボレーション アプリケーションおよびサービスにアクセスして利用できます。

図 4-2 に示すように、Cisco Expressway ソリューションには、2 つの主なコンポーネント（Expressway-E ノードと Expressway-C ノード）が含まれています。この 2 つのコンポーネントは、Cisco Unified Communications Manager（Unified CM）と連携して、セキュアなモバイルおよびリモート アクセスを可能にします。Expressway-E ノードは、モバイルおよびリモート デバイスにセキュアなエッジ インターフェイスを提供します。

Expressway-C は、Expressway-E ノードとのセキュアな TLS 接続を構築します。Expressway-C ノードは、Unified CM へのプロキシ登録を提供し、リモート セキュア エンドポイント登録を可能にします。Expressway-C ノードには、メディア終端機能を提供するバックツーバック ユーザ エージェント（B2BUA）が含まれます。

図 4-2 に、すべてのモバイルおよびリモート アクセス コールのシグナリングとメディアの両方が Expressway-C と Expressway-E を行き来する様子を示します。

図 4-2　　Expressway 上の B2BUA とコール レッグ

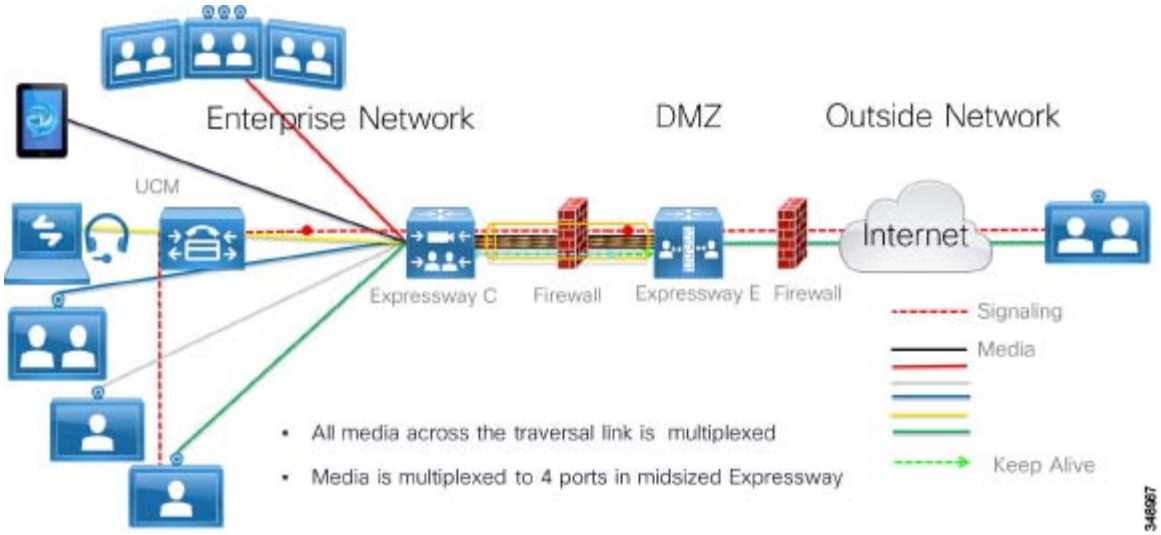


Business-to-Business（B2B）コミュニケーション

Expressway-C と Expressway-E は、連携してインターネット経由の Business-to-Business（B2B）コミュニケーション用のコア コンポーネントであるファイアウォール トラバーサル ソリューションを形成するように設計されています。

Expressway-C は、企業ネットワークの内部（信頼された側）に配置され、Expressway-E へのセキュアで信頼できる各種の標準規格に準拠した接続手段を提供する役割を果たします。また、背後にあるすべてのデバイスのトラバーサル クライアントとして機能します。このソリューションは、アウトバウンド通信用に開かれた少数のポートにすべてのメディアを多重化することによって、大量のメディア ポートを使用するデバイスの問題を解決します。また、Expressway-C から Expressway-E までのトラバーサル ゾーンに関するキープアライブを送信することによって、社内から社外への認証された信頼できる接続を実現します。加えて、すべてのインターネット通信に単一接点を提供します。つまり、セキュリティ リスクが最小化されます（図 4-3 を参照）。

図 4-3　　Expressway-C の多重化とキープアライブ



SIP、H.323、XMPP などのリアルタイムや準リアルタイムの通信プロトコルでは、ファイアウォールの背後に設置されたデバイスとの通信ニーズは解決されません。このようなプロトコルを使用した典型的な通信には、シグナリングとメディア内にデバイス IP アドレスが含まれており、それぞれが TCP パケットと UDP パケットのペイロードになります。これらのデバイスが、内部的にルーティング可能な同じネットワーク上に存在する場合は、相互に直接通信することができます。TCP パケットのペイロードで伝送されるシグナリング IP アドレスは送信デバイスに戻すルーティングが可能であり、その逆もできます。ただし、送信デバイスがパブリックまたはネットワーク エッジ ファイアウォールの背後の別のネットワーク上に存在する場合は、2 つの問題が発生します。1 つ目の問題は、受信デバイスが、パケットの復号化後に、ペイロードで伝送された内部 IP アドレスに応答することです。この IP アドレスは、通常、ルーティング不可能な RFC 1918 アドレスであり、絶対に返信先に到達しません。発生する 2 つ目の問題は、返信先 IP アドレスがルーティング可能であっても、メディア（RTP/UDP）が外部ファイアウォールによってブロックされることです。このことは、Business-to-Business（B2B）コミュニケーションと、モバイルおよびリモート アクセスの通信の両方に当てはまります。

Expressway-E は DMZ 内のネットワーク エッジに配置されます。これは、標準の相互運用性を維持しながら、SIP、H323、および XMPP に関するシグナリングとメディアの両方のルーティング問題を解決する役割を果たします。さらに、ネットワーク内部のエンドポイント、デバイス、およびアプリケーション サーバの代わりにメディアとシグナリングを処理するために該当するヘッダーと IP アドレスを変更します。

インスタント メッセージおよびプレゼンス フェデレーション

インスタント メッセージおよびプレゼンス フェデレーションは、ある組織のユーザがチャットやプレゼンス ステータス情報に関する XMPP トラフィックをその組織の外部ファイアウォール経由で別の組織のユーザとやり取りできるようにします。

以前のシスコ アーキテクチャは、シスコ適応型セキュリティ アプライアンス（ASA）ファイアウォールを TLS プロキシとして使用して、外部ファイアウォール経由で直接内部の IM and Presence サーバにアクセスするために受信ポートを開くことができるようにしていました。現在は、Expressway-C と Expressway-E が IM and Presence フェデレーションの推奨アーキテクチャです。

インスタント メッセージおよびプレゼンス フェデレーションは、XMPP トラフィックを外部の宛先とやり取りするための信頼できるセキュアなファイアウォール トラバーサル ソリューションとして同じ Expressway-C と Expressway-E のペア アーキテクチャを使用します。Expressway-E は、XMPP 用のセキュアな DMZ ベースのターミネーション ポイントをインターネットに提供します。Expressway-C は、ファイアウォール トラバーサル用の Expressway-E への TLS ベースで認証されたセキュアな接続を提供します。

また、Expressway-C は、IM and Presence サーバへの AXL API 接続も提供します。AXL API は、Expressway-E から収集された XMPP サーバ間情報を IM and Presence データベースに送信します。これにより、Expressway-E 経由で他の組織へのフェデレーション接続を開始するために必要な接続情報が IM and Presence サーバに提供されます。

PSTN アクセス

ここでは、Cisco Unified Border Element をセッション ボーダー コントローラ（SBC）として使用した PSTN アクセス用のアーキテクチャについて説明します。

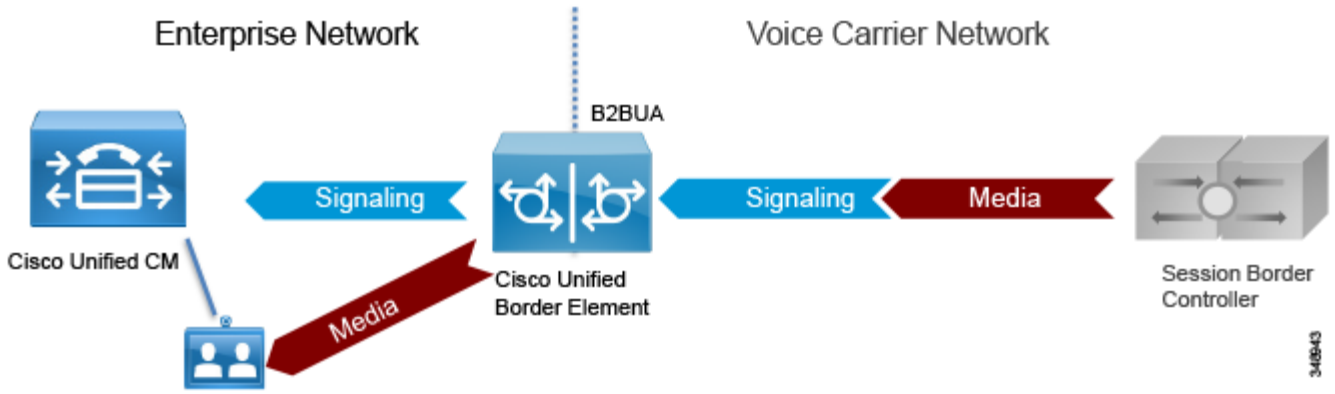
Cisco Unified Border Element の役割

従来の PSTN 接続の代わりに通信事業者への IP トランクを使用した音声接続は人気が高まっており、徐々に既存の TDM ベースの PSTN アクセスに取って代わろうとしています。SIP はプロバイダー ネットワークに接続するためのアクセス プロトコルとして広く使用されており、今日では、多くの通信事業者が音声専用サービスを Cisco Unified Border Element などのセッション ボーダー コントローラ経由で PSTN に提供しています。セッション ボーダー コントローラは、SIP バックツーバック ユーザ エージェント（B2BUA）であり、各コールの音声メディアと SIP シグナリングの両方が Cisco Unified Border Element を通過するフロースルー モードでよく使用されます（図 4-4 を参照）。

Cisco Unified Border Element は、さまざまな Cisco ルータおよびゲートウェイ上で利用可能なライセンス供与された Cisco IOS アプリケーションであり、通信事業者のボーダー エレメントへの SIP トランク経由で PSTN に接続するための推奨プラットフォームです。

また、Cisco Unified Border Element は、Cisco Unified Communications Manager（Unified CM）に基づくエンタープライズ音声ネットワークを SIP トランク サービス経由で通信事業者に接続して相互運用できるようにします。さらに、Cisco Unified Border Element は、シグナリング ストリームとメディア ストリームの両方を終端処理して再発信することにより、IP ネットワーク間のセキュアなボーダー相互接続サービスを提供します。Cisco Unified Border Element を使用しているお客様は、現在のネットワーク サービスを縮小して、ネットワーク アーキテクチャを簡略化し、機能強化中のネットワークをコラボレーション サービスに位置付けることができます。

図 4-4　　B2BUA としての Cisco Unified Border Element



Cisco Unified Border Element は、エンタープライズ ネットワークと通信事業者ネットワークの間で次の機能を実行します。

- セッション制御：SIP セッションに対して、柔軟なトランク ルーティング、コール アドミッション制御、復元力、およびコール アカウンティングを提供する機能。
- インターワーキング：音声用のメディア トランスコーディング サービスと、SIP の遅延オファーと早期オファー間の相互運用性を提供する機能。
- 境界設定：2 つのネットワーク間のアドレス変換用とポート変換用に別々の境界ポイントとして機能し、トラブルシューティングを容易にする機能。
- セキュリティ：ネットワーク間のリアルタイム トラフィックをインテリジェントに許可または禁止し、アプリケーションの必要に応じてリアルタイム トラフィックを暗号化する機能。

音声ゲートウェイの役割

集中型 PSTN アクセスが使用できない場合は、TDM ゲートウェイを使用して PSTN に接続することをお勧めします。シスコでは、適切なインターフェイス カード（低密度デジタル（BRI）、高密度デジタル（T1、E1、および T3）、およびアナログ（FXS、FXO、および E&M）の各インターフェイス）が有効になっている ISR G2/G3 ルータ上で PSTN へのアナログ接続とデジタル接続を可能にする広範な種類の TDM ゲートウェイを提供しています。

音声ゲートウェイの詳細については、『*Cisco 3900 Series, 2900 Series, and 1900 Series Software Configuration Guide*』を参照してください。

ビデオ ISDN ゲートウェイの役割

ビデオ通信には ISDN とともに長い歴史があります。当初から、通信プロトコルとして ISDN を使用したビデオ会議は商業的に成功しつつありました。そのため、いまだにレガシー ビデオ システムを使用した ISDN 経由の双方向通信のニーズがあります。Cisco TelePresence ISDN Gateway は、ビデオ会議コールのために ISDN から SIP への変換、または、その逆変換を行う役割を担っています。シスコが推奨する企業コラボレーション用アーキテクチャには、レガシー ビデオ会議システムと通信する目的で Unified CM にトランキングされた ISDN ゲートウェイ アクセスが含まれます。

プロトコル変換による損失を最小限に抑えるには、シスコ製品間の通信用として内部的に使用されるプロトコルをそのまま維持するために H.323/ISDN 変換ではなく、SIP/ISDN 変換をお勧めします。

Cisco TelePresence ISDN Gateway の詳細については、次の URL から入手可能なマニュアルを参照してください。

http://www.cisco.com/c/en/us/support/conferencing/telepresence-isdn-gateway/tsd-products-support-series-home.html

展開の概要

ここでは、インターネット接続用の Cisco Expressway と PSTN アクセス用の Cisco Unified Border Element の展開方法について説明します。

インターネット接続用の Expressway-C と Expressway-E の展開

シスコ コラボレーション エッジ アーキテクチャの標準展開には、企業のコラボレーション サービスに対するセキュアなモバイルデバイスおよびリモート VPN レス アクセス用の 1 つ以上の Expressway-C と Expressway-E のペアの展開が含まれます。

復元力を高めるためには、Expressway-C と Expressway-E の両方をクラスタ内に展開する必要があります。クラスタごとのサーバ数は、Unified CM に対する同時プロキシ化登録の数と同時コールの数によって異なります。前者の数には Expressway 経由で Unified CM に登録するモバイル ユーザとリモート ユーザの数が数えられるのに対して、後者の数には Business-to-Business（B2B）とモバイルおよびリモート アクセス（MRA）の同時コールの数が数えられます（詳細については、サイジングの章を参照してください）。

このサービスは、Jabber クライアントと Cisco TelePresence System エンドポイント（C、EX、MX、および SX シリーズ モデル）に提供されます。しばしば、地理的範囲とスケーリングのために複数のペアの Expressway-C と Expressway-E が展開され、これにより、コラボレーション サービスの複数のインスタンスへのアクセスが可能になります。インターネット サービス プロバイダーからのさまざまなメトリックに基づいてリモート クライアントおよびエンドポイント アクセスのバランスを取るため、GeoDNS を使用する必要があります。

この同じ Expressway を Business-to-Business（B2B）コミュニケーションに利用することもできます。コール量が Expressway クラスタの能力（中型 OVA テンプレートの場合の 600 同時コールまたは大型 OVA テンプレートの場合の 2,000 同時コール）を上回っている場合は、Business-to-Business（B2B）サービスと MRA サービスを別々のボックスに分離する必要があります。詳細については、サイジングの章を参照してください。

Expressway が両方のサービスに使用されている場合は、Unified CM がインターネット上のユニファイド ビジネス コミュニケーション アクセス用の SIP トランク経由で Expressway-C に接続されます。Expressway-C は、ネットワークの信頼された側に配置され、セキュアなファイア ウォール トラバーサル サービスを Expressway-E に提供します。

エンタープライズ セキュリティ ポリシーに基づいて、さまざまな展開モデルを実装できます。このマニュアルでは、デュアル インターフェイスを備えた DMZ 展開を中心に説明します。これは、この展開が最も一般的でセキュアな展開モデルだからです。その他の展開モデルについては、『*Cisco Expressway Basic Configuration Deployment Guide*』を参照してください。

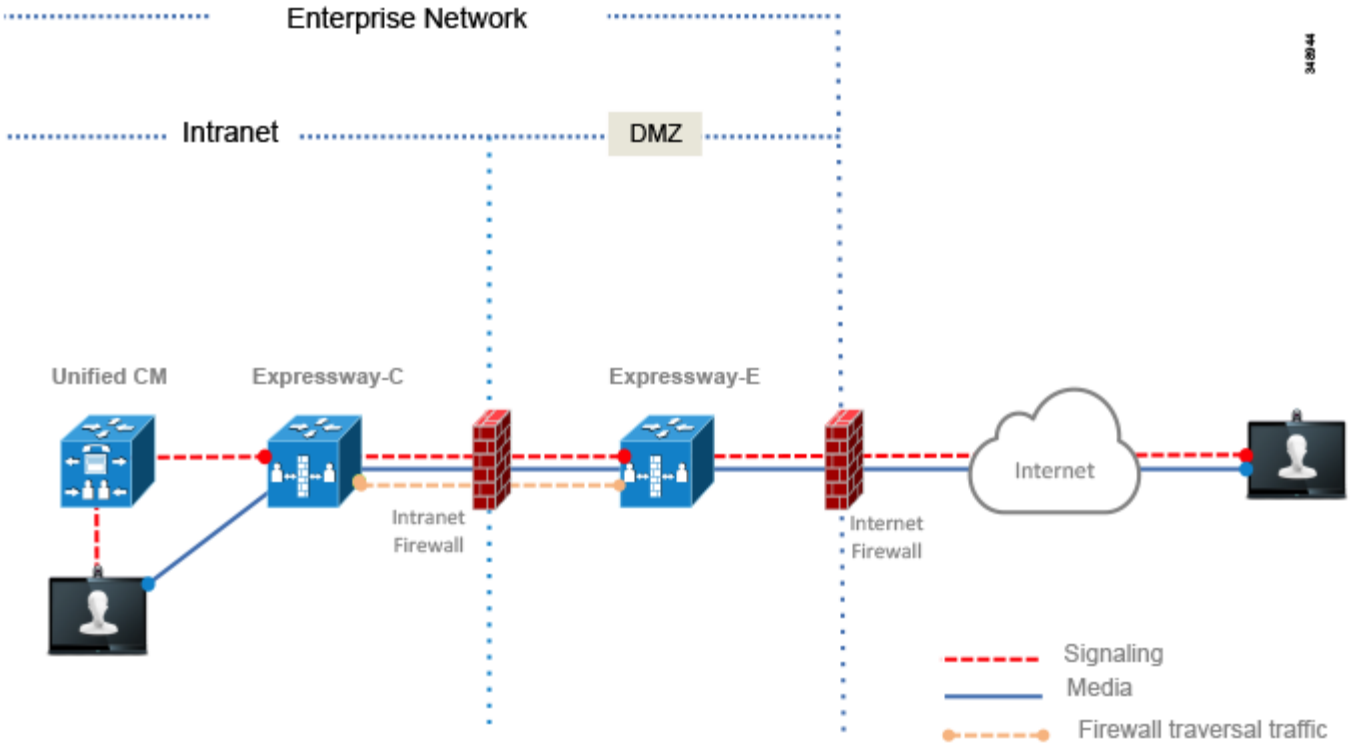
Expressway-C と Expressway-E は、ファイアウォール トラバーサル機能を提供します。ファイアウォール トラバーサルは次のように動作します。

1. Expressway-E はエンタープライズ DMZ 内に設置されたトラバーサル サーバです。Expressway-C は企業ネットワーク内部に設置されたトラバーサル クライアントです。
2. Expressway-C は、セキュアなログイン クレデンシャルを使用して、ファイアウォールを通って Expressway-E 上の特定のポートに至るトラバーサル アウトバウンド接続を開始します。ファイアウォールがほとんどの場合の動作と同様にアウトバウンド接続を許可している場合は、企業のファイアウォールで追加のポートを開く必要はありません。ポートの詳細については、『*Unified Communications Mobile and Remote Access via Cisco Expressway Deployment Guide*』を参照してください。

   モバイルおよびリモート アクセスには、Unified Communications トラバーサル ゾーンと呼ばれる別のトラバーサル ゾーンが必要です。Unified Communications トラバーサル ゾーンは SIP と連動します。一方、Business-to-Business（B2B）トラバーサル ゾーンは SIP と H.323 を音声とビデオのシグナリング プロトコルとして許可します。Unified Communications トラバーサル ゾーンは、IM and Presence サーバへの接続とプロビジョニング目的で使用される XMPP と HTTPs も許可します。
3. 接続が確立されると、Expressway-C がキープアライブ パケットを定期的に Expressway-E に送信して接続を維持します。
4. Expressway-E が着信コールやその他のコラボレーション サービス要求を受け取ると、着信要求を Expressway-C に発行します。
5. その後で、Expressway-C がその要求を Unified CM またはその他のコラボレーション サービス アプリケーションにルーティングします。
6. 接続が確立され、アプリケーション トラフィック（音声メディアとビデオ メディアを含む）が既存のトラバーサル接続経由で安全にファイアウォールを通過します。

ファイアウォール トラバーサルが機能するためには、Expressway-C 上でトラバーサル クライアント ゾーンを設定し、Expressway-E 上でトラバーサル サーバ ゾーンを設定する必要があります。図 4-5 に、ファイアウォール トラバーサル プロセスの概要を示します。

図 4-5　Expressway-C と Expressway-E のファイアウォール トラバーサル プロセス



デュアルインターフェイス展開シナリオでは、Expressway-E が次の 2 つのファイアウォール間の DMZ 内に配置されます。インターネット ファイアウォールはインターネット向けの NAT サービスを提供し、イントラネット ファイアウォールは企業信頼ネットワークへのアクセスを提供します。

Expressway-E は次の 2 つの LAN インターフェイスを備えています。1 つはインターネット ファイアウォール向け（*外部インターフェイス*とも呼ばれる）で、もう 1 つはイントラネット ファイアウォール向け（*内部インターフェイス*とも呼ばれる）です。

外部インターフェイスにパブリック IP アドレスを割り当てる必要はありません。これは、NAT によってアドレスを静的に変換できるためです。この場合は、Expressway-E 自体にパブリック IP アドレスを設定する必要があります。

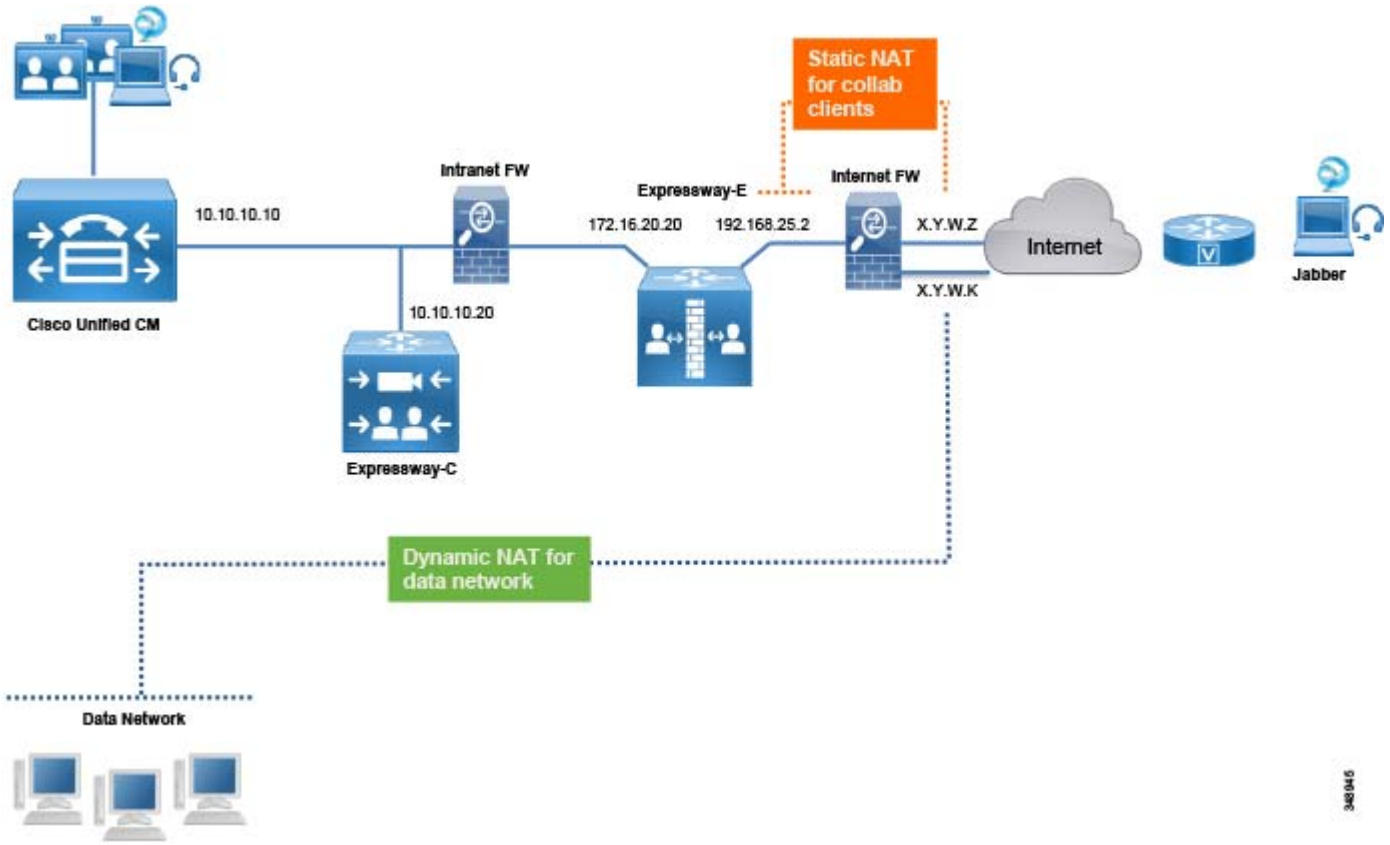
Expressway-C には、Expressway-E からの音声とビデオのシグナリングとメディアを含むコラボレーション アプリケーション トラフィックを終端処理する B2BUA が組み込まれています。その後で、Expressway-C がこのトラフィックを Cisco Unified CM やその他の企業のコラボレーション アプリケーションに向けて再発信します。モバイルおよびリモート アクセスの場合は、常に、Expressway-E 経由のインターネットから Expressway-C への接続が暗号化されます。Expressway-C とバックエンド アプリケーション サービス間の Business-to-Business（B2B）コミュニケーション用のインターネットからの接続は、その設定と会社の方針に基づいて暗号化される場合とされない場合があります。このケースでは、リモート Business-to-Business（B2B）パーティが公開証明書を使用した暗号化をサポートしている場合にのみ通信がエンド ツーエンドで暗号化されることに注意してください。これ以外のケースでは、ビデオコールが暗号化されずに送信されます。このマニュアルでは、モバイルおよびリモート アクセス サービスに関するインターネットと Expressway-C 間の暗号化を中心に説明しますが、Expressway-C と内部バックエンド サーバおよびクライアントの間の通信は暗号化されずに送信されます。Business-to-Business（B2B）暗号化機能については、後述のコラボレーション エッジのセキュリティに関するセクションで説明します。

Expressway-C は、モバイルおよびリモート アクセス Jabber クライアントまたは Cisco TelePresence System エンドポイントの Unified CM への登録をプロキシします。Unified CM では、それらが Expressway-C の IP アドレスで登録されたデバイスとして一覧表示されます。

図 4-6 に、前述した展開を示します。関連する IP アドレスが図に示されています。場所やインターネット サービス プロバイダーによって異なるパブリック IP アドレスが数字ではなく文字で表現されています。

Expressway-E は 2 つのインターフェイスを備えています。内部インターフェイスの IP アドレスは 172.16.20.20 で、外部インターフェイスの IP アドレスは 192.168.25.2 です。外部インターフェイスの IP アドレスは静的に X.Y.W.Z に変換されます。このアドレスは Expressway-E 上でも設定されます。Expressway-E が INVITE を送信すると、独自のアドレスを使用するのではなく、変換されたインターフェイス アドレスに設定された IP アドレスを使用して Session Description Protocol（SDP）メッセージが作成されるため、着信側はプライベート アドレスではなくルーティング可能なパブリック アドレスを使用できます。

図 4-6　　インターネット ファイアウォール上の NAT インターフェイス



インターネット上のエンドポイントが Expressway 経由で Unified CM やその他のコラボレーション アプリケーションに接続すると、その IP アドレスが最初にパブリック IP アドレスに変換されます。Expressway-E 上では、送信元 IP アドレスが Expressway-E の内部 IP LAN インターフェイスのアドレスに置き換えられます。パケットが Expressway-C に入ると、Expressway-C が、そのパケットをコラボレーション サービス アプリケーションに転送する前に、その送信元 IP アドレスを独自の IP アドレスに置き換えます。

もう一方の方向では、内部エンドポイントからのトラフィックが Expressway を通ってインターネットに入ると、その送信元 IP アドレスが Expressway-E 外部 LAN インターフェイス アドレスに置き換えられ、その後、インターネット ファイアウォール上の NAT によって静的に変換されます。データ デバイスの送信元 IP アドレスは、インターネット ファイアウォールの別のインターフェイスを使用して X.Y.W.K に動的に変換されます。

データと Jabber やブラウザなどの通信アプリケーションを使用する PC では、Jabber アプリケーション アドレスは NAT によって静的に変換され、ブラウザ アプリケーション アドレスは NAT によって動的に変換されます。

ファイアウォール内でスタティック NAT 変換が実行される場合でも、パケットの送信元 IP アドレスは転送中に次のように変換されます。パケットが Expressway-C から Expressway-E に到達すると Expressway-C の IP アドレスに変換され、パケットが Expressway-E からファイアウォールに到達すると Expressway-E の IP アドレスに変換されます。ファイアウォールでは、パケットが NAT によって静的に変換されてからインターネットに送信されます。

モバイルおよびリモート アクセス

コール制御サービスの場合は、図 4-7 に示すように、Expressway-C プロキシが独自の IP アドレスを使用してエンドポイントを Unified CM に登録します。

図 4-7　　パケットの寿命に基づく NAT

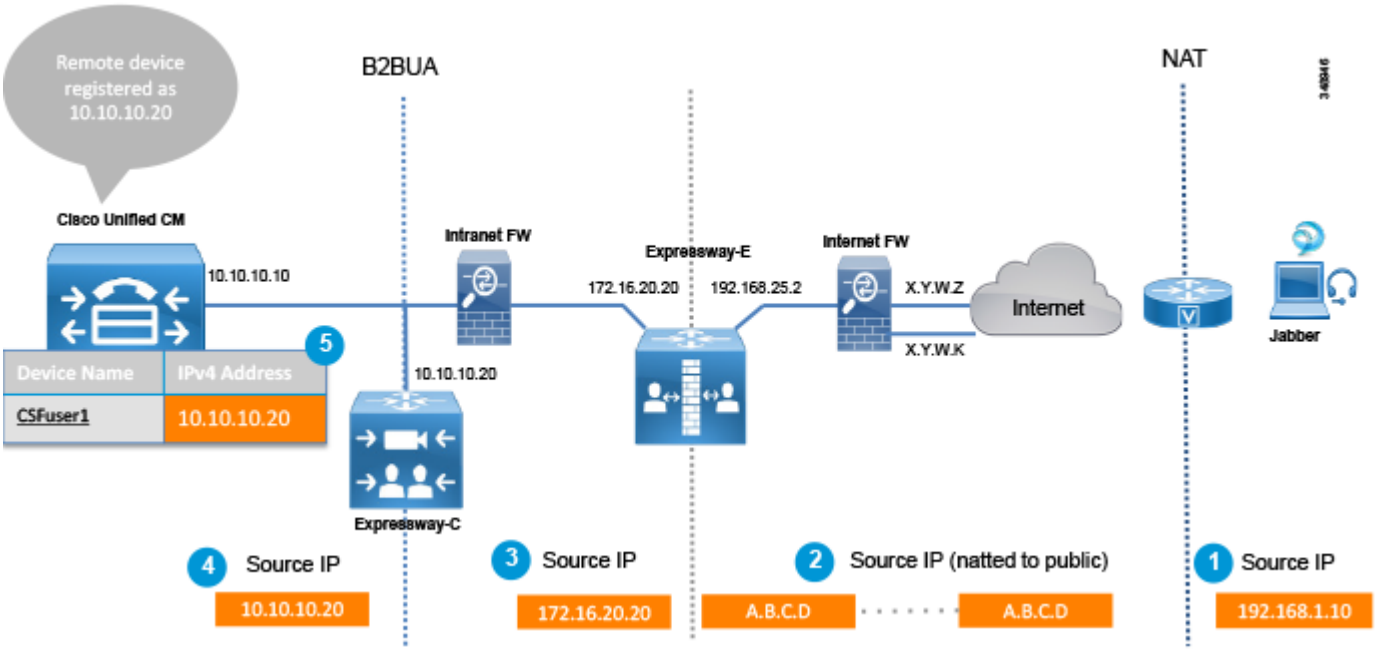


図 4-7 に示すアドレス変換プロセスは次のステップで構成されます。

1. エンドポイントにパブリック IP アドレスが割り当てられていない場合は、インターネットへのアクセスを提供するルータでエンドポイントの送信元 IP アドレスが NAT によって（192.168.1.10 から A.B.C.D に）変換されます。
2. パケットが Expressway-E に到着します。

3. Expressway-E が独自の内部 LAN インターフェイス アドレスを使用して Expressway-C にパケットを送信します（A.B.C.D から 172.16.20.20 に）。
4. Expressway-C がそのパケットを受け取って、接続を終了します。また、独自の IP アドレスを使用して、Unified CM 向けの別の接続を再発信します（172.16.20.20 から 10.10.10.20 に）。
5. エンドポイントが Expressway-C の IP アドレス（10.10.10.20）を使用して Unified CM に登録されます。

Expressway-C の IP アドレスを使用してデバイスを Unified CM に登録する場合は、次のような固有のメリットが得られます。たとえば、リモート デバイスが企業ネットワークに直接接続されていない場合にビデオ帯域幅を制限し、リモート デバイスがオンプレミスの場合にはビデオ帯域幅に別の値を割り当てたりできます。ここでは説明しませんが、この方法は Unified CM 上のモビリティ機能を使用して簡単に実現できます。このモビリティ機能は、IP アドレス範囲に基づく特定のポリシーの定義を可能にします。

エンドポイントがインターネット経由で登録された場合は、シスコ コラボレーション アーキテクチャでリモートから管理することはできません。これは、エンドポイントの IP アドレスが動的に変換され、ファイアウォールの背後に配置されるためです。リモート管理が必要な場合は、エンドポイントを VPN 経由で展開してください。

VPN Technologies はこのアーキテクチャの一部ではありませんが、必要に応じて追加することができます。

モバイルおよびリモート アクセスは Expressway-E 上と Expressway-C 上で有効にする必要があります。そうすれば、Unified CM と IM and Presence のパブリッシャ ノードの DNS 名を指定することによって、Unified CM クラスタと IM and Presence クラスタを検出するように Expressway-C を設定できます。

DMZ 内に展開された Expressway-E は、モバイルおよびリモート アクセス サービスを使用する Jabber クライアントと TelePresence エンドポイントに信頼できるエントリ ポイントを提供します。また、リモート Jabber クライアントと TelePresence エンドポイントだけでなく、インターネット経由の Business-to-Business（B2B）接続にも、認証、プロビジョニング、登録、コーリング サービス、IM and Presence、ボイスメッセージング、およびディレクトリ サービスを提供します。

Expressway-C は、HTTPs、SIP、および XMPP を使用して、Unified CM クラスタ、IM and Presence クラスタ、および Cisco Unity Connection に接続します（図 4-8 を参照）。

さらに、Jabber が HTTP 経由で特定のサーバに接続しなければならない場合が数多くあります。たとえば、ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどです。このようなケースでは、Jabber が Unified CM を経由せずに直接これらのサーバに接続します。Expressway-C は Jabber クライアントが接続を許可されたサーバを示す HTTP 許可リストを必要とします。

図 4-8　Unified CM、IM and Presence サービス、および Unity Connection への Expressway 接続

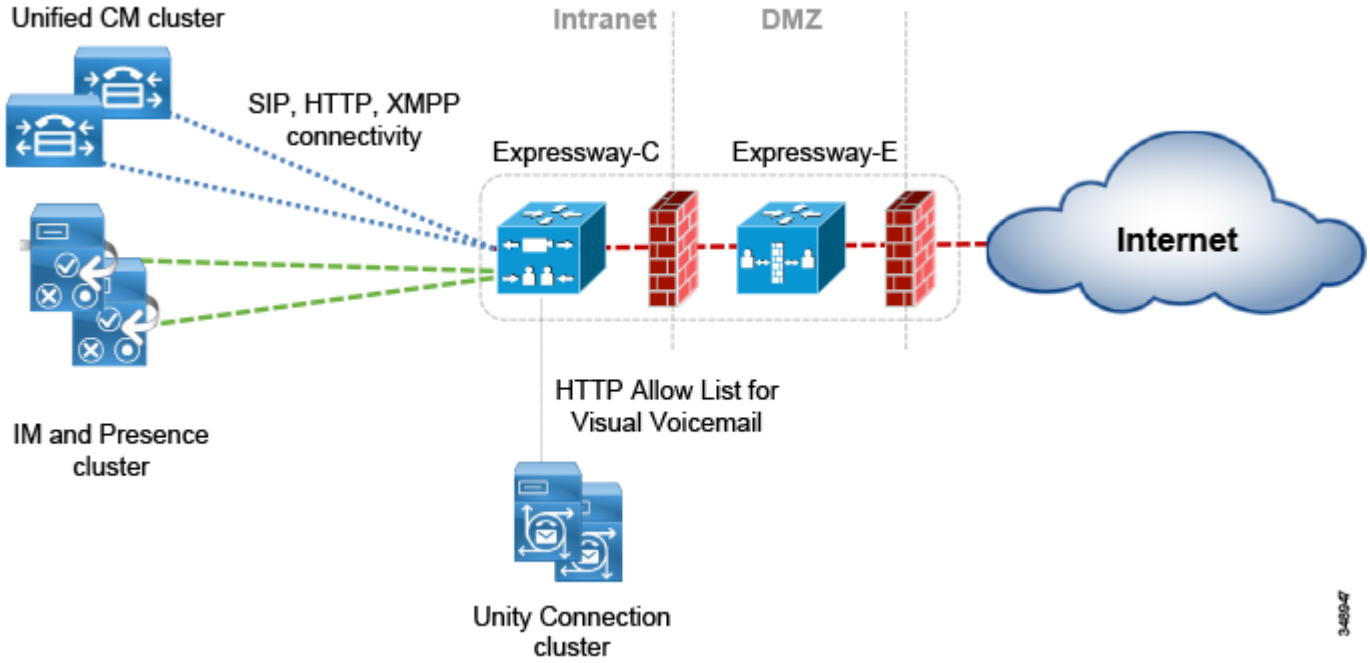


表 4-2 に、モバイルおよびリモート アクセスのために Expressway によって使用されるプロトコルの概要を示します。

表 4-2　モバイルおよびリモート アクセス用の Expressway プロトコル

プロトコル	セキュリティ	サービス
SIP	TLS	セッションの確立：登録や招待など
HTTPS	TLS	ログイン、プロビジョニング、設定、連絡先検索、ビジュアル ボイスメール
XMPP	TLS	インスタント メッセージ、プレゼンス
RTP	SRTP	音声、ビデオ、コンテンツ共有、高度なコントロール

Jabber または TelePresence エンドポイント ユーザがログインするときには、完全修飾名（user1@ent-pa.com など）を指定します。クライアントが次の特定の SRV レコードをパブリック DNS サーバにクエリします。

- _cisco-uds._tcp.ent-pa.com：企業 DNS サーバ上でのみ設定されます。
- _collab-edge._tls.ent-pa.com：パブリック DNS サーバ上でのみ設定され、Expressway-E クラスタのパブリック インターフェイスに解決されます。このレコードは常に TLS を示していることに注意してください。

クライアントがインターネット経由で接続されている場合は、パブリック DNS サーバから _cisco-uds に対する応答が返されず、クライアントが _collab-edge SRV レコードをクエリします。

その後で、DNS サーバが Expressway-E に関する A レコード（または Expressway-E がクラスタ化されている場合は複数のレコード）をクライアントに送信します。クライアントが Expressway-E の DNS 名を認識したら、プロビジョニングと登録の手順を開始できます。

プロビジョニングは HTTPs を使用して実行されるのに対して、登録では SIP と XMPP が使用されます。

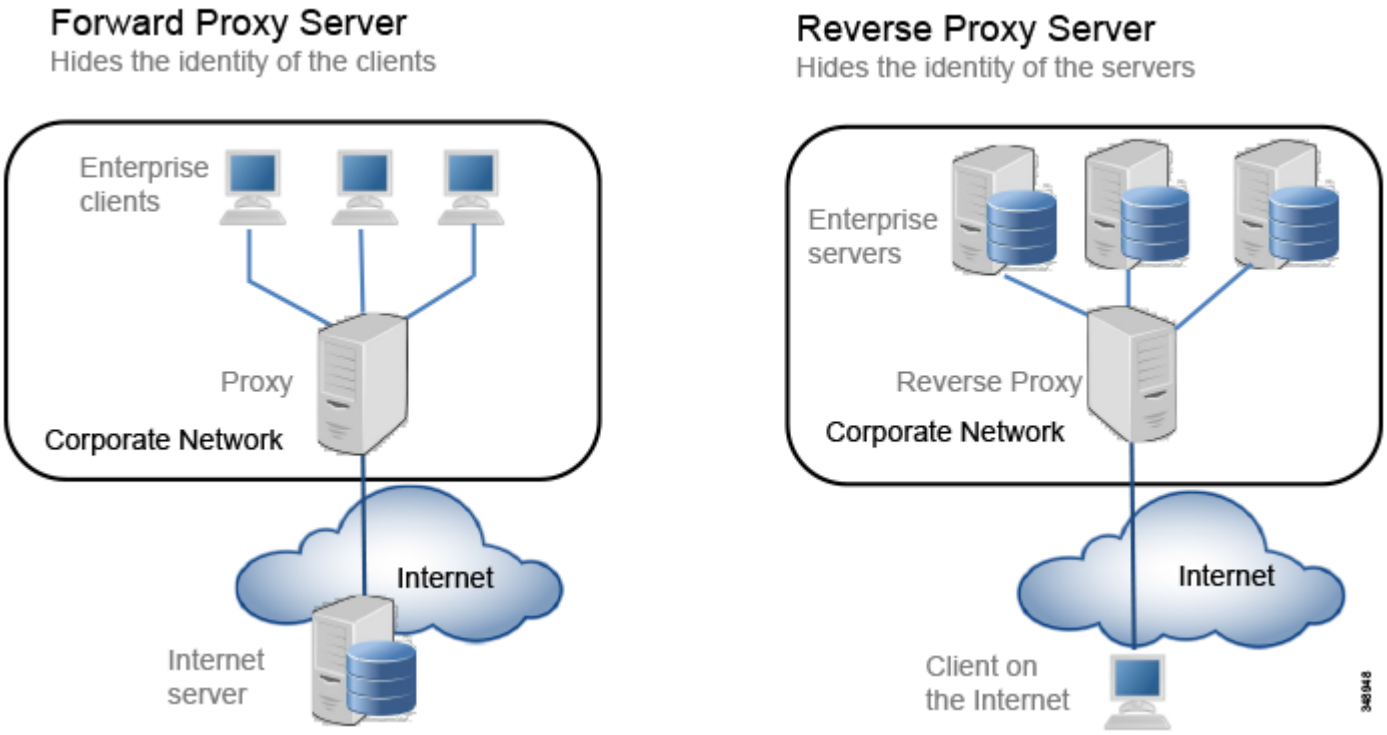
Expressway-C は、プロビジョニング プロセスを管理するための HTTPs 逆プロキシ サーバ機能を備えています。逆プロキシは、*プロキシ サーバ*とも呼ばれる最も一般的な転送プロキシ サーバの逆です。

図 4-9 に示すように、転送プロキシ サーバはインターネット サーバへの接続時にクライアント詳細を隠すことによってオンプレミス クライアントに関するサービス情報を提供するのに対して、逆プロキシ サーバはオンプレミス サーバ情報を隠すことによってオフプレミス クライアントに関する情報を提供します。転送プロキシ経由でインターネット サーバに接続している社内ネットワーク内のクライアントは接続先のサーバの ID は知っていますが、サーバはクライアントの ID を知りません。

一方、逆プロキシ経由で接続しているインターネット上のクライアントは、逆プロキシ サーバ経由で接続しているためオンプレミス サーバの ID を知りませんが、オンプレミス サーバは接続先のクライアントの ID を知っています。その後、この情報は、オンプレミス サーバから発信されたかのようにクライアントに戻されます。

Expressway-C は、Cisco Unified CM、IM and Presence、Unity Connection などのコラボレーション アプリケーション サーバの代わりに、プロビジョニング、登録、およびサービスの詳細をインターネット上のクライアントに提供する逆プロキシ機能を備えています。

図 4-9　　転送プロキシ サーバと 逆プロキシ サーバの比較



ビジュアル ボイスメール、Jabber 更新サーバ、カスタム HTML タブおよびアイコン、ディレクトリ フォト ホストなどのサービスに対して、Expressway-C は HTTP サービス用のアクセス リストの一種である *HTTP 許可リスト*でこれらのサービスが指定されている場合にこれらの接続を許可することにも留意してください。

プロビジョニングと登録は、クライアント、Expressway-C、Expressway-E、Unified CM、および IM and Presence サーバが関与する多段階プロセスです。

クライアントがコラボレーション エッジ経由で登録する場合に関係する主なステップの概要を以下に示します。

1. プロビジョニングは、クライアントから発行された **get_edge_config** 要求で開始されます。次に例を示します。

   https://expressway_e.ent-pa.com:8443/ZeW50LXBhLmNvbQ/get_edge_config?service_name=_cisco-uds&service_name=_cuplogin

   この要求と一緒に、クライアントはユーザのクレデンシャル（たとえば、ユーザ名「user1」とパスワード「user1」）を送信します。クエリは Expressway-E に送信されてから、Expressway-C に転送されます。

2. Expressway-C が Unified CM に対する UDS クエリを実行して user1 のホーム クラスタを特定します。これはマルチクラスタ シナリオでは必須です。

   GET cucm.ent-pa.com:8443/cucm-uds/clusterUser?username=user1

3. ホーム クラスタが見つかったら、応答が Expressway-C に送信されます。この応答には、クラスタ内のすべてのサーバが含まれます。

4. Expressway-C がクライアントの代わりに user1 に関する次のクエリを発行することによって、ホーム クラスタにプロビジョニング情報を問い合わせます。

   GET /cucm-uds/user/user1/devices はデバイス割り当てリストを取得します。

   GET /cucm-uds/servers はクラスタのサーバ リストを取得します。

   GET /cucm-uds/user/user1 は user1 のユーザ設定と回線設定を取得します。

   クエリに対する応答で、TFTP サーバも返されます。

http://us_cucm1.ent-pa.com:6970/SPDefault.cnf.xml などの以降のクエリは HTTP 経由の TFTP クエリです。こうして、プロビジョニング プロセスが UDS と TFTP サーバに対するクエリによって実行されます。これらのクエリの結果として、プロビジョニング情報がクライアントに転送され、クライアントは登録プロセスを開始することができます。

登録プロセスは次の 2 つのアクションで構成されます。

1. IM and Presence ログイン：Expressway-C 上の XCP ルータ機能経由で実現されます。XCP ルータが Expressway-C 上の IM and Presence クラスタに問い合わせて、ユーザが設定されている IM and Presence クライアントを探し、Jabber クライアントが IM and Presence サービスにログインできます。
2. SIP REGISTER メッセージを使用した Unified CM 登録：Expressway SIP プロキシ機能によってプロキシされます。

Business-to-Business（B2B）コミュニケーション

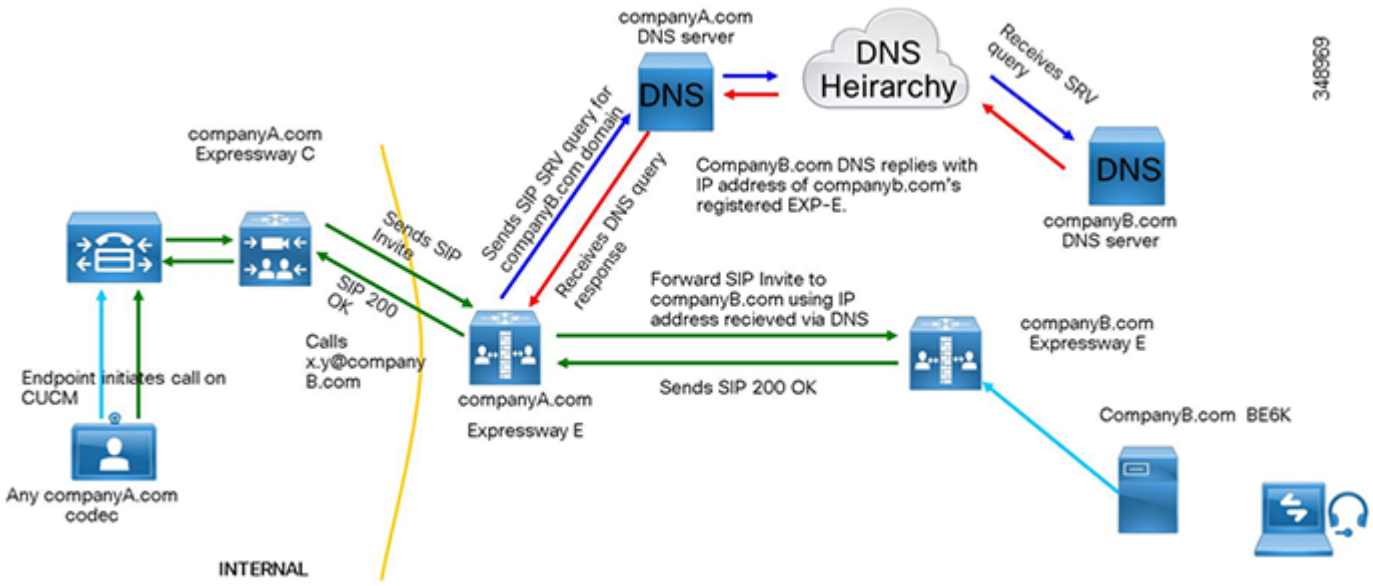
Business-to-Business（B2B）コミュニケーションには、URI ルーティングの目的でリモート組織のドメインを検索できる機能が必要です。これは、Expressway-E 上で DNS ゾーンを作成することによって実現されます。このゾーンはデフォルト設定を使って設定する必要があります。デフォルトで SIP と H.323 の両方が設定されます。これにより、Expressway-E は、自動的に、開始コールで使用されていない別のプロトコルを使用して DNS クエリを再発行できます。そのため、このコールは成功する可能性が高くなります。Expressway-C と Expressway-E は、コールを開始するために使用されたプロトコルを使用しますが、Expressway 上で SIP/H.323 間ゲートウェイ インターワーキングが有効になっている場合は自動的に別のプロトコルを使用しようとします。

Expressway-E では、SIP / H.323 間インターワーキングを [オン（On）] に設定する必要があります。これにより、コールが H.323 コールとして受信された場合に、Expressway-E がそのコールを SIP に接続し、Unified CM への残りのコール レッグにネイティブ SIP を使用できます。同様に、H.323 システムへの発信コールは、Expressway-E に到達して H.323 に接続されるまで SIP コールを維持します。

インターネット経由で Business-to-Business（B2B）コミュニケーションを受信するには、外部 SIP レコードと H.323 DNS レコードが必要です。これらのレコードを使用すれば、他の組織は URI のドメインをそのコール サービスを提供している Expressway-E に解決できます。シスコの検証済みデザインには、Business-to-Business（B2B）コミュニケーション用の SIP レコード、SIPS SRV レコード、および H.323cs SRV レコードが含まれています。H.323ls SRV レコードは、エンドポイントが登録用のゲートキーパーを探すために使用するもので、Expressway-E には必要ありません。

図 4-10 に、URI のドメインを解決する DNS プロセスを示し、例 4-1 に、SRV ルックアップの例を示します。

図 4-10　　DNS を使用した URI ダイヤリング



例 4-1　　ent-pa.com ドメインの SRV レコードの例

```
>nslookup
set type=srv
_sips._tcp.ent-pa.com

Non-authoritative answer:
_sips._tcp.ent-pa.comSRV service location
    priority= 1
    weight  = 10
    port    = 5061
    srv hostname= expe.ent-pa.com.
```

Expressway-E 上での DNS ゾーンの設定方法については、『*Cisco Expressway Basic Configuration Deployment Guide*』を参照してください。

Business-to-Business（B2B）コールの IP ベース ダイヤリング

IP ベース ダイヤリングは、H.323 エンドポイントを使ってダイヤルする場合のほとんどのシナリオで使用されるよく知られた機能です。シスコ コラボレーション アーキテクチャでは、SIP URI を使用するため、IP ベース ダイヤリングは必要ありません。ただし、コールの発着信に IP アドレスしか使用できない他の組織のエンドポイントと対話する場合は、シスコ コラボレーション アーキテクチャで着信コールと発信コールの両方に IP ベース ダイヤリングを使用できます。

アウトバウンド コール

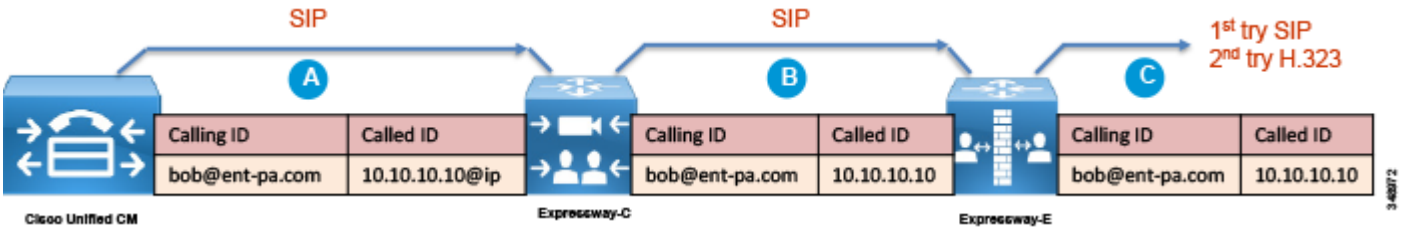
アウトバウンド IP ダイヤリングは Expressway-E と Expressway-C ではサポートされますが、Cisco Unified Communications Manager では完全なネイティブ サポートはありません。ただし、後述するように、IP ベース ダイヤリングを使用するように Unified CM をセットアップすることができます。

IP アドレス単独でダイヤルする代わりに、Cisco Unified CM 上のユーザは、10.10.10.10@ip のように SIP URI ベースの IP アドレスにダイヤルすることができます。ここで、「@ip」は、リテラルで、「external」、「offsite」、またはその他の意味のある単語に置き換えることができます。

Unified CM は、設定された SIP ルート パターンを照合して、「ip」架空ドメインを Expressway-C にルーティングします。Expressway-C はドメイン「@ip」を除外して、そのコールを IP アドレス ダイヤリング用にも設定されている Expressway-E に送信します。

Expressway -E 上の不明な IP アドレス宛てのコールは [直接（Direct）] に設定する必要があります。コール制御が展開されていない場合は IP ベース アドレス ダイヤリングのほとんどが H.323 エンドポイントで設定されるため、Expressway-E は H.323 コールをパブリック IP アドレスにあるエンドポイントに直接送信できます。図 4-11 に示すように、コールは Expressway-E 上で接続されるまで SIP コールを維持します。

図 4-11　　アウトバウンド IP ベース ダイヤリングの例



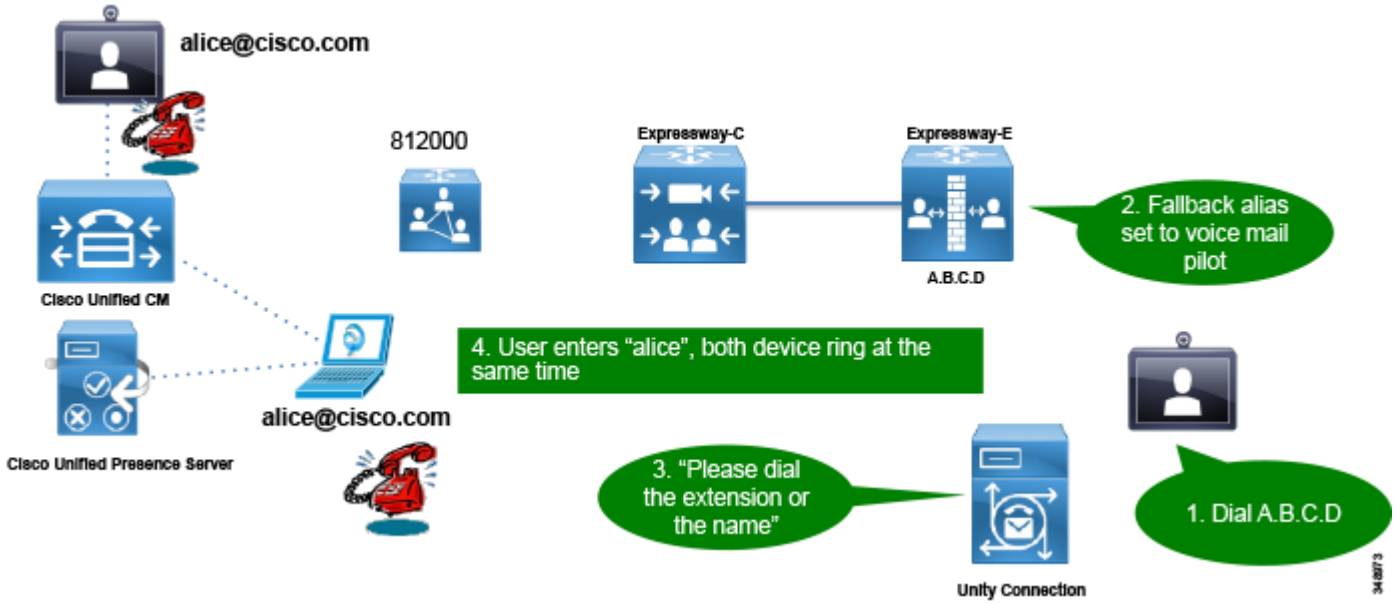
着信コール

IP ベースの着信コールは、Expressway-E で設定された *フォールバック エイリアス* を利用します。インターネット上のユーザが Expressway-E 外部 LAN インターフェイスの IP アドレスにダイヤルすると、Expressway-E がそのコールを受信して、フォールバック エイリアス設定内のエイリアスに送信します。たとえば、フォールバック エイリアスがコールを会議番号 80044123 または会議エイリアス meet@ent-pa.com に送信するように設定されている場合は、着信コールはその会議を担当する TelePresence サーバに送信されます。

IP アドレスとフォールバック エイリアス間の静的マッピングが制限されている場合は、フォールバック エイリアスを Cisco Unity Connection のパイロット番号に設定できます。この方法では、Unity Connection 自動応答機能を使用して、DTMF 経由で、または、Unity Connection でサポート可能な場合は音声認識によって、最終宛先を指定できます。

Unity Connection が Expressway-E の IP アドレスにダイヤルする外部エンドポイントの自動応答機能として使用されている場合は、Unity Connection の Unified CM トランク設定で [再ルーティング用コーリングサーチスペース（Rerouting Calling Search Space）] に設定することを忘れないでください。図 4-12 に、セットアップを示します。

図 4-12　　インバウンド IP ベース ダイヤリングの例



Expressway-C と Expressway-E 経由の外部 XMPP フェデレーションの展開

XMPP フェデレーションは、モバイルおよびリモート アクセスと同じタイプのトラバーサル接続（Unified Communications トラバーサル）を利用します。XMPP フェデレーションはスタンドアロン サービスとして展開できます。また、同じ Unified Communications トラバーサル リンクを利用するモバイルおよびリモート アクセスと一緒に、同じ Expressway-C と Expressway-E のペア上に展開することもできます。

インスタント メッセージおよびプレゼンス フェデレーションを展開するには、次の標準作業を実行します。

1. フェデレーション用のメールアドレスを検証します。

   Expressway 経由の XMPP フェデレーションは、メールアドレスから XMPP アドレスへの変換をサポートしていません。メールアドレスから Jabber ID への変換は、IM and Presence サーバ フェデレーション モデルの機能です。この機能は、ユーザ エクスペリエンスを向上させ、電子メール URI 表記と JID URI 表記が異なる場合に XMPP フェデレーションに関する通信を簡略化するためによく使用されます。Expressway 経由で XMPP フェデレーションを展開する場合は、ユーザ エクスペリエンスの向上と通信の簡略化という同じ目的が適用されます。IM and Presence ドメインは電子メール ドメインと同じドメインに設定することをお勧めします。また、UserID、メールアドレス表記、および Jabber ID に対して LDAP sAMaccount 名を使用することもお勧めします。コラボレーション アーキテクチャ全体では、反復可能でスケーラブルな URI 表記に関する包括的で一貫した戦略を策定することをお勧めします。

2. IM and Presence サービスが稼働可能で、XMPP フェデレーションがオフになっていることを確認してください。

   IM and Presence サーバ上の XMPP フェデレーションは、Expressway 上で設定されたフェデレーションと競合しないようにするため、オフにする必要があります。

3. サーバ証明書要件を解決します。

   Expressway-C と Expressway-E の証明書をセットアップする前に計画します。XMPP フェデレーションの一部としてチャット ノード エイリアスを使用する予定の場合は、チャット ノード エイリアス FQDN を証明書のサブジェクト代替名（SAN）フィールドに含める必要があります。これを事前に行うことによって、新しい証明書を生成する必要がなくなるだけでなく、Expressway-E 上での公開証明書に対する経費の増加が抑えられます。

4. Expressway-C 上で XMPP フェデレーション用のローカル ドメインを設定します。

5. Expressway-E を XMPP フェデレーションとセキュリティ用に設定します。

   このステップによって、フェデレーションと、外部フェデレーションに必要なセキュリティ レベルが有効になります。認証は必須であり、ダイヤルバック シークレット経由でセットアップされます。TLS 経由の通信保護が推奨設定です。許可または拒否する外部ドメインと外部チャット ノード エイリアスの承認もこのセクションで設定されます。

6. フェデレーテッド ドメインとチャット ノード エイリアス用の XMPP サーバを DNS ルックアップまたは静的ルートを使用してどのように配置するかを設定します。

   Expressway シリーズは、DNS SRV レコード経由のフェデレーションと静的ルート経由のフェデレーションをサポートしています。静的ルートは、DNS クエリを実行せずに外部ドメインに到達するパスを定義します。パブリック XMPP SRV レコードは、フェデレーションをサポートする外部ドメインを解決するために使用されます。これらのレコードは、オープン フェデレーション モデルを展開するときに、他の組織があなたの組織に到達するために必要です。

7. 正しいファイアウォール ポートが開いていることを確認します。

8. XMPP フェデレーションのステータスをチェックします。

SIP トランク経由の PSTN 音声接続用の Cisco Unified Border Element の展開

Cisco Unified Border Element は、PSTN 集中型アクセスに推奨されているセッション ボーダー コントローラです。これは、企業ネットワークと通信事業者ネットワークの間に境界ポイントとして展開されます。外部インターフェース経由の IP PSTN へのアクセスと、内部インターフェイス経由の企業ネットワークへのアクセスを提供します。集中型 PSTN サービスを有効にするため、企業ネットワークが通信事業者のネットワークに接続されている場所に展開する必要があります。

すべてのリモート サイトが中央の PSTN 接続を利用するため、Cisco Unified Border Element は高い冗長性を備えている必要があります。PSTN 中央サービスが使用できない場合は、ローカル PSTN アクセスを備えたオフィスだけが外部コールを発信できます。そのため、Cisco Unified Border Element をペアで展開して冗長性を確保することをお勧めします。

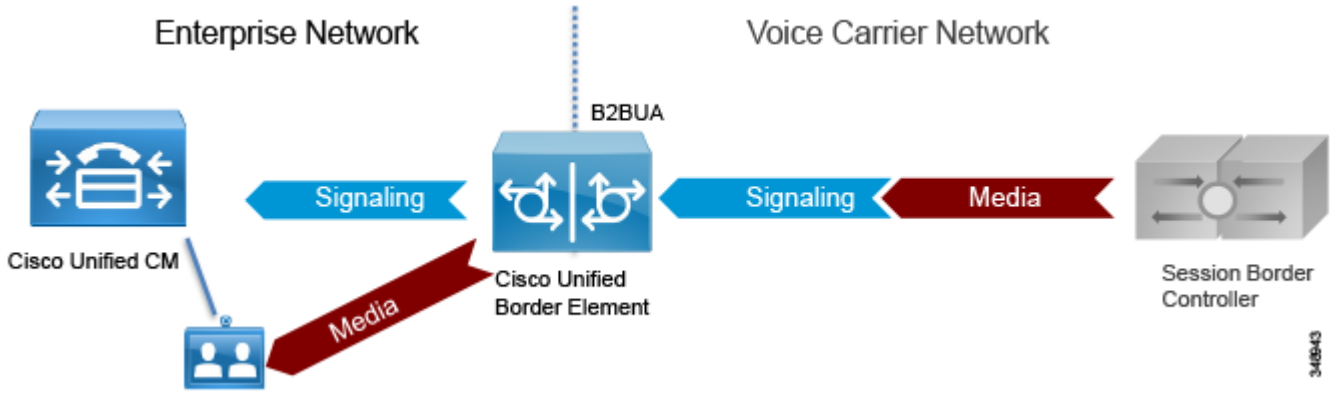
Unified Border Element は、Cisco IOS サービス統合型ルータ（ISR）プラットフォームとアグリゲーション サービス ルータ（ASR）プラットフォーム上でサポートされる Cisco IOS フィーチャ セットです。正しいプラットフォームの選択方法については、サイジングの章を参照してください。

Cisco Unified Border Element は、Unified CM からのセッションを終了して通信事業者ネットワークに向けて再発信する、または、その逆を実行するセッション ボーダー コントローラです。インターネット上で公開される Expressway-E とは対照的に、Cisco Unified Border Element はプライベート ネットワーク（社内ネットワークと通信事業者のネットワーク）間に展開されることに注意してください。通信事業者の視点では、集中型 PSTN へのトラフィックが Cisco Unified Border Element の外部インターフェイスから開始されます。企業の視点では、通信事業者からのトラフィックが Cisco Unified Border Element の内部インターフェイスから開始されます。この意味で、Cisco Unified Border Element はトポロジ隠蔽を実行しています。

Cisco Unified Border Element の展開は Expressway のそれとは異なります。前者は通信事業者ネットワーク（プライベートな管理および保護されたネットワーク）へのアクセスを提供するのに対して、後者はインターネットへのアクセスを提供します。そのため、Cisco Unified Border Element の展開では DMZ が必要ありません。

図 4-13 に示すように、この推奨アーキテクチャでは、Unified Border Element が、通信事業者ネットワークに対する WAN インターフェイスと企業ネットワークに対する LAN インターフェイスを備えています。

図 4-13　　IP PSTN アーキテクチャ

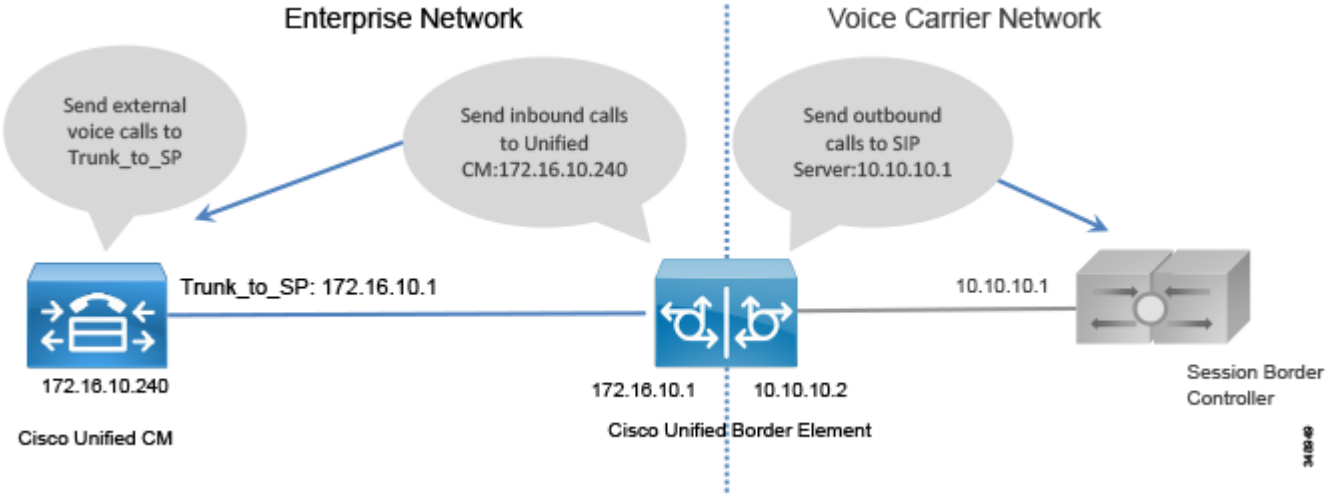


Cisco Unified Border Element は次の機能を実行します。

- 図 4-14 に示すアドレス変換とポート変換を含むトポロジ隠蔽。Unified CM からのすべてのトラフィックが Unified Border Element 内部インターフェイスに送信され、通信事業者ソフトスイッチからのすべてのトラフィックが Unified Border Element 外部インターフェイスに送信されます。これらの間の直接接続は存在しません。図 4-14 に、Cisco Unified CM 上のトランキング設定と Unified Border Element 上の音声ルートの詳細を示します。
- 遅延オファーから早期オファーへの変換とその逆変換
- メディア インターワーキング：インバンドおよびアウトオブバンド DTMF サポート、DTMF 変換、FAX パススルーおよび T.38 FAX リレー、音量およびゲイン制御
- コール アドミッション制御（CAC）：CAC は、CPU、メモリ、コール到着スパイク検出などのリソース消費に基づいて Unified Border Element によって実行できます。CAC はインターフェイス レベルでまたはグローバルに実装できます。Unified CM 上で設定される CAC はロケーションベースですが、Unified Border Element 上で設定される CAC はリソースベースです。Unified Border Element のオーバーサブスクリプションを避ける目的、およびセキュリティ上の理由から、リソースベースの CAC を推奨します（コラボレーション エッジのセキュリティに関するセクションを参照）。

- RTP/SRTP 間インターワーキング、SIP 不正パケットの検出、非ダイアログ RTP パケットの破棄、SIP リスニング ポートの設定、ダイジェスト認証、同時コール数制限、コール レート制限、電話料金の詐欺行為からの保護、および複数のシグナリングとメディアの暗号化オプションを含むセキュリティ機能
- 保留、転送、および会議を含む通話中補足サービス
- PPI/PAI/プライバシーおよび RPID：通信事業者との ID ヘッダー インターワーキング
- 複数の通信事業者からの SIP トランクに対する同時接続
- マルチキャスト保留音（MoH）からユニキャスト MoH への変換
- 課金統計情報と呼詳細レコード（CDR）の収集

図 4-14　Cisco Unified Border Element のトランキングに関する留意点



PSTN ゲートウェイ

レガシー PSTN ゲートウェイは、サイトごとに独自の PSTN 接続が割り当てられる分散アーキテクチャで展開されます。集中型 PSTN アクセスには Cisco Unified Border Element の使用をお勧めしますが、日常業務の実行を外部コールに大きく依存しているサイトのバックアップとして PSTN ゲートウェイを使用することもできます。

この場合は、同時 ISDN チャネル数が集中型 PSTN への同時コール数を大きく下回る可能性があります。これは、それらがバックアップ シナリオでしか使用されないためです。たとえば、通常の状況で集中型 PSTN への 30 本の同時コールが許容される場合は、バックアップ シナリオでしか使用されないバックアップ ISDN ゲートウェイを 2 つの BRI チャネルだけをサポートする規模に設定できます。

シスコ音声ゲートウェイは以下をサポートしています。

- DTMF リレー機能
- 補足サービス サポート：補足サービスは、保留、転送、会議などの基本的なテレフォニー機能です。
- FAX パススルーと T.38 FAX リレー

PSTN ゲートウェイはさまざまなプロトコル（SCCP、MGCP、H.323、SIP）をサポートしています。SIP は、シスコ コラボレーション ソリューション全体と調和しているうえ、新しい音声製品やビデオ製品に選択されたプロトコルであるため、お勧めのプロトコルです。

音声ゲートウェイ機能は、適切な PVDM とサービス モジュールまたはカードが実装されたすべての Cisco ISR 上で有効になっています。

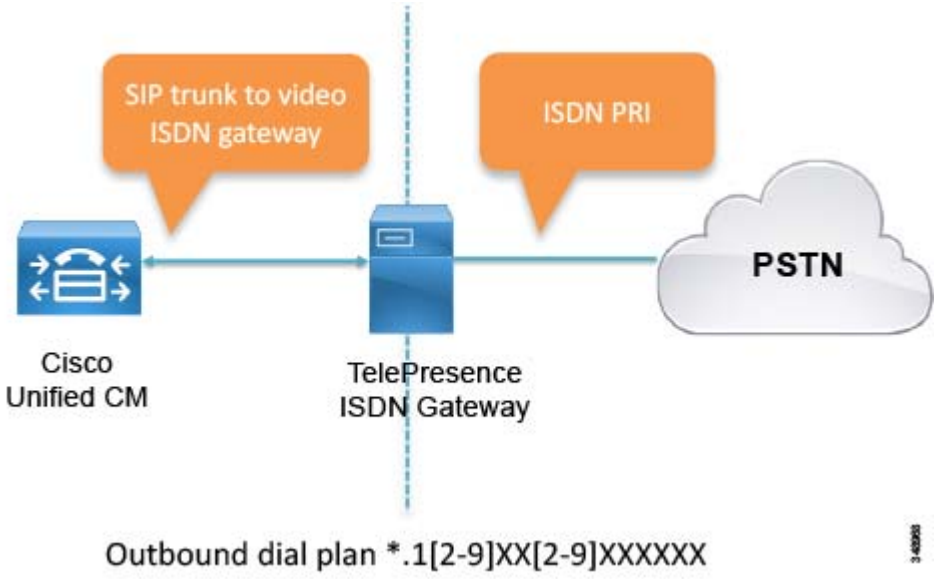
ビデオ ISDN ゲートウェイ

推奨する企業コラボレーション用アーキテクチャは、ISDN PRI トランクと Unified CM への SIP トランクを使用した Cisco TelePresence ISDN Gateway の展開を包含しています。Cisco TelePresence ISDN Gateway には、MSE 8321 ゲートウェイと GW 3241 ゲートウェイが含まれます。TelePresence ISDN Gateway は、オプション アイテムであり、レガシー ISDN ビデオ会議システムからのコールを送受信しなければならない場合にのみ必要です。

要件と推奨事項

- Unified CM と通信するための IP プロトコルとして H.323 ではなく SIP を使用します。
- ISDN ゲートウェイ上ではできるだけシンプルなダイヤル プランを作成し、Unified CM 上ですべてのダイヤル文字列操作を実行します。
- ダイヤル プラン セットアップは最後まで残しておきます。ISDN ゲートウェイは、デフォルトで、ダイヤル プラン設定が構成されるまですべてのコールをブロックします。これにより、使用する準備が整うまでゲートウェイが保護されます。
- コールを TelePresence ISDN ゲートウェイにルーティングするために ISDN 番号の前にプレフィクスとして * を付けます。* によって、ビデオ ISDN コールと音声 PSTN コールが区別され、既存の国際番号計画との競合が避けられます。また、ダイヤリング時のユーザ エクスペリエンスの変更が最小限に抑えられます。Unified CM ダイヤル プランでは、* が削除され、残りの数字が TelePresence ISDN ゲートウェイにルーティングされます（図 4-15 を参照）。

図 4-15　　ビデオ ISDN ゲートウェイ ダイヤル プラン



ISDN ビデオ ゲートウェイの制限と制約

- ISDN ビデオ コール中にサポートされるのは、保留機能と再開機能のみです。
- ビデオコール転送はサポートされません。
- CMR Cloud への ISDN コールはサポートされません。

モバイルおよびリモート アクセスの制限と制約

次の制限と制約がモバイルおよびリモート アクセス接続に適用されます。

- CTI はサポートされません。
- Jabber デスクフォン制御はサポートされません。
- Jabber ファイル転送はサポートされません。
- Jabber モバイル機能の Dial-Via-Office Reverse（DVO-R）、デュアルモード ハンドオフ、およびセッション持続性はサポートされません。
- TelePresence Conductor ベースの TelePresence に対するワンボタン プッシュはサポートされません。
- TelePresence Conductor エンドポイント管理機能はサポートされません。

Cisco Unified Border Element の制限と制約

- Cisco ISR では、トランスポート プロトコルを TCP と UDP にしかすることができません。Cisco ASR では、トランスポート プロトコルを TLS にすることもできます。
- トランスコーディング、DTMF インターワーキング、IVR、SIP/TLS 変換と RTP/SRTP 変換、および FAX とモデムの各機能は、フェールオーバー シナリオで使用されます。Cisco ISR では、DSP 関連機能が使用されません。

コラボレーション エッジのハイ アベイラビリティ

ハイ アベイラビリティは、コラボレーション システムの設計と展開における重要な側面です。コラボレーション エッジによって、冗長性、ロード シェアリング、およびコール ライセンス共有が実現されます。

Expressway-C と Expressway-E のハイ アベイラビリティ

Expressway-C と Expressway-E はクラスタで展開することをお勧めします。クラスタごとに最大 6 つの Expressway ノードと最大 N+2 の物理冗長性を設定できます。クラスタ内のすべてのノードがアクティブです。クラスタ設定の詳細については、『*Cisco Expressway Cluster Creation and Maintenance Deployment Guide*』を参照してください。

Expressway クラスタは設定の冗長性を提供します。クラスタ内で設定される最初のノードは*パブリッシャ*で、その他のすべてのノードは*サブスクライバ*です。設定はパブリッシャ内で実行され、自動的に他のノードにレプリケートされます。

Expressway クラスタは、コール ライセンス共有と回復力を提供します。すべてのリッチ メディア セッションと TURN ライセンスがクラスタ内の全ノードで等しく共有されます。コール ライセンスはノードごとに設定されたライセンスによって供与されます。

仮想マシンとして展開された Expressway-C と Expressway-E は VMware VMotion をサポートします。VMware VMotion は、物理サーバ間の実行中の仮想マシンのライブ マイグレーションを可能にします。仮想マシンの移動中は、Expressway-C サーバと Expressway-E サーバが、シグナリングのみを処理するとき、または、シグナリングとメディアの両方を処理するときにアクティブ コールを維持します。これにより、Expressway ノードのハイ アベイラビリティだけでなく、Cisco Unified Computing System（UCS）ホスト全体でのコール回復力も提供されます。

次のルールが Expressway クラスタリングに適用されます。

- Expressway-C ノード タイプと Expressway-E ノード タイプを同じクラスタ内に混在させることはできません。
- クラスタ内のすべてのノードで、サブゾーン、ゾーン、リンク、パイプ、認証、帯域幅制御、およびコール ポリシーの設定を同一にする必要があります。
- 設定の変更はパブリッシャ ノードでのみ行う必要があり、この変更によってレプリケーション時にクラスタ内のサブスクライバ ノード上の設定が上書きされます。
- あるノードが使用できなくなった場合は、そのノードがクラスタに供与していたライセンスが 2 週間後に使用できなくなります。
- Expressway-C クラスタと Expressway-E クラスタには同じ数のノードを展開します。
- クラスタ全体に同じ OVA テンプレートを展開します。
- クラスタ内のすべてのノードは、他のすべてのクラスタ ノードへの最大ラウンドトリップ時間を 30 ms 以内にする必要があります。したがって、WAN 経由のクラスタリングは遅延の制約があるためお勧めできません。
- 同じクラスタ内のすべてのノードに対して同じクラスタ事前共有キーを使用する必要があります。
- データベース レプリケーションのために、クラスタ内のすべてのノードで H.323 を有効にする必要があります。H.323 シグナリングは、帯域幅使用状況情報を検索してクラスタ内の他のノードと共有するエンドポイント ロケーションで使用されます。
- 同じ Expressway-C と Expressway-E のペアでモバイルおよびリモート アクセスと Business-to-Business（B2B）コミュニケーションが有効になっている場合は、Unified CM と Expressway-C 間の SIP トランク上で使用されている SIP ポート番号をデフォルトの 5060 または 5061 から変更する必要があります。
- DNS SRV レコードは、クラスタに対して使用可能にする必要があり、クラスタのノードごとに A レコードまたは AAAA レコードを含む必要があります。

Expressway-C は内部ネットワークに、Expressway-E は DMZ に展開されるため、モバイルおよびリモート アクセス用の *トラバーサル ゾーン*を介して Expressway-C と Expressway-E を接続する必要があります。Expressway-C がモバイルおよびリモート アクセス用の *トラバーサル クライアント*で、Expressway-E が *トラバーサル サーバ*です。Cisco Expressway ソフトウェア バージョン X8.2 以降のリリースでは、クライアント ゾーンとサーバ ゾーンの両方が *Unified Communications トラバーサル ゾーン*と呼ばれます。Business-to-Business（B2B）コールでは別々のトラバーサル ゾーンが必要なため、Expressway-C 用のトラバーサル クライアント ゾーンと Expressway-E 用のトラバーサル サーバ ゾーンという名前が残されています。トラバーサル サーバ ゾーンとトラバーサル クライアント ゾーンには Expressway-C と Expressway-E のすべてのノードが含まれているため、ノードのいずれかが到達不能になった場合は、代わりにクラスタの別のノードが使用されます。

図 4-16 に示すように、Expressway-C が Cisco Unified CM、IM and Presence、および Unity Connection の各クラスタのすべてのサーバに接続するため、接続パス全体でハイ アベイラビリティと冗長性が確保されます。

図 4-16　Expressway サービス接続

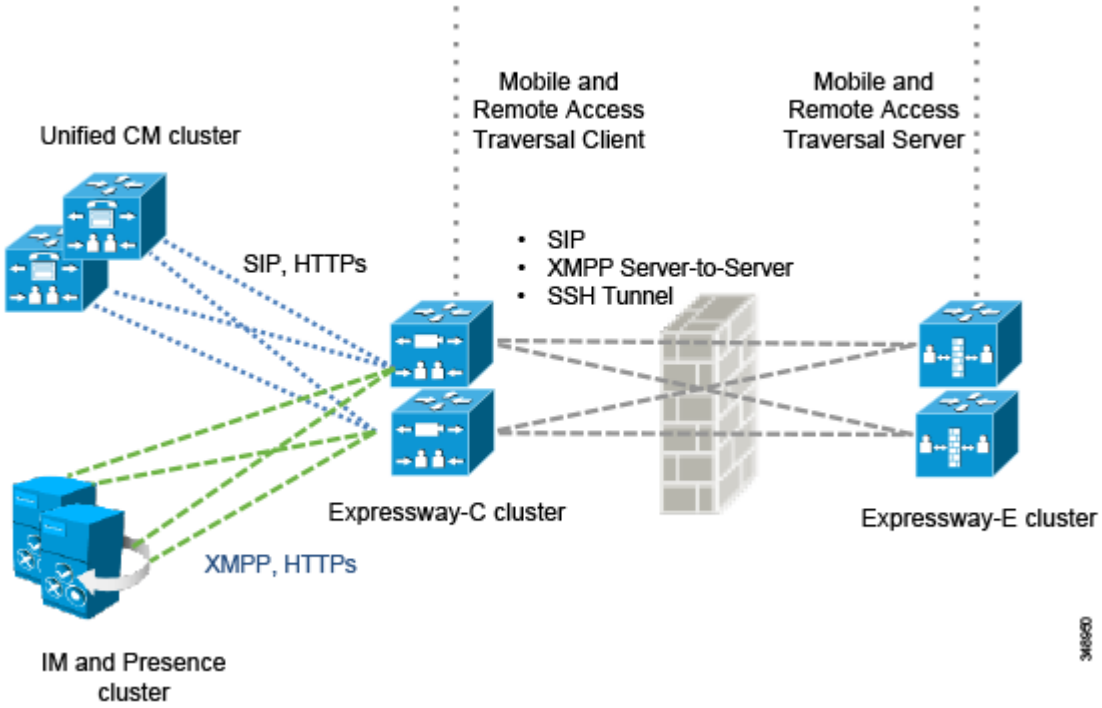


図 4-16 に、Unified Communications トラバーサル ゾーンとモバイルおよびリモート アクセスに組み込まれているハイ アベイラビリティを示します。ただし、次の説明は、Unified Communications トラバーサル ゾーンと標準の（クライアントとサーバ）トラバーサル ゾーンの両方に適用されます。

Expressway-C 上に設定されたトラバーサル クライアント ゾーンには、対応する Expressway-E クラスタのすべてのクラスタ ノードの完全修飾ドメイン名を含める必要があります。同様に、トラバーサル サーバ ゾーンはすべての Expressway-C クラスタ ノードに接続する必要があります。これは、Expressway-C 証明書のサブジェクトの別名に Expressway-C クラスタ ノードの FQDN を含め、**TLS 検証サブジェクト名**を Expressway-C クラスタの FQDN と同一に設定することによって実現されます。これにより、トラバーサル ゾーン全体にクラスタ ノードのメッシュ構成が形成され、最後のクラスタ ノードが使用不能になるまでトラバーサル ゾーンのハイ アベイラビリティが維持されます。

Expressway-C はトランク経由で Unified CM に接続して、Business-to-Business（B2B）の着信コールと発信コールをルーティングします。Unified CM も Expressway-C にトランキングします。ハイ アベイラビリティを維持するために、各 Expressway-C クラスタ ノードの完全修飾ドメイン名を Unified CM 上のトランク設定に列挙する必要があります。Unified CM がクラスタ化されている場合は、クラスタの各メンバーの完全修飾ドメイン名（FQDN）を Expressway-C のネイバー ゾーン プロファイルにリストする必要があります。

ここでも、メッシュ状のトランク構成が形成されます。Unified CM は、SIP Options Ping 経由でトランク設定内のノードのステータスをチェックします。あるノードが使用できなくなると、Unified CM はそのノードを運用停止にして、そのノードに対するコールをルーティングしなくなります。Expressway-C も SIP OPTIONS Ping 経由で Unified CM からのトランクのステータスをチェックします。コールは、アクティブかつ使用可能として示されているノードにのみルーティングされます。これにより、トランク設定の両側にハイ アベイラビリティが提供されます。

DNS SRV レコードは、インバウンド Business-to-Business（B2B）トラフィックに対する Expressway-E の可用性を高めることができます。ハイ アベイラビリティを維持するためには、クラスタ内のすべてのノードを SRV レコード内に同じ優先度でリストする必要があります。これにより、すべてのノードを DNS クエリで返すことができます。DNS SRV レコードは、クライアントがルックアップに費やす時間を最小にするために役立ちます。これは、DNS 応答に SRV レコード内に列挙されたすべてのノードを含めることができるためです。 通常は、遠端サーバまたは遠端エンドポイントが DNS 応答をキャッシュし、応答が受信されるまで DNS クエリで返されたすべてのノードを試します。これにより、コールが成功する確率が高まります。

加えて、Expressway クラスタは、クラスタ全体での Rich Media ライセンス共有と TURN ライセンス共有をサポートします。クラスタからノードが削除された場合は、そのコール ライセンスの共有が次の 2 週間だけ継続されます。どの Expressway も、その物理能力を上回るライセンスを保持することはできても、その物理能力を上回る Rich Media ライセンスを処理することはできません。

Cisco Unified Border Element のハイ アベイラビリティ

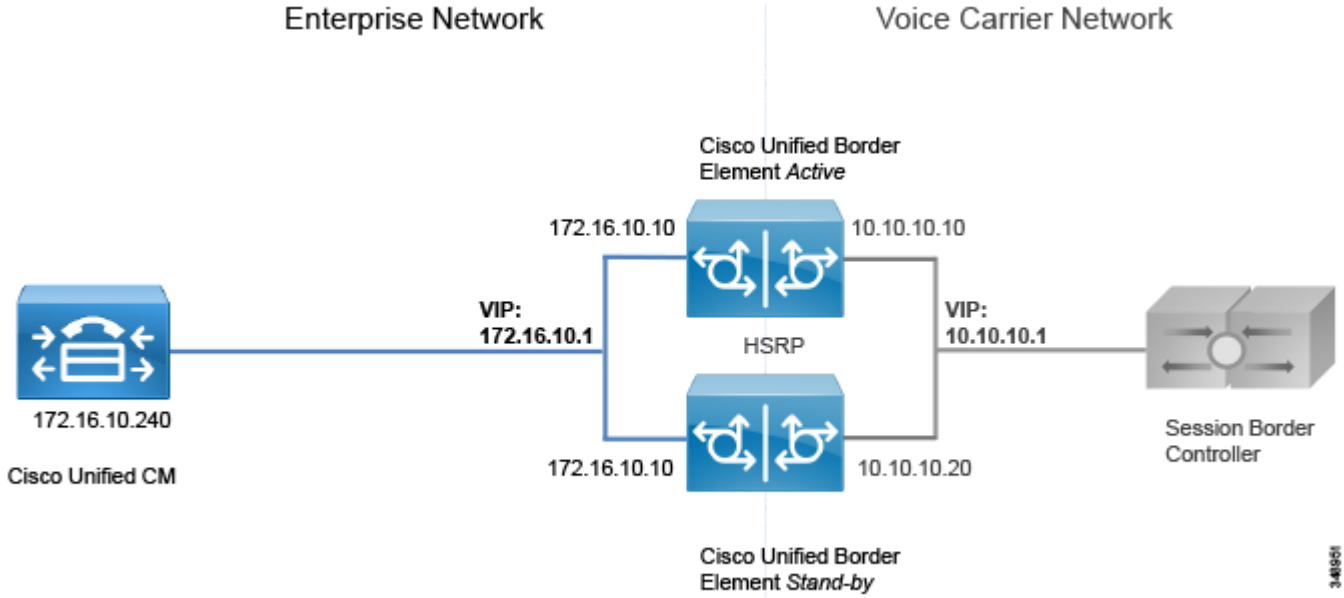
Cisco Unified Border Element のハイ アベイラビリティは複数の方法で実現できます。推奨アーキテクチャでは、コールの保存によるボックスツーボックス冗長性をお勧めします。これは、Unified Border Element で障害が発生した場合にシグナリングとメディアの両方のコールの保存が実施されるためです。

Unified Border Element サーバは、次のアクティブ/スタンバイ モデルのペアで展開されます。アクティブ Unified Border Element がダウンすると、スタンバイ Unified Border Element が起動され、すべてのアクティブ セッションが移行されます。これにより、シグナリングとメディアの両方のハイ アベイラビリティが提供されます（図 4-17 を参照）。

Hot Standby Routing Protocol（HSRP）テクノロジーは、1 つのルータの可用性に頼らずに、ネットワーク上のホストからの IP トラフィックをルーティングすることによって、ネットワークのハイ アベイラビリティを実現します。ルータのグループで HSRP を使用して、アクティブ ルータとスタンバイ ルータを選択します HSRP は内部と外部の両方のインターフェイスをモニタします。インターフェイスのいずれかがダウンした場合は、デバイス全体がダウンしたと見なされ、スタンバイ デバイスがアクティブになってアクティブ ルータの役割を引き継ぎます。

ボックスツーボックス冗長性は、HSRP プロトコルを使用してルータの HSRP アクティブ/スタンバイ ペアを形成します。アクティブ サーバとスタンバイ サーバは、同じ仮想 IP アドレスを共有し、ステータス メッセージを継続的に交換します。図 4-17 に示すように、Unified Border Element セッション情報がルータのアクティブ/スタンバイ ペア全体で共有されます。ここで、172.16.0.1 と 10.10.10.10 は Cisco Unified Border Element ペアの仮想 IP アドレスです。これにより、アクティブ ルータが予定どおりにまたは予定外の理由で稼働停止状態になった場合に、すぐにスタンバイ ルータがすべての Unified Border Element コール処理の役割を引き継ぐことができます。

図 4-17　Cisco Unified Border Element のボックス ツーボックス冗長性



音声ゲートウェイのハイ アベイラビリティ

PSTN ゲートウェイは、物理インターフェイスを介して直接 PSTN ネットワークに接続します。ゲートウェイがダウンすると、PSTN とのすべての通信がクリアされます。HSRP などのメカニズムは、このケースではメリットがありませんが、通信事業者向けの IP トランク経由の PSTN アクセスのケースではメリットがあります。ゲートウェイ相互接続を使用した集中型 PSTN が展開される場合もありますが、Unified Border Element と違って、TDM ベースの PSTN ゲートウェイ展開は基本的に分散型です。また、PSTN 音声ゲートウェイは Unified Border Element ほど多くのコール量を管理できません。PSTN の特性上、このシナリオではメディア保存ができません。

ただし、同じ Unified CM ルート グループ内の複数のゲートウェイをコールがロード バランシングされるように設定することによって、シグナリング回復力を提供できます。グループ内のゲートウェイのいずれかがダウンすると、すべてのコールが破棄されますが、残りの使用可能なゲートウェイのいずれかを使用して新しいコールが確立されます。

コラボレーション エッジのセキュリティ

ここでは、コラボレーション エッジでのセキュリティの実装方法について説明します。

Expressway-C と Expressway-E のセキュリティ

Expressway-C と Expressway-E 上のセキュリティは、ネットワーク レベルとアプリケーション レベルでさらに分割することができます。ネットワーク レベル セキュリティにはファイアウォール ルールや侵入からの保護などの機能が含まれるのに対して、アプリケーション レベル セキュリティには承認、認証、および暗号化が含まれます。

ネットワーク レベル保護

Expressway-C と Expressway-E 上のネットワーク レベル保護は、2 つの主なコンポーネント（ファイアウォール ルールと侵入からの保護）で構成されます。

ファイアウォール ルールは次の機能を有効にします。

- トラフィックを許可または拒否する送信元 IP アドレスのサブネットを指定する。
- 拒否対象のトラフィックを破棄または拒否するかを選択する。
- SSH や HTTP/HTTPS などの既知のサービスを設定する、または、トランスポート プロトコルとポート範囲に基づいてカスタマイズされたルールを指定する。
- Expressway-E 上の LAN 1 インターフェイスと LAN 2 インターフェイスで別々のルールを設定する。

悪意のあるトラフィックを検出してブロックし、ログイン セキュリティを破壊するディクショナリベースの試行から Expressway を保護するためには、自動侵入保護機能を使用する必要があります。

自動侵入保護は、システム ログ ファイルを解析して、SIP、SSH、Web/HTTPS などの特定のサービス カテゴリへのアクセスの連続的な失敗を検出することによって機能します。指定された時間内の失敗回数が設定されたしきい値を超えた場合は、送信元ホスト IP アドレス（侵入者）と宛先ポートが、指定された期間ブロックされます。その期間が過ぎると、自動的にホスト アドレスがブロック解除されるため、一時的に設定が間違っていた正式なホストがロックアウトされなくなります。

モバイルおよびリモート アクセス

モバイルおよびリモート アクセスでは、TLS と SRTP がインターネット上のクライアントと Expressway-E の間の唯一の設定オプションです。Expressway-C と Expressway-E の間のモバイルおよびリモート アクセス トラバーサル ゾーンは TLS を使用して暗号化されます。

Unified CM と Expressway-C の間の接続は設定に応じて、暗号化と認証が行われます。Unified CM が混合モードの場合は、メディアとシグナリングのエンドツーエンド暗号化をお勧めします。

これらの接続時はセキュリティ証明書が必要です。証明書は、サーバとクライアントのアイデンティティを提供し、Expressway-C、Expressway-E、Unified CM、および Unified CM IM and Presence Service に展開する必要があります。自己署名証明書を展開することもできますが、認証局（CA）を使用して証明書に署名する設定をお勧めします。

CA はプライベートにもパブリックにもできます。プライベート CA 展開にはコスト効率が高いというメリットがありますが、この証明書は組織内部でしか有効ではありません。パブリック CA はセキュリティを向上させ、すべての組織から信頼されます。そのため、異なる組織間の通信に広く利用されています。

Expressway-C と Expressway-E をモバイルおよびリモート アクセス専用に使用している会社では、プライベート CA を展開することも、パブリック CA に依存することもできます。ただし、Expressway-C と Expressway-E が Business-to-Business（B2B）コミュニケーションにも使用されている場合は、パブリック CA によって署名された証明書を Expressway-E 上に展開する必要があります。この場合は、Expressway-E 証明書が VeriSign/Symantec、GeoTrust、GoDaddy などのパブリック CA によって署名される必要があります。Expressway-E が信頼された CA 証明書リストに存在する CA によって証明書が署名されている事業体から Business-to-Business（B2B）コールを受信した場合は、そのコールが許可されます。証明書に署名した CA がそのリストに掲載されていない場合は、そのコールは拒否されます。そのため、Expressway が Business-to-Business（B2B）に対しても有効になっている場合は、主要な CA 証明書の信頼リストを Expressway-E に事前に入力しておくことが重要です。

コストを削減するために、Expressway-C 証明書が社外で認定されていない内部 CA によって署名されている場合があります。この場合は、Expressway-C と Expressway-E の接続を確立するために、内部 CA 証明書を Expressway-E の信頼された CA 証明書リストに含めることが重要です。表 4-3 に、証明書展開に対するパブリック アプローチとプライベート アプローチの概要を示します。

表 4-3　　パブリック証明機関、プライベート証明機関、および証明書

	Unified CM	IM and Presence Service	Expressway-C	Expressway-E
証明書の署名者	内部 CA	内部 CA	内部 CA	パブリック CA
信頼リストへの掲載	内部 CA 証明書	内部 CA 証明書	内部 CA 証明書とパブリック CA 証明書	内部 CA 証明書とパブリック CA 証明書

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの保護には、認証、暗号化、および承認が含まれます。Business-to-Business（B2B）コミュニケーションでは、デフォルトで、認証されたトラバーサル リンクが使用されます。トラバーサル リンクは、Expressway-C と Expressway-E 間の相互認証 Transport Layer Security（MTLS）接続によって検証された Public Key Infrastructure（PKI）の使用からも恩恵を受けることができます。Business-to-Business（B2B）トラバーサル リンクがモバイルおよびリモート アクセスと同じ Expressway-C と Expressway-E のインフラストラクチャ上に展開されている場合は、トラバーサル ゾーンで Expressway-C と Expressway-E のクラスタ ノードの FQDN が使用されていることを確認してください。これにより、各サーバの証明書を使用して、提示された証明書をトラバーサル接続に対して信頼された証明書に照らして検証するのが容易になります。

着信コールは認証済みか未認証かによって区別できます。この区別は、保護されたリソースへのアクセスの承認に使用できます。不明なリモート Business-to-Business（B2B）コールは、未認証として処理され、IP 音声およびビデオ ゲートウェイなどの保護されたリソースへのアクセスが制限されます。これは、Call Processing Language（CPL）ルールをゲートウェイ アクセスに使用されるプレフィクスへのアクセスをブロックする正規表現を使用して設定することによって実現されます（図 4-18 を参照）。

図 4-18　　未認証発信者に関する CPL ルール

シグナリングとメディアの暗号化は Business-to-Business（B2B）コールにとって重要ですが、コールの受信機能を限定または制限しないように慎重に展開する必要があります。通信先の旧式の SIP または H.323 システムの中には、シグナリングまたはメディアの暗号化をサポートしていないものが多数含まれています。

要件と推奨事項

- Business-to-Business（B2B）コールのメディア暗号化を Expressway-C 上に展開する必要があります。ただし、Expressway-E 上で NAT が設定されている場合は、Expressway-E 上に展開することができません。
- Business-to-Business（B2B）トラバーサル ゾーンのトラバーサル クライアント側のメディア暗号化を**ベスト エフォート**に設定します。これは、コールの暗号化が常に最初に試されることを意味します。また、暗号化されていないコールへのフォールバックも可能になります。
- Unified CM と Expressway-C 間の SIP トランクのシグナリング暗号化には TLS を使用します。

組織内にモバイルおよびリモート アクセス（MRA）も展開されている場合は、MRA コールと Business-to-Business（B2B）コールの両方が暗号化されずに出力される可能性があります。ベスト エフォート メディア暗号化は、発信コールが最初に暗号化を使用して試されることを意味します。

Cisco Unified Border Element のセキュリティ

インターネット接続とは異なり、IP トランク経由の PSTN 接続は、通信事業者から提供されたプライベート ネットワークを介して配信されます。つまり、この接続は制御されたネットワークです。したがって、インターネット エッジ用に展開されたセキュリティは、IP PSTN アクセス用に展開されたセキュリティとは異なります。Cisco Unified Border Element と通信事業者間にはファイアウォールが存在しません。ただし、特定のケースでは、企業と電気通信プロバイダーでエンタープライズ DMZ を使用する必要があります。

通信事業者と企業のネットワーク間では、トラフィックが暗号化されずに送信されます。会社のポリシーによって、内部のエンタープライズ トラフィックを暗号化できる場合とできない場合があります。このようなケースでは、Unified Border Element で TLS/TCP 変換と SRTP/RTP 変換を実行できます。複数のゲートウェイが展開されている場合は、内部 CA を使用して Unified Border Element 証明書に署名することをお勧めします。

Unified Border Element はファイアウォールなしで展開されるため、さまざまなレイヤで保護されます。たとえば、通信事業者のセッション ボーダー コントロールのみに PSTN 側からのコールの開始を許可し、Unified CM のみに内部ネットワーク側からのコールの開始を許可するアクセス コントロール リストを作成できます。

Unified Border Element は、電話料金の詐欺行為やテレフォニー サービス拒否（TDoS）攻撃からも保護されます。ラージ パケット到着率は、CPU、メモリ、帯域利用率、およびコール到着スパイク検出に基づくコール アドミッション制御メカニズムを通して削減することもできます。

音声ゲートウェイのセキュリティ

PSTN ゲートウェイは、顧客ネットワークに 1 つのインターフェイス、PSTN 上に 2 つ目のインターフェイスを備えています。これらのインターフェイスは社内ネットワーク内に展開され、インターネットからは到達できません。PSTN は本質的にセキュアなので、ゲートウェイを保護するための特定のツールは存在しません。ただし、インターネットにアクセス可能なルータ上にゲートウェイが展開されている場合は例外です。この場合は、ゲートウェイ上の Cisco IOS 機能を使用してファイアウォールと侵入からの保護を実行できます。その他の場合は、ゲートウェイを保護するために必要な特定のツール（サービス拒否（DoS）からの保護など）はありません。

ただし、常に、エンドポイントからゲートウェイへのメディアを暗号化することができます。このようなケースでは、ゲートウェイで TLS と SRTP が使用されます。この場合は、CA 署名証明書を使用することをお勧めします。

ビデオ ISDN ゲートウェイのセキュリティ

ビデオ ISDN ゲートウェイは、顧客ネットワークに IP インターフェイス、PSTN にもう 1 つのインターフェイスを備えています。ゲートウェイで保護する必要のある 2 つの一般的なセキュリティに対する脅威が IP から ISDN への電話料金の詐欺行為とコールの ISDN へアピニングです。

Expressway-E 上の基本的な CPL ルールを使用して、インターネットからの ISDN ゲートウェイリソースへのアクセスをブロックできます。Unified CM 登録デバイスからのアクセスをブロックする場合は、コーリング サーチ スペースを使用する必要があります。

コラボレーション エッジ ソリューションのスケーリング

展開されたコラボレーション エッジ クラスタの数は、コール制御クラスタの数ではなく、インターネットへの接続ポイントの数に左右されます。複数の Unified CM および IM and Presence クラスタと、複数の TelePresence Conductor クラスタを使用しているお客様は、単一のインターネット ブレークアウト ポイントが設置されていれば、単一のインターネット エッジを所有していることになります。通信事業者が PSTN ネットワークへの接続ポイントを複数提供している場合は、同じ環境に複数の PSTN ホップオフが設置されている可能性があります。同じ考え方はビデオ ISDN アクセスに適用されます。

インターネット エッジ ソリューションのスケーリング

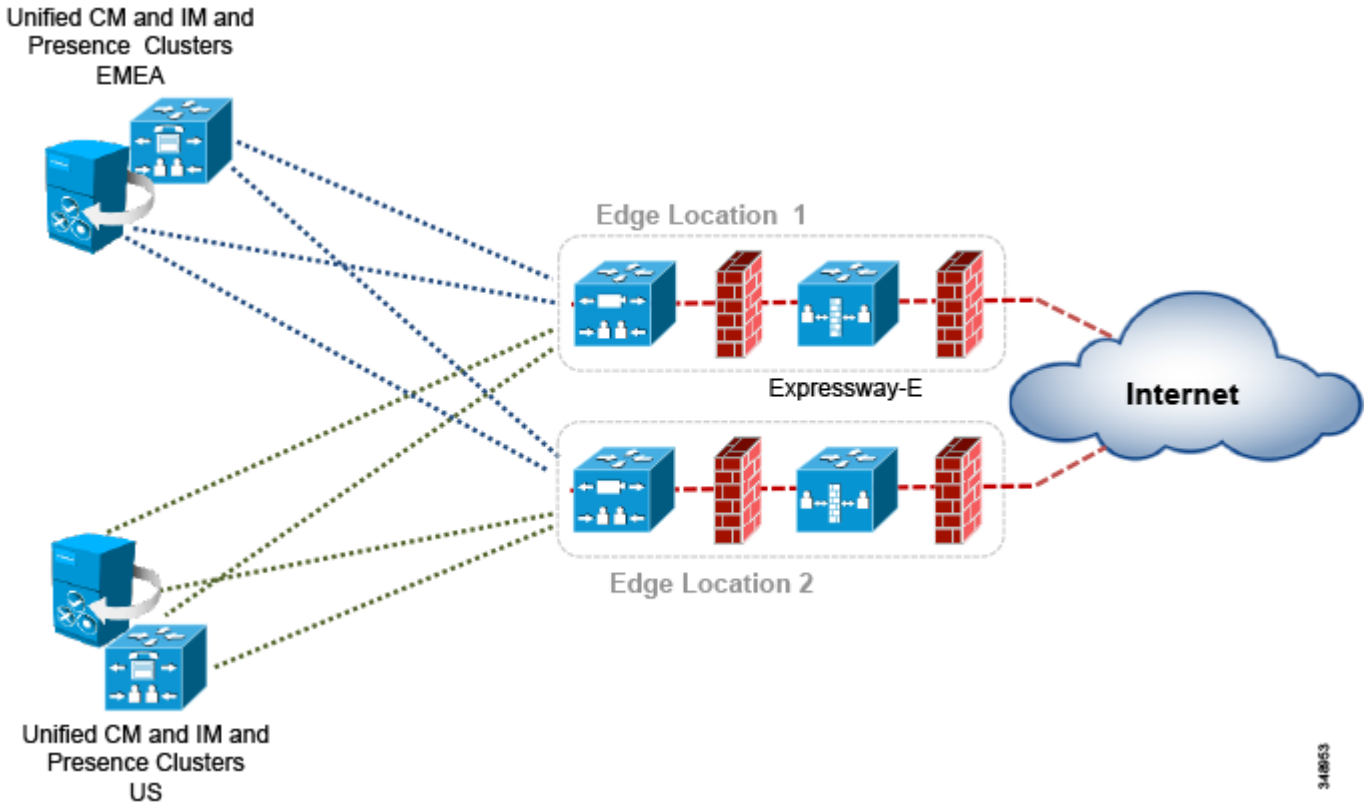
複数のインターネット エッジが展開されている場合は、コラボレーション トラフィックを最も近いインターネット エッジに送信するためのルーティング ルールを正しく設定することが重要です。

モバイルおよびリモート アクセス

複数の Unified CM および IM and Presence クラスタが展開されている場合は、すべての Expressway-C がすべての Unified CM クラスタを検出する必要があります。Expressway-C が一部のクラスタしか検出しない場合は、検出されたクラスタに属しているユーザに関する登録しかプロキシできません。

登録要求が Expressway-C によって検出されていない Unified CM および IM and Presence クラスタに属しているクライアントから発行された場合、そのクライアントはログインできません。これは、図 4-19 に示すように、ユーザがモビリティに対して有効になっている場合は、それぞれの Expressway-C がすべての Unified CM および IM and Presence クラスタを検出することが重要だからです。

図 4-19　　複数の Unified CM および IM and Presence クラスタのサービス検出



複数のインターネット エッジが展開されている場合は、それらの間の負荷分散方法を理解しておくことが重要です。インターネット エッジが同じデータセンターまたは同じエリアに展開されている場合は、DNS SRV レベルでロード バランシングを実行できます。たとえば、企業ネットワークにモバイルおよびリモート アクセス用の 3 つのインターネット エッジが含まれており、それぞれが 2 つの Expressway-E ノードと Expressway-C ノードのクラスタで構成されている場合は、_collab-edge._tls.ent-pa.com に 6 つすべての Expressway-E レコードが同じ優先度と重要度で追加されます。これにより、登録とコールがさまざまな Expressway-E クラスタと Expressway-C クラスタに均等に分配されます。

モバイルおよびリモート アクセス接続エンドポイントが特定の Expressway クラスタ ペアを介して登録されると、クライアントが切断されるか、クライアントのスイッチがオフにされるまで接続されたままになります。

ただし、Expressway クラスタが地理的地域全体に展開されている場合は、エンドポイントが確実に最も近い Expressway-E クラスタを使用するようにするため、DNS SRV の優先度と重要度のレコードに加えて何らかのインテリジェント メカニズムが必要になります。

たとえば、ある企業が 2 つの Expressway クラスタを使用しており、1 つは米国（US）に、もう 1 つはヨーロッパ（EMEA）に設置されている場合、US に住んでいるユーザは US 内の Expressway-E クラスタに転送され、ヨーロッパに住んでいるユーザはヨーロッパ内の Expressway-E クラスタに転送されるのが理想的です。これは、GeoDNS サービスを実装することによって容易に実現できます。GeoDNS サービスはコスト効率が高く、設定が簡単です。GeoDNS サービスがどのように機能するかを示すために、次の例では Amazon Route 53 Geo DNS サーバを使用します。Amazon Route 53、Edge Director、GeoScaling、Max Mind GeoIP2 など、さまざまな GeoDNS サービスが市場で利用可能です。

GeoDNS を使用すれば、位置（IP アドレス ルーティング）や遅延（最小遅延）などの複数のポリシーに基づいてトラフィックをルーティングできます。Amazon Route 53 は、遅延と地理的位置の両方によるルーティングを可能にします。ここでは、遅延ベースのルーティングを設定することにしますが、この設定手順は IP アドレスに基づく地理的位置ルーティングと同じです。

遅延ベースのルーティングを使用した場合は、インターネット上の遅延が変化すると、同じサイト内のクライアントが時間と共に別のデータセンターにアクセスすることになります。ただし、この現象は、一定期間の平均値として評価されるため、遅延の変化直後に発生するわけではありません。つまり、インターネットの瞬時輻輳によるスパイクは平均値によって吸収されます。

このシナリオでは、2 つのインターネット エッジ Expressway クラスタを US とヨーロッパに 1 つずつ展開し、それぞれが 2 つの Expressway-C サーバと Expressway-E サーバで構成されます。エンドポイントとヨーロッパ エッジ間で測定された遅延がエンドポイントと US エッジ間の遅延を下回った場合は、エンドポイントがヨーロッパ エッジに転送されて登録されます。

このシナリオに従って、単一の SRV レコード _collab-edge._tls.ent-pa.com をモバイルおよびリモート アクセス用に設定します。このレコードは、リソースの実際の A レコードに解決されるエイリアスである CNAME レコードの expe.ent-pa.com に解決されます。expe.ent-pa.com 用のレコードは 2 つ存在します。1 つは us-expe.ent-pa.com（US エッジの DNS 名）に解決され、もう 1 つは emea-expe.ent-pa.com（EMEA エッジの DNS 名）に解決されます。A レコードの us.expe.ent-pa.com と emea-expe.ent-pa.com は、US とヨーロッパの Expressway-E サーバ ノードの IP アドレスに解決されます。

_collab-edge._tls.ent-pa.com は標準ルーティングに設定されますが、expe.ent-pa.com レコードはルーティング ポリシーが「latency」に設定されます。そのため、Expressway-E クラスタの場所を指定する必要があります。クライアントと emea-expe.ent-pa.com 間の遅延がクライアントと us-expe.ent-pa.com 間の遅延を下回った場合は、登録要求がヨーロッパ Expressway-E に送信されます。何らかの理由で徐々に遅延が変化して US への遅延を上回った場合は、代わりに、us-expe.ent-pa.com が選択されます。

emea-expe.ent-pa.com と us-expe.ent-pa.com の両方が A レコードで、Jabber クライアントまたは TelePresence Conductor システムが _collab-edge._tls.ent-pa.com SRV レコードの応答に基づいて、emea-expe.ent-pa.com または us-expe.ent-pa.com に対する以降のクエリを実行します。ただし、標準の A レコードでは SRV レコードのように優先度と重要度を設定できないため、クライアントが接続すべき Expressway-E クラスタのサーバを指定するために別のロードバランシングおよび冗長性メカニズムが必要です。これは、ラウンドロビン メカニズムを使用して実現できます。たとえば、2 つの emea-expe.ent-pa.com レコードを作成して、それぞれのルーティング ポリシーを「weighted」に設定したとします。2 つのレコードに対して同じ重要度を指定すれば、クラスタのサーバ間で同一のロードバランシング プロセスが実行されることになります。最初のレコードは、同じクラスタの複数の Expressway-E サーバ（この場合は 2 つのサーバ）に解決されます。2 つ目のレコードは、同じサーバのセットに解決されますが、順序が逆になります。

図 4-20 に、地域の Expressway-E クラスタ間の遅延ベースのルーティングと同じクラスタ内部のラウンドロビンを使用した GeoDNS の DNS レコード構造を示します。図からわかるように、両方のレコードの emea-expe.ent-pa.com が Expressway-E ノードの同じセットに解決されますが、順序が異なっています。これにより、冗長性とロード バランシングの両方が提供されます。

図 4-20　遅延ベース ルーティング用 Route 53 DNS レコード構造

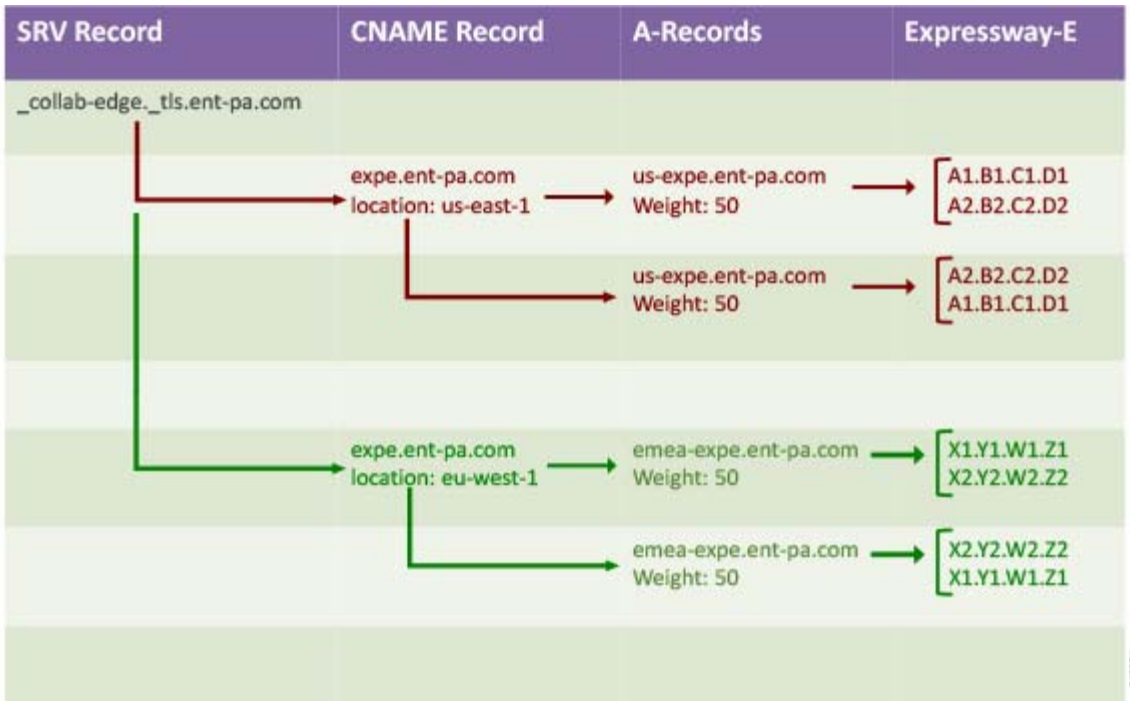


図 4-21 に示すように、Expressway クラスタ ノードごとに、A レコードを作成する必要があります。

図 4-21　Expressway ノードの DNS A レコード

A-Records for Expressway-E	IP addresses for Expressway-E
us-expe1.ent-pa.com	X1.Y1.W1.Z1
us-expe2.ent-pa.com	X2.Y2.W2.Z2
emea-expe1.ent-pa.com	A1.B1.C1.D1
emea-expe2.ent-pa.com	A2.B2.C2.D2

新しい Expressway 位置展開ごとに、1 つの新しい CNAME レコードと、Expressway クラスタ内のノード数と同数の A レコードが必要です。加えて、個々の Expressway-E ノードの A レコードも必要です。

Business-to-Business（B2B）コミュニケーション

Business-to-Business（B2B）コミュニケーションの拡張性は、複数の Expressway-C クラスタと Expressway-E クラスタを同じ物理位置にまたは地理的に分散して追加することによって解決できます。

複数の Expressway-C と Expressway-E のペアが展開されている場合は、Unified CM が発信コールを発信側エンドポイントに最も近いエッジ サーバに転送できるため、内部 WAN トラフィックが最低限に抑えられます。加えて、複数のエッジ クライアントが利用されている場合は、Expressway-C が Unified CM クラスタを使用してメッシュ状のトランク構成を形成する必要があります。これにより、地理的に見つけたトラバーサルがいっぱいになった場合または使用できない場合に、追加のアウトバウンド トラバーサル パスを許可することで拡張性と復元力が高まります。

大規模展開では、モバイルおよびリモート アクセスから分離した Expressway-C と Expressway-E のペア上で Business-to-Business（B2B）コミュニケーションをホストした方が適切な場合があります。これにより、サーバ リソースを外部インターネット通信専用にすることができます。

着信コールに関する留意点

DNS SRV レコードは、SIP と H.323 ent-pa.com ドメインに対して承認された Expressway-E クラスタを特定するために使用されます。重要度と優先度が同じ SRV レコードは、Expressway-E クラスタ ノード全体でコールのバランスを取るために使用されます。

地理的に分散した複数の Expressway-E クラスタ全体で着信コールをスケーリングする場合は、トラフィックのロード バランシングが主要課題になります。Expressway-C と Expressway-E は SIP または H.323 トラフィックのロード バランシングをサポートしません。そのため、DNS クエリに対する応答のロード バランシングがソリューションの重要なスケーリング手段になります。

モバイルおよびリモート アクセス サービスと同様に、GeoDNS は同じクエリに対する別々の DNS 応答を送信するために使用されます。ネットワーク遅延や地理的位置などのさまざまなメトリックを使用して、DNS 応答で正しい Expressway-E クラスタを指定する必要があります。GeoDNS サービスを提供しているインターネット サービス プロバイダーによっては、Expressway-E サーバのステータス モニタリングも含める必要があります。これにより、アウトオブサービス Expressway-E を含まないなどのより効率的な DNS 応答が可能になります。

GeoDNS は、お客様が選択したメトリックに基づいて、接続先の他のサーバまたはエンドポイントに最適なエッジ Expressway-E を提供する非常に優れた手段です。この場合の応答は、通常、クエリの発行元のサーバに物理的に最も近いエッジに基づいて行われます。このメカニズムは、SRV レコードが異なることを除いて、前述したメカニズムと同じです。たとえば、SIP TLS の SRV レコードは _sips._tcp.ent-pa.com になります。図 4-20 は、GeoDNS サービスのセットアップに使用できます。ここで、_collab-edge._tls.ent-pa.com は _sips._tcp.ent-pa.com に置き換えられます。

別のソリューションとしては、宛先のエンドポイントまたはデバイスに最も近いエッジを返すように設計します。この場合は、宛先エンドポイントの位置を検索または確認して、該当するエッジを返す必要があります。このソリューションのメリットは、最短の内部パスをエンドポイントに提供することによって顧客ネットワーク上の帯域幅の使用が最小限に抑えられることです。

これは、Geo DNS を使用しながら、着信側のエンドポイントが別の地域に属している場合にコールをその地域の Expressway-E に転送するように Expressway-E を設定することによって実現できます。

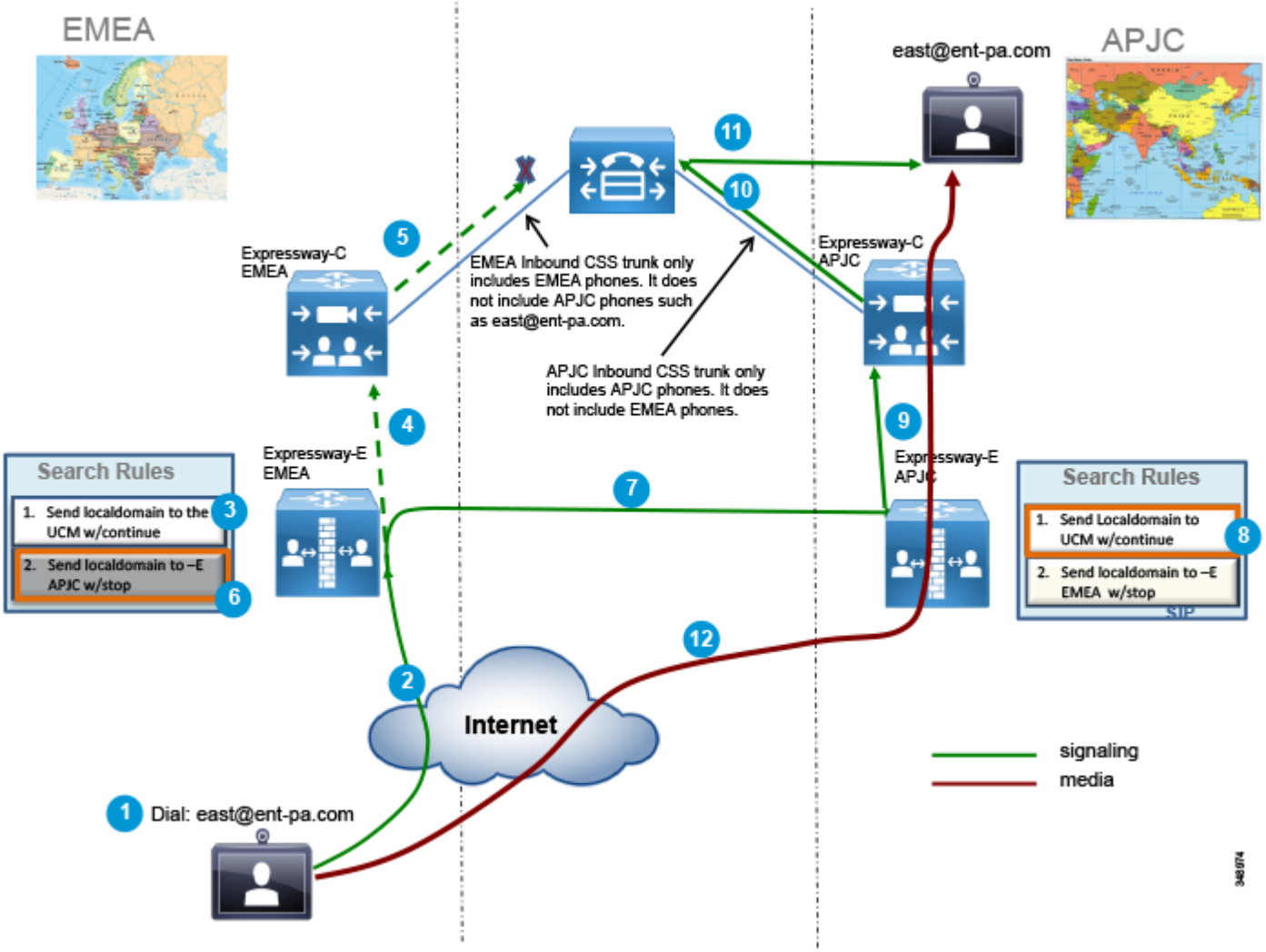
たとえば、EMEA 内の 2 つの Expressway-C クラスタと Expressway-E クラスタと、APJC 内の別の 2 つの Expressway-C クラスタと Expressway-E クラスタについて考えます。EMEA 内の Expressway-C トランク上の Unified CM インバウンド コーリング サーチ スペースには、EMEA 電話機のパーティションは含まれますが、APJC 電話機のパーティションは含まれません。同様に、APJC 内の Expressway-C トランク上のインバウンド コーリング サーチ スペースには、APJC 電話機のパーティションは含まれますが、EMEA 電話機のパーティションは含まれません。EMEA 内のインターネット上のユーザが APJC にある企業エンドポイントにコールした場合は、そのコールが Geo DNS から EMEA Expressway-E クラスタに送信されます。EMEA Expressway-E と Expressway-C はそのコールを宛先に送信しようとしますが、Expressway-C トランクのインバウンド コーリング サーチ スペースがそのコールをブロックします。その後で、EMEA Expressway-E がそのコールを APJC Expressway-E に転送します。こうして、コールが宛先に配信されます。これは、APJC Expressway-C のインバウンド コーリング サーチ スペースに APJC エンドポイント パーティションが含まれているためです。

EMEA 内の Expressway-E がシグナリングとメディアのパスからそれ自体を削除できるようにするには、Expressway-E EMEA クラスタ上に TCP/TLS 変換または RTP/SRTP 変換が確実に存在しないようにし、すべての Expressway-C と Expressway-E でコール シグナリング最適化パラメータが確実に [オン（on）] に設定することが重要です。

これは確定的プロセスではないため、Expressway エッジが 3 つ以上の場合は、検索メカニズムに時間がかかりすぎることがあります。したがって、この設定は Expressway エッジが 2 つ以下の場合にお勧めします。

図 4-22 に、宛先エンドポイントに最も近いエッジの選択を可能にする Expressway エッジ設計を示します。

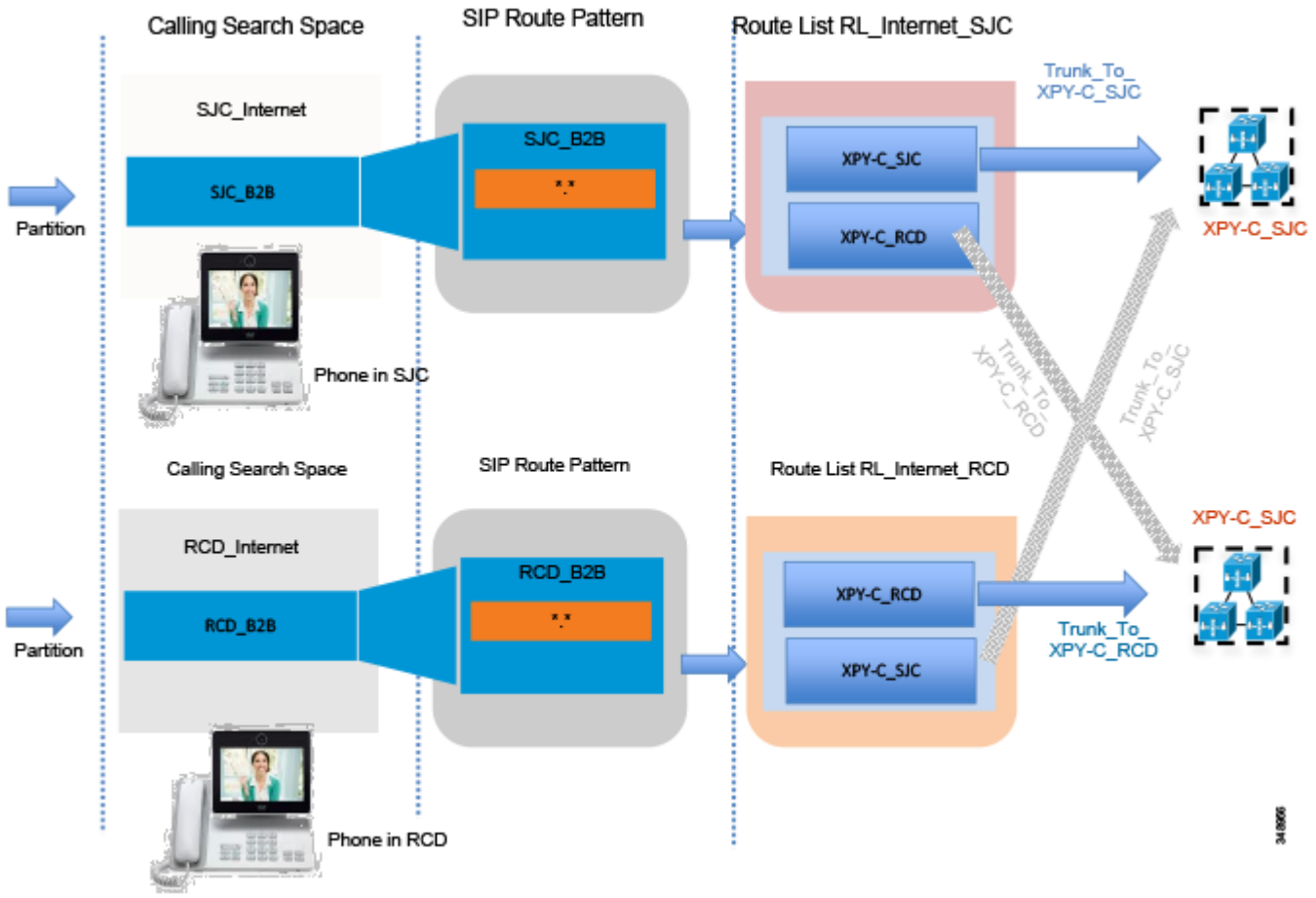
図 4-22　　宛先に最も近い Expressway クラスタの選択



発信コールに関する留意点

発信コールは発信側のエンドポイントに最も近い Expressway-C に転送する必要があります。これは、コーリング サーチ スペースやパーティションなどの Cisco Unified CM メカニズムを使用して実現できます。図 4-23 に、Unified CM の設定を示します。

図 4-23　Unified CM で設定するパーティションとコーリング サーチ スペース



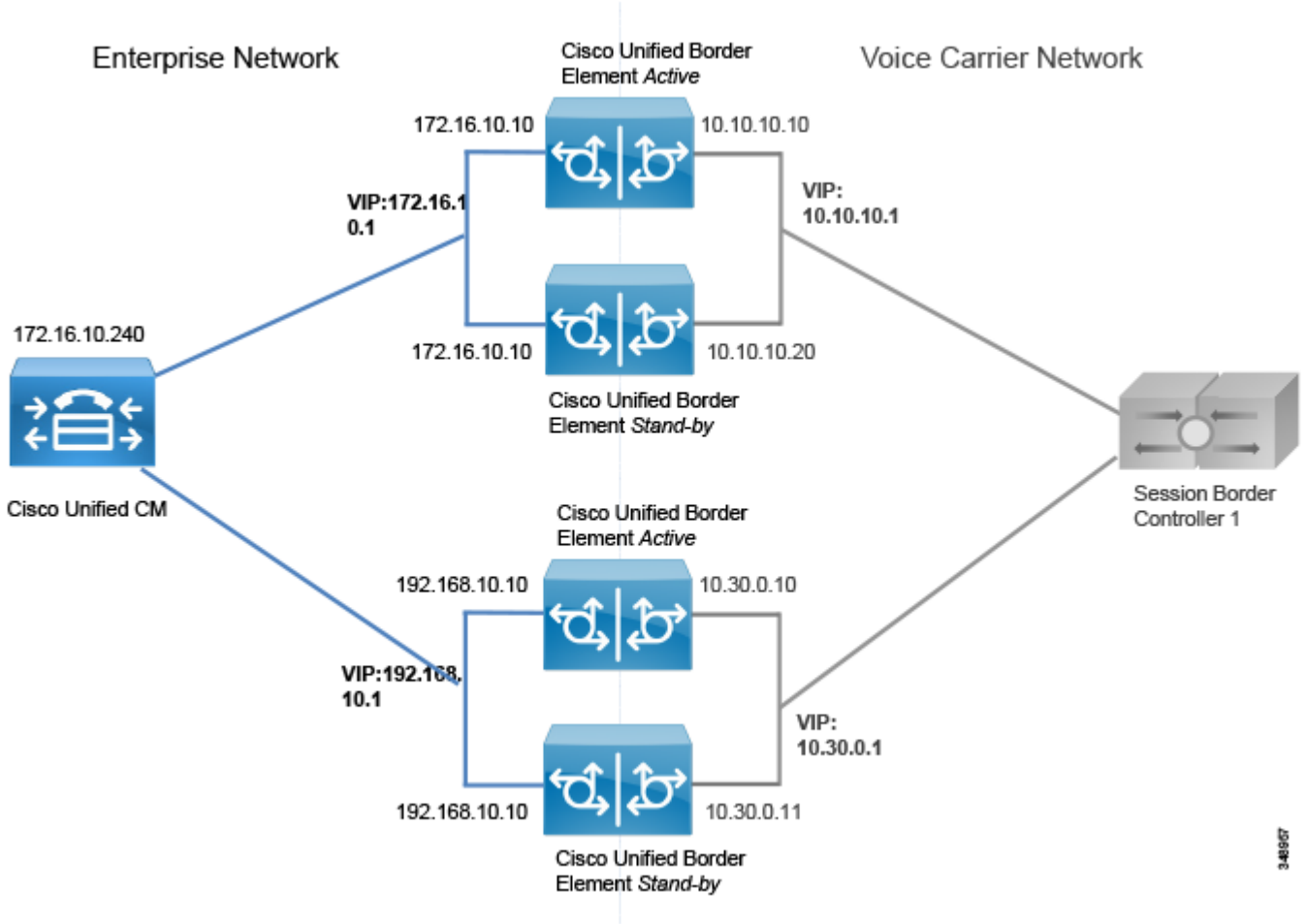
Unified CM ローカル ルート グループ機能は、複数のサイトが複数の Expressway-C クラスタにアクセスする場合にこのソリューションのスケーリングに役立ちます。このメカニズムは、ISDN ゲートウェイや Cisco Unified Border Element 上でも適用されます。詳細については、次のセクションで説明します。設定の詳細は、Cisco Unified Border Element や音声ゲートウェイにも当てはまるため、次の 2 つのセクションで説明します。

Cisco Unified Border Element のスケーリング

プラットフォームあたりのセッション容量については、サイジングの章を参照してください。

複数のデータセンターを展開している場合は、それぞれのデータセンターに Cisco Unified Border Element を展開することができます。この構成はさまざまな用途に使用されます。たとえば、図 4-24 に示すようなディザスタ リカバリ アーキテクチャが必要な場合があります。

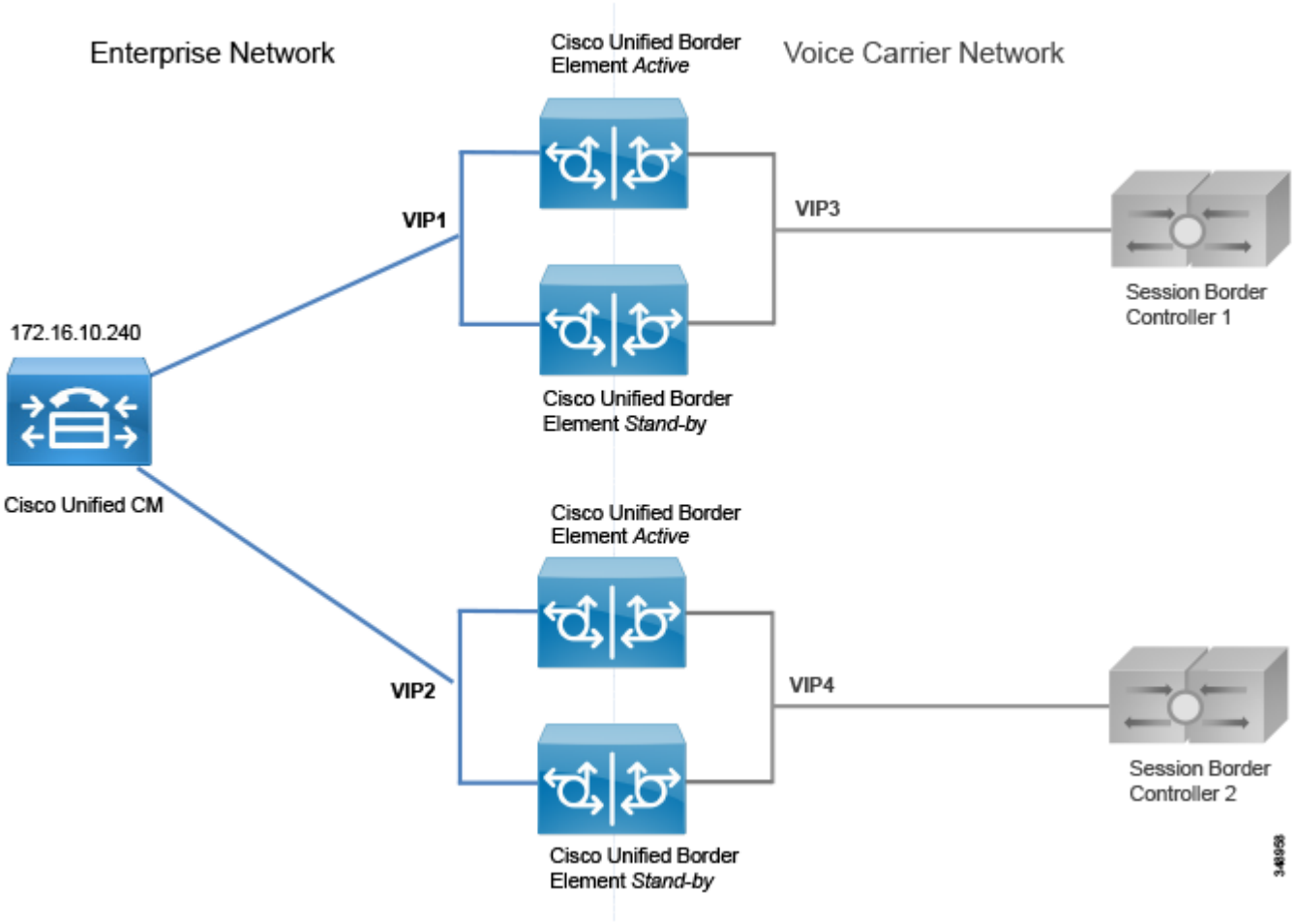
図 4-24　　複数の Cisco Unified Border Element



Unified Border Element へのすべてのトランク（通常は 2 つか 3 つ）を同じルート グループ内に含めることができます。これにより、データセンター間にロード バランシングが実現します。データセンター内のアクティブ ルータが故障した場合は、アクティブ コールが保存されます。あるデータセンターが到達不能になった場合、コール要求は残りのデータセンターに送信されます。この場合は、アクティブ コールが破棄されるため、ユーザは手動で回復する必要があります。

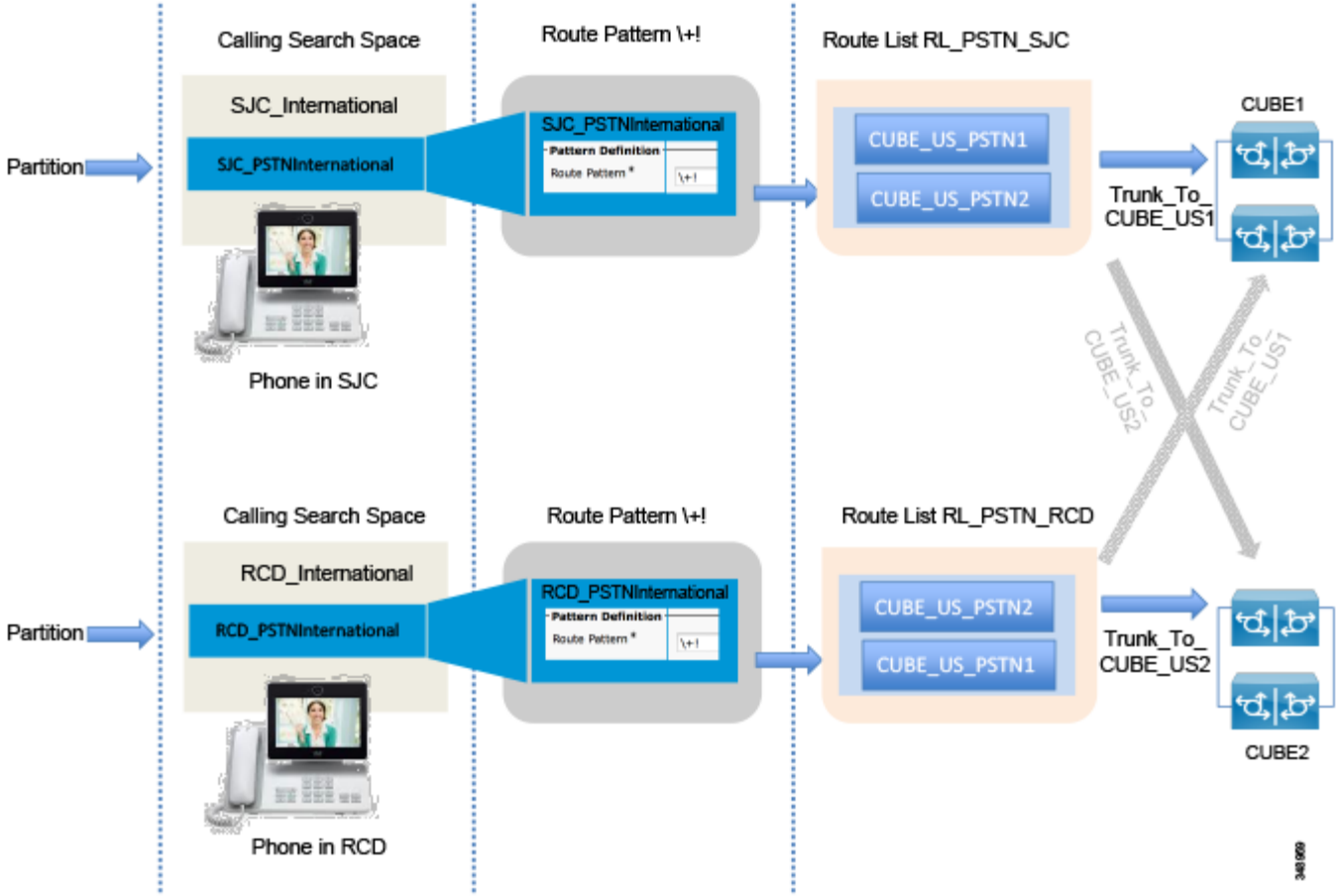
図 4-25 に示すように、企業音声ネットワークが広範囲に広がっている場合は、通信事業者からの複数のセッション ボーダー コントローラ（SBC）が使用されます。通信事業者の推奨事項に基づいて、SBC ごとに Cisco Unified Border Element が展開される場合があります。

図 4-25　別々の SBC に接続された複数の Cisco Unified Border Element



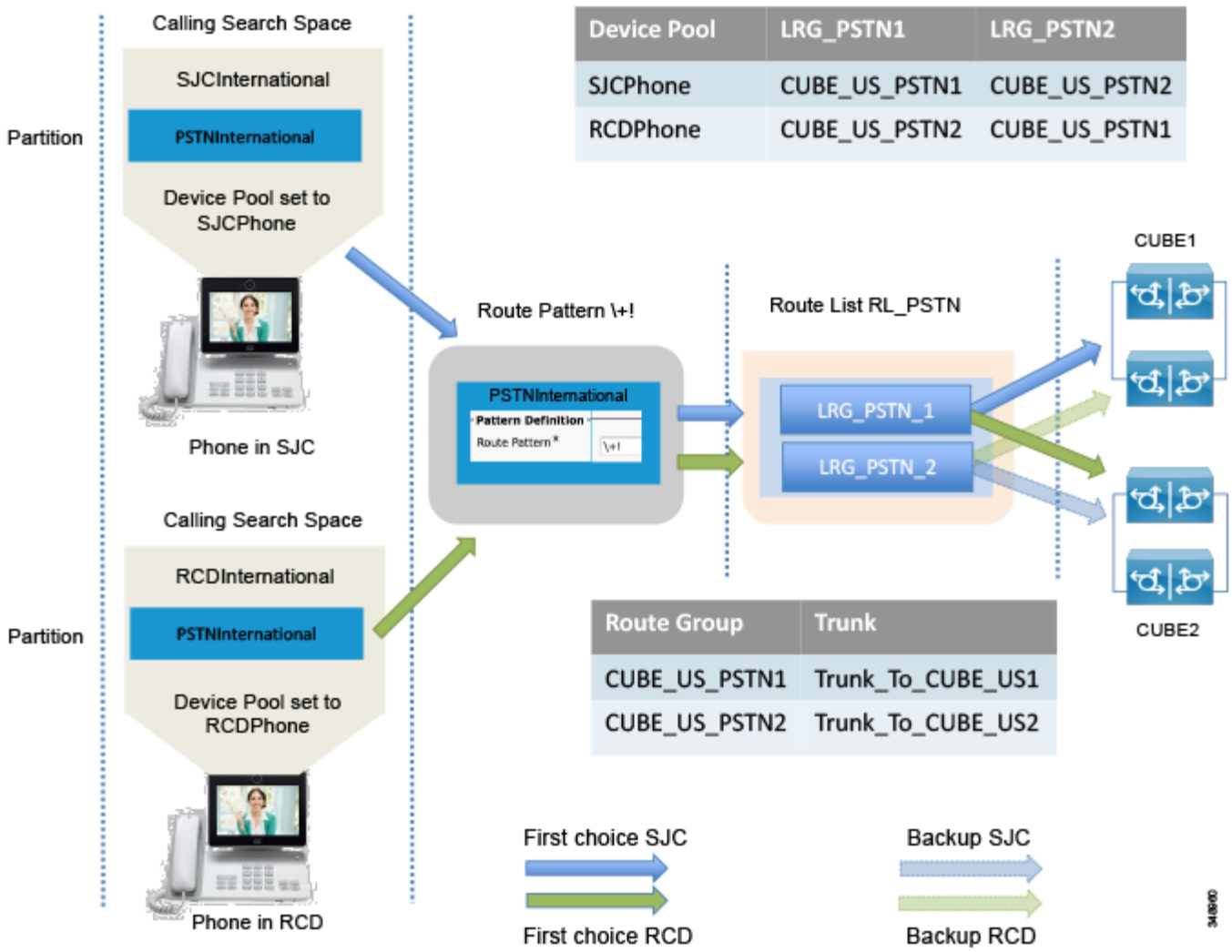
たとえば、US ですでに展開済みのものに加えて、別の Unified Border Element が必要になったとします。Trunk_to_CUBE_US2 という名前の新しいトランクを追加します。図 4-26 に、コーリング サーチ スペースとルート パターン間の標準の一対一マッピングに基づく設定を示します。この設定は、Unified Border Elements の数が増えるにつれて、Unified CM リソースに対する影響が大きくなるため、いくつかの制限があります。この設定を図 4-26 に示します。図 4-27 に示すローカル ルート グループ アプローチと比較してみてください。

図 4-26　Cisco Unified Border Element 接続用の Unified CM の設定



同じルート パターン \+! がすべての物理宛先分繰り返され、別々のパーティションに配置されます。オリジナルのパーティション PSTNInternational を SJC_PSTNInternational と RCD_PSTNInternational の 2 つに分割する必要があり、ルート パターン \+! を削除して、新しく作成した 2 つのパーティションに移動する必要があります。このアプローチは、サイト数があまり多くない（3 つ以下の）場合に機能します。さらに優れたアプローチは、図 4-27 に示すローカル ルート グループの概念を使用したアプローチです。

図 4-27　ローカル ルート グループ アプローチを使用した Cisco Unified Border Element 接続用の Unified CM の設定



この場合、デバイス プール SCJPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN1 と同じに設定されるのに対して、デバイス プール RCDPhone の LRG_PSTN1 はルート グループ CUBE_US_PSTN2 と同一に設定されます。LRG_PSTN2 は、SJC 電話機では CUBE_US_PSTN2 と同じに設定され、RCD 電話機では CUBE_US_PSTN1 と同一に設定されます。このアプローチをお勧めする理由は、新しいパーティションやルート パターンが必要ないうえ、図 4-26 に示すアプローチよりはるかにスケーラブルなことです。

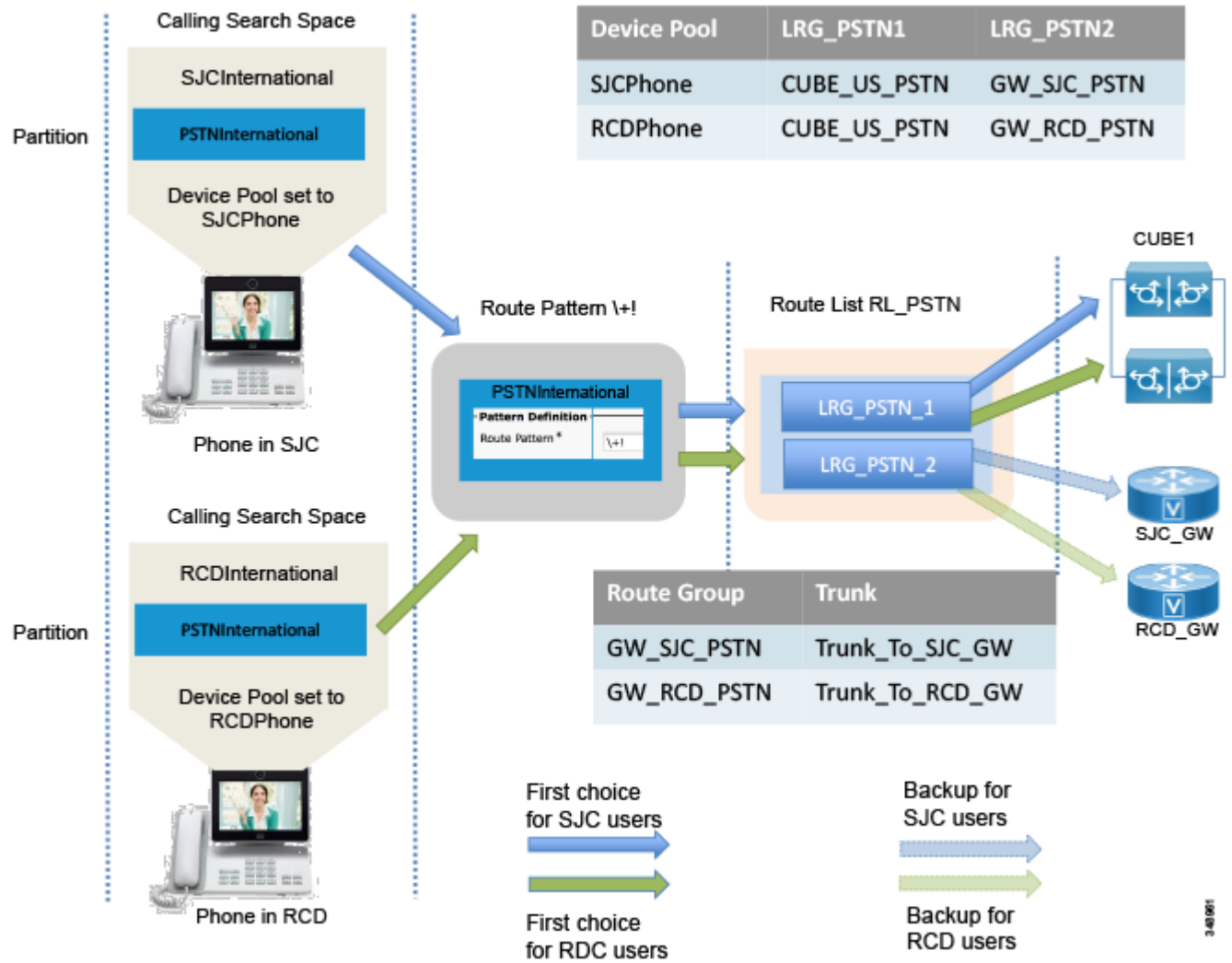
PSTN ソリューションのスケーリング

ローカル PSTN アクセスを提供する分散ゲートウェイは、支店に展開され、バックアップ サービスとして使用されます。

支店の数が多い場合は、Unified CM 内のルート グループとルート リスト設定の構造がうまくスケーリングしません。この展開では、PSTN へのルート パターンをサイトごとにレプリケートする必要のないローカル ルート グループ機能の使用をお勧めします。

以前のセクションで説明した設定は、このシナリオをカバーするように簡単に適合します。必要なことは、図 4-28 に示すように、デバイス プロファイル LRG_PSTN1 をルート グループ CUBE_US_PSTN に割り当て、LRG_PSTN2 をそのデバイス プール用のローカル ゲートウェイに対応するルート グループに割り当てることです。

図 4-28　　ローカル ISDN ゲートウェイを使用した集中型 PSTN アクセスに関する設定



ビデオ ISDN ソリューションのスケーリング

ビデオ ISDN ソリューションのスケーリングは PSTN ソリューションのスケーリングと非常によく似ています。数台を超えるビデオ ISDN ゲートウェイが必要な場合は、Unified CM のローカル ルート グループの使用が PSTN のコール ルーティングに推奨されている方法です。ISDN ゲートウェイを地理的に分散させることによって、着信コールと発信コールの両方の通話料金が削減されます。

コラボレーション エッジの展開プロセス

ここでは、コラボレーション エッジの展開プロセスの概要について説明します。すべての展開ですべてのアクセス手段が必要なわけではないため、コラボレーション エッジの各コンポーネントは個別に取り扱われます。たとえば、ある会社は PSTN しか所有していないが、別の会社は PSTN を特定のローカル サイトで IP PSTN 用のローカル バックアップとして使用し、インターネット エッジ展開を所有し、Business-to-Business（B2B）インターネット コールに対して有効になっていないユーザを ISDN ビデオ ゲートウェイを使用してコールする場合が考えられます。

コラボレーション エッジ コンポーネントは次の順序で展開する必要があります。

- Expressway-C と Expressway-E を展開する
- Cisco Unified Border Element を展開する
- Cisco Voice Gateway を展開する
- Cisco ISDN Video Gateway を展開する

Expressway-C と Expressway-E を展開する

ここでは、Expressway-C と Expressway-E のインストールと展開に必要な作業の概要について説明します。作業は次の順序で実行する必要があります。

1. Expressway-C と Expressway-E の OVA テンプレートをダウンロードして展開し、Expressway ソフトウェアをインストールします。アプライアンス モデル（Cisco Expressway CE500 または CE1000）が使用されている場合、OVA テンプレートと Expressway ソフトウェアをダウンロードしてインストールする必要はありません。
2. DNS と NTP を含むネットワークのインターフェイスと設定、およびシステムのホスト名とドメイン名を構成します。Expressway-E は 2 つの LAN インターフェイスを備えています。外部インターフェイスの IP アドレスを静的に変換しなければならない場合は、変換後のインターフェイスの IP アドレスを設定する必要があります。Expressway-E はペイロード参照内のパブリック IP アドレスを使用します。
3. クラスタリングを設定します。

モバイルおよびリモート アクセスを展開する

1. Unified Communications モードを [モバイルおよびリモート アクセス（Mobile and remote access）] に設定することによって、モバイルおよびリモート アクセスを有効にします。
2. モバイルおよびリモート アクセスが有効にするドメインを選択します。[Unified CM上のSIP登録およびプロビジョニング（SIP registration and provisioning on Unified CM）]、[Unified CM上のIM and Presenceサービス（IM and Presence service on Unified CM）]、および [会社間フェデレーションの場合のXMPPフェデレーション（XMPP federation if inter-company federation）] をオンにします。
3. CA 証明書を Expressway-C と Expressway-E にアップロードします。[TLS検証モード（TLS verify mode）] が [オン（on）]（推奨）になっている場合は、Unified CM クラスタと IM and Presence クラスタを検出するためにこの証明書が必要です。このように、Expressway-C は、証明書をチェックすることによって、クラスタ サーバのアイデンティティを検証します。
4. 各クラスタのパブリッシャを設定することによって、Unified CM サーバと IM and Presence サーバを検出します。
5. Expressway-C と Expressway-E の両方に証明書をインストールします。どちらのタイプの Expressway ノードも、その後 CA によって署名される、証明書署名要求（CSR）を生成できます。内部 CA を使用している場合は、CSR をその CA で署名する必要があります。Expressway-C と Expressway-E が Business-to-Business（B2B）コミュニケーションに使用されている場合は、前述したように、パブリック CA が Expressway-E の証明書に署名する必要があります。その後で、署名した証明書を Expressway-C と Expressway-E にアップロードする必要があります。
6. Expressway-C と Expressway-E の間の Unified Communication トラバーサル ゾーンを設定して、Cisco Unified CM へのプロキシ登録を許可します。
7. すべてが正しくセットアップされていることを確認するために、Unified Communications のステータスをチェックします。

（注）
- この設定によって、モバイルおよびリモート アクセスが有効になります。Business-to-Business（B2B）では追加の設定が必要です。
- 上記設定は、Expressway-C と Expressway-E 上だけで完結します。
- これらのステップは、Unified CM への TCP/RTP 接続（TLS/SRTP は表示されていない）の場合に必要です

Business-to-Business（B2B）コミュニケーションを展開する

ここでは、Business-to-Business（B2B）コミュニケーションのセットアップに必要な追加のステップの概要について説明します。

1. Expressway-C と Expressway-E の両方で NTP、DNS、およびシステム名を含む基本的なレイヤ 3 設定を構成します。
2. Expressway-E 上でトラフィック ルーティングに必要な IP ルートを含む NAT 設定をセットアップします。
3. Expressway-E を DMZ に配置する前に、外部ファイアウォールが Expressway-E 宛てのすべてのトラフィックをブロックするように設定されていることを確認します。
4. Expressway-C と Expressway-E の両方のローカルまたはリモート認証を含む管理アクセス ポリシーを設定します。

5. 該当する DNS サーバ内の DNS A レコードを各サーバの FQDN が解決できるように設定します。
6. Expressway-C からのトラバーサル クライアント接続を認証する目的で Expressway-E 内のローカル認証クレデンシャルをセットアップします。
7. Expressway-E 上で SIP 専用のトラバーサル サーバ ゾーンをセットアップします。
8. Expressway-E 上のインターワーキングを [オン（On）] に設定します。これにより、Expressway-E で H.323 コールを送受信して、それらをネットワークのエッジで SIP に接続できるようになるため、企業内部で単一のプロトコルが維持されます。
9. Expressway-C 上で SIP 専用のトラバーサル クライアント ゾーンをセットアップします。
10. Expressway-E の FQDN を使用してトラバーサル リンクを有効にして PKI の使用を可能にします。
11. 外部 DNS ゾーンを Business-to-Business（B2B）コミュニケーションのアウトバウンド ドメイン解決用に設定します。
12. Expressway-E 上でビデオ、音声、IP PSTN ゲートウェイなどの保護されたリソースへのアクセスを制限する基本的な CPL ルールを導入します。
13. Expressway-C と Expressway-E が権限を与えられたドメインをセットアップします。
14. Expressway-C と Expressway-E 上で事前検索変換、検索ルール、DNS 検索ルール、および外部 IP アドレス ルーティングを使用してダイヤル プランをセットアップします。
15. Expressway-C 上で Unified CM までの SIP ネイバー ゾーンを設定します。
16. Unified CM 上の SIP トランクが Expressway-C と通信するように設定します。

Cisco Unified Border Element を展開する

ここでは、ボックスツーボックス冗長性を備えた Cisco Unified Border Element を展開するためのプロセスの概要について説明します。ボックスツーボックス冗長性は両方の Unified Border Element ルータ上で設定する必要があり、設定内容は両方とも同じです。アクティブ Unified Border Element から スタンバイ Unified Border Element に設定をコピーして貼り付けることができます。

1. ネットワーク設定（アクティブ Unified Border Element とスタンバイ Unified Border Element の両方の 2 つのイーサネット インターフェイス（LAN 向けと WAN 向け）と IP ルーティング）を構成します。
2. 両方のルータ上の Unified Border Element を SIP 間コール、FAX のリレーまたはパススルー、プライバシー ヘッダーとしての発信元 ID 処理、および早期オファーの強制に対して有効にします。Unified CM がベスト エフォート早期オファー専用に設定されているため、Unified Border Element 上でこの機能を有効にすることをお勧めします。新しい展開では早期オファーのみがエンドポイントから送信されますが、代わりに遅延オファーが送信される旧式のシスコ デバイスが関与している場合もあります。このマニュアルではこのようなケースを取り上げませんが、Cisco Unified Border Element 上で早期オファーを強制することをお勧めします。
3. ボックスツーボックス冗長性を有効にして、アクティブ ルータとスタンバイ ルータの LAN インターフェイスと WAN インターフェイスの両方で HSRP をグローバルに設定します。
4. 音声コーデック優先順位を設定します（音声コーデックがネゴシエート可能であり、Unified CM または通信事業者ソフト スイッチによって強制されない場合）。
5. 保留音を設定します。

6. ダイヤルピアを設定します。ダイヤルピアはコール レッグに関連付けられており、インバウンドまたはアウトバウンドで照合できます。たとえば、Unified CM からの着信コールはインバウンド ダイヤルピア（着信コール レッグに対応する）によって照合されます。もう 1 つのコール レッグは、通信事業者のセッション ボーダー コントローラ（SBC）向けの Cisco Unified Border Element（CUBE）によって生成され、別のダイヤルピアに照らして照合されます。同じダイヤルピアで着信コールまたは発信コールを照合できますが、それぞれのダイヤルピアで別々のコール レッグを照合することをお勧めします。この提案に従うと、次の 4 種類のダイヤルピアが用意されます。Unified CM から CUBE へのインバウンド ダイヤルピア、CUBE から SBC へのアウトバウンド ダイヤルピア、SBC から CUBE へのインバウンド ダイヤルピア、および CUBE から Unified CM へのアウトバウンド ダイヤルピア。ダイヤルピアは、発信側または着信側の番号またはパターンに照らして照合できます。また、ダイヤルピアは、単一のコーデックを強制することも、ステップ 4 で設定したコーデックのリストをネゴシエートすることもできます。**incoming called-number** コマンドはダイヤルピア インバウンドのみを作成します。

   インバウンド ダイヤルピアにはターゲットが関連付けられませんが、アウトバウンド ダイヤルピアには Unified CM または通信事業者の SBC がターゲットとして定義されます。

   外部宛先へのコールは汎用パターンと一致するため、Unified Border Element 上のダイヤルピア設定がエラーの原因になる場合があります。たとえば、図 4-29 では、発信コールがダイヤルピア 201 と 101 の両方と一致するため、ルーティングが正しく機能しません。

図 4-29　Cisco Unified Border Element 上でのインバウンド ダイヤルピアとアウトバウンド ダイヤルピアの設定

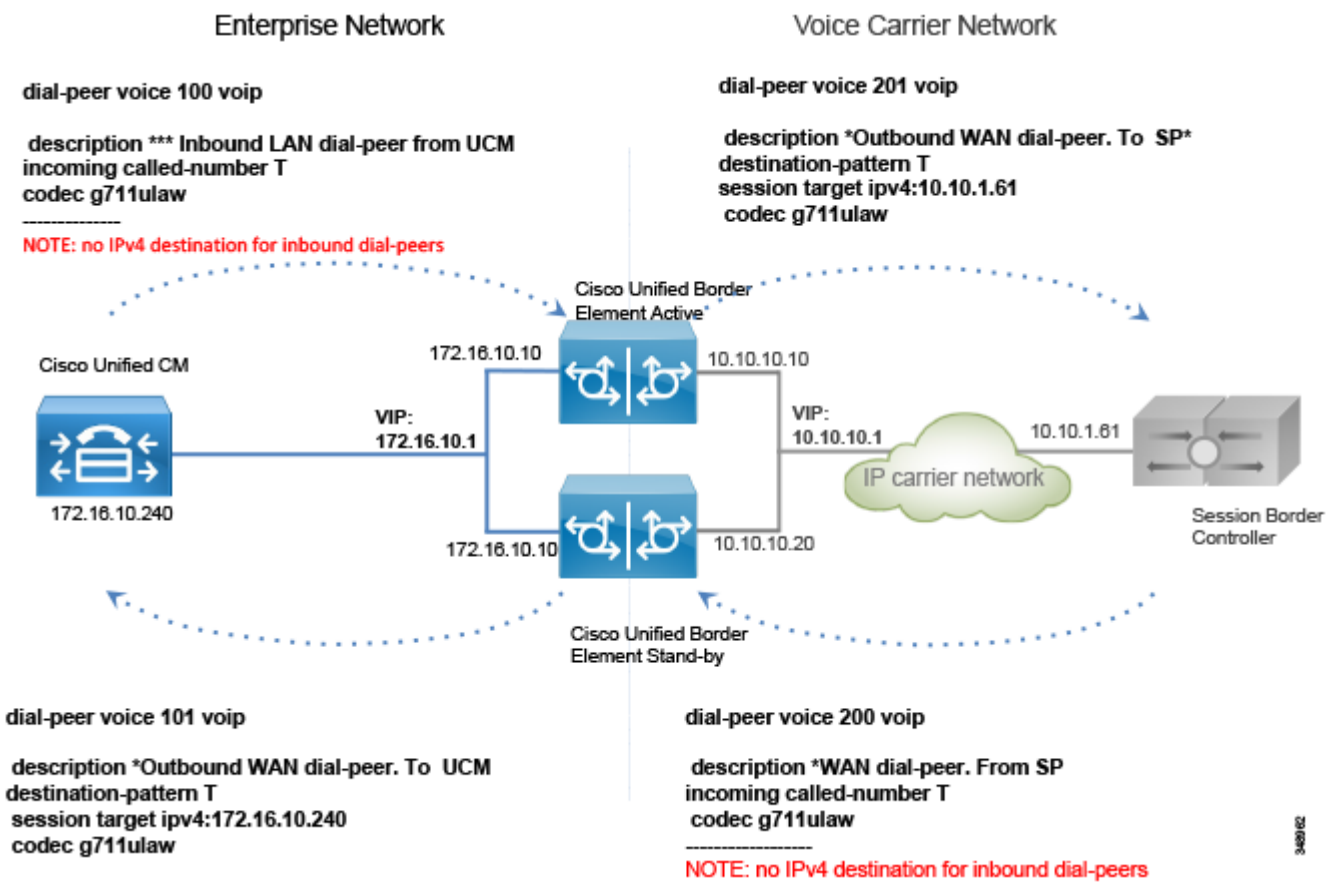


図 4-30 の変数 T は任意の長さの任意の数値文字列を表します。これは、Unified CM からのコールが世界中の任意の宛先に送信される可能性があるためです。最も近い一致が役に立つ場合もありますが、Unified Border Element が一元管理されており、複数の場所にサービスを提供している場合は、「宛先パターン」設定内で可能性のあるすべての宛先を列挙するのは実用的ではありません。この制限を克服し、ルーティング プロセスを簡略化して応答性を高めるために、次の追加の設定を実行します。

a. アウトバウンド ダイヤルピア内のサーバ グループ：サーバ グループがダイヤルピア内の宛先として設定され、ラウンドロビン アルゴリズムが選択されている場合は、Unified Border Element は複数のサーバで負荷を共有します。

```
voice class server-group 1
    ipv4 172.16.10.240
    ipv4 172.16.10.241
    ipv4 172.16.10.242
    ipv4 172.16.10.243
    ipv4 172.16.10.244
    hunt-scheme round-robin
```

b. SIP Out-of-Dialog OPTIONS Ping：サーバが稼働中の ping 間隔やサーバがダウン中の間隔（この例ではそれぞれ 30 秒と 60 秒に設定）などのさまざまなパラメータを設定できます。

```
voice class sip-options-keepalive 171
    transport tcp
    sip-profile 100
    down-interval 30
    up-interval 60
    retry 5
    description Target Unified CM
```

この方法では、Unified CM へのアウトバウンド ダイヤルピアが次のようになります。

```
dial-peer voice 101 voip
    description *Outbound WAN dial-peer.ToUnified CM
    destination-pattern T
    session protocol sipv2
    session server-group 1
    voice-class sip options-keepalive profile 171
    codec g711ulaw
```

c. 通信事業者への発信コール レッグがアウトバウンド ダイヤルピアによって照合されます。

```
dial-peer voice 201 voip
description *Outbound WAN dial-peer.To  SP*
destination-pattern T
session target ipv4:10.10.1.61
 codec g711ulaw
```

d. 先行する「*」は、発信コール（Unified Border Element から見れば着信コール）で Unified CM から送信されます。これにより、ルータはコールの方向を識別できます。この記号はコールが IP PSTN に到達する前に除去する必要があります。また、設定されたダイヤル プランに基づいて、発信者番号を「+」を使って正規化する必要があります。ルール 2 は「+」を前に付加し、発信者番号に適用されますが、ルール 1 は先行する「*」を「+」に置き換えます。これらのルールは着信者番号にも適用されます。そのため、着信者番号用と発信者番号用の 2 つのルールを作成できます。ただし、着信者番号は常に最初のルールと照合され、発信者番号は常に 2 つ目のルールと照合されるため、単一の音声トランスレーション ルールを使用できます。これは、インバウンド ダイヤルピア上で設定されます。

発信コール レッグ（ダイヤルピア）は **dpg** コマンド経由でインバウンド ダイヤルピアにバインドされるため、「*」が先行するコールが受信された場合は、SBC に対向しているダイヤルピアに送信され、Cisco Unified CM 向けのダイヤルピアには送信されません。

```
voice class dpg 201
    dial-peer 201

voice translation-rule 2
    rule 1 /^\*/ /+/
    rule 2 // /+/
voice translation-profile SIPtoE164
    translate called 2
    translate calling 2
dial-peer voice 100 voip
    translation-profile outgoing SIPtoE164
    incoming called-number *T
destination dpg 201
    codec g711
```

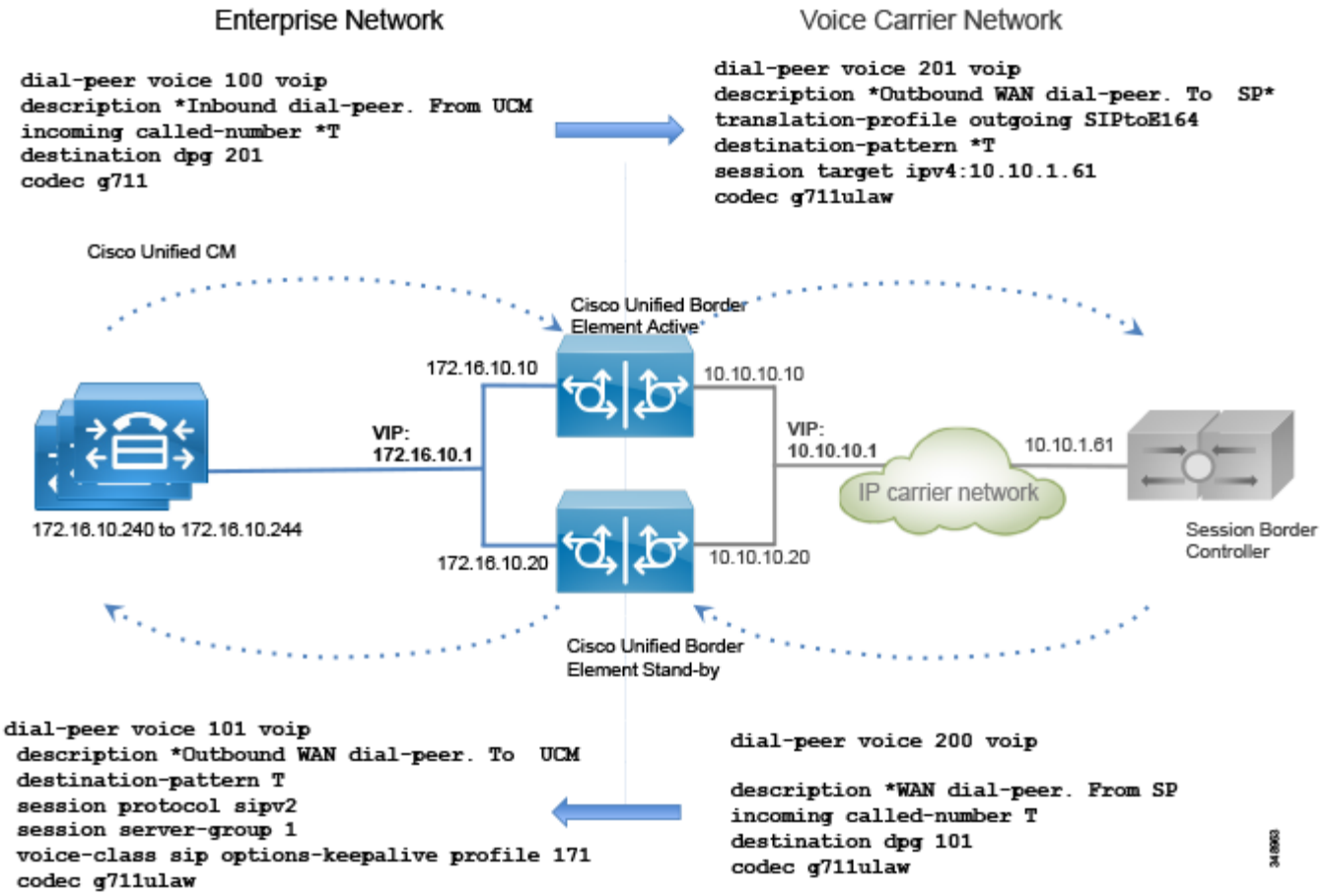
ダイヤルピア 200 はダイヤルピア 101 にもバインドする必要があります。

```
voice class dpg 101
    dial-peer 101

dial-peer voice 200 voip
    description *WAN dial-peer.From SP
    incoming called-number T
    destination dpg 101
    codec g711ulaw
```

図 4-30 に、この設定を示します。

図 4-30　Cisco Unified Border Element のダイヤルピア設定



コール レッグが Unified CM から到着した場合は、「*」が先行する Unified Border Element にヒットするため、ダイヤルピア 100 と一致します。その後で、このコールは、インバウンド ダイヤルピア宛先としてアウトバウンド ダイヤルピア グループを使用してダイヤルピア 200 に送信されます。ダイヤルピア 200 は先行する「*」を除外し、そのコールを PSTN に送信します。この機能を使用しない場合は、ダイヤルピア 201 も一致するため、ルーティング エラーが発生することに注意してください。

コール レッグが SBC から到着した場合は、ダイヤルピア 201、101、および 200 と一致する可能性があります。ただし、「着信者番号」の方が「宛先パターン」より優先されるため、ダイヤルピア 200 が一致します。また、ダイヤルピア 200 がダイヤルピア 101 にリンクされているため、コールは正しく宛先にルーティングされます。

7. 必要に応じて、トランスコーディングを設定します。トランスコーディングには専用のハードウェア リソース（DSP）が必要なことを覚えておいてください。

Unified CM 上で次の設定作業を実行します。

1. コール制御の章で指定されているように、各 Unified Border Element にベスト エフォート早期オファー トランクを設定します。
2. ルート グループ CUBE_US_PSTN を設定し、メンバーとして Unified Border Element トランクを追加します。

3. ローカル ルート グループ LRG_PSTN1 を設定します。
4. デフォルト ローカル ルート グループとルート グループ LRG_PSTN1 を含むルート リストを設定します。
5. デバイス プールごとに、LRG_PSTN1 を CUBE_US_PSTN に設定します。

Cisco Voice Gateway を展開する

PSTN インターフェイスは Cisco ISR G2/G3 ルータや ASR ルータなどのさまざまなルータで使用できます。PSTN インターフェイスには、アナログ、BRI、および PRI ISDN 音声カードが含まれます。アナログ インターフェイスは、ほとんど、FAX マシンとアナログ電話機に接続するために使用されます。

ISDN 音声インターフェイスを備えた PSTN ゲートウェイを設定するには、次の作業を実行します。

1. ルータ上でネットワーク設定とルーティングを構成します。
2. ISDN インターフェイスをアクティブ化します。
3. 通信事業者の要件に基づいて、ユーザ側の ISDN パラメータ、スイッチタイプ、フレーミング、および回線コードを設定します。
4. ダイヤルピアを設定します。

ダイヤルピア ロジックは IP PSTN や Unified Border Element 用のものと同じですが、この場合は、「voip」ダイヤルピアに加えて、音声ゲートウェイには PSTN 向けの「pots」ダイヤルピアもあります。

FAX マシンなどのアナログ装置が存在する場合は、アナログ インターフェイスを介してルータに接続できます。

ルータがアナログ FAX 相互接続専用に使用されていて、PSTN インターフェイスが別のルータに接続されている場合は、T.38 FAX リレーを設定できます。これは、特に PSTN ゲートウェイへのパスが WAN をトラバースする場合に、このリレーがより高い復元力を示すためです。

ダイヤルピア設定は IP PSTN や Unified Border Element の設定と異なります。ゲートウェイは特定の場所に展開され、その場所の電話機を制御するため、パターン宛先は +14085554XXX のようによく見る形式になります。

一方、着信 PSTN コールのアドレスはプラン、タイプ、および番号で構成されます。プランとタイプは SIP でサポートされておらず、通信事業者に基づくため、コールは別のプランとタイプを使用してゲートウェイに到達する可能性があります。たとえば、ドイツの同じエリア コード 6100 内のトランク上の E.164 宛先 4961007739764 へのコールの場合は、出力 ISDN SETUP メッセージ内の着信者番号（プラン/タイプ/番号）が ISDN/national/61007739764、ISDN/subscriber/7739764、または unknown/unknown/061007739764 として送信されます。

プラン/タイプに基づいて番号が変化するため、ダイヤルピアが一致しない場合があります。そのため、プラン/タイプを unknown/unknown に強制する必要があります。この方法では、完全な E164 番号が宛先に開示されます。ダイヤルピア構造は、コール制御の章で詳しく説明されており、ここでは一貫性を保つために参照されています。

アウトバウンド ダイヤルピアの場合は、次のルールによって、発信者番号がプラン「unknown」とタイプ「unknown」に変換され、着信者番号が先行する「*」を使って +E.164 番号に変換されます。

```
voice translation-rule 1
       rule 1 /^\*/ // type any unknown plan any unknown
       rule 2 // // type any unknown plan any unknown
voice translation-profile ISDNunknown
       translate called 1
translate calling 1
dial-peer voice 1 pots
       translation-profile outgoing ISDNunknown
```

インバウンド ダイヤルピアの場合は、発信者情報にタイプが「national」の 10 桁の数字が含まれていれば（および米国を示す国番号「1」が含まれていなければ）、コールは「+1」が先行する +E.164 番号に正しく変換されます。「unknown」の場合は、以降のルールが一致しません。

着信者番号が海外の宛先から送られてきたため国番号が含まれており、E.164 形式だった場合は、ルール 2 によって先行する「+」が付加されます。

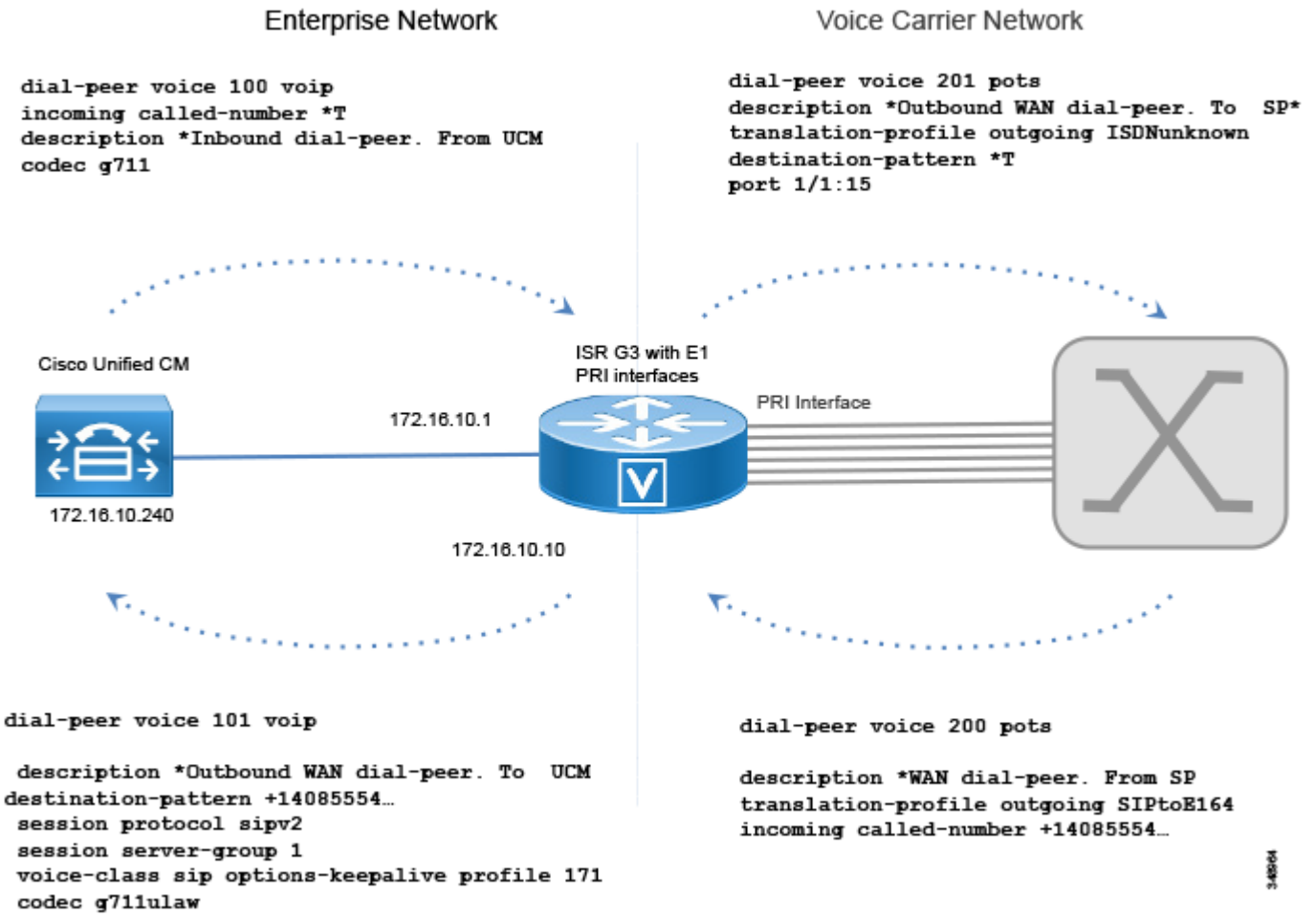
ただし、ISDN セットアップはホップバイホップのため、タイプが「national」のコールはそれほど多くないことが予想されます。これは、最近のスイッチが強制的にタイプを「national」にしているためです。いずれの場合も、次のルールによって、発信者番号と着信者番号が正しく正規化されます。

```
voice translation-rule 3
    rule 1 /^\(.+\)$/ /+1\1/ type national unknown plan any unknown
    rule 2 /^\(.+\)$/ /+\1/ type international unknown plan any unknown
voice translation-profile ISDNtoE164
    translate called 3
    translate calling 3

dial-peer voice 1 pots
    translation-profile incoming ISDNtoE164
```

図 4-31 に、G.711 のダイヤルピア設定と E1 PRI インターフェイスを示します。

図 4-31　音声ゲートウェイのダイヤルピア設定



Unified CM 上で次の設定作業を実行します。

1. 各ゲートウェイのベスト エフォート早期オファー トランク（Trunk_to_SiteID_GW、SiteID は場所を識別する変数）を設定します。
2. ルート グループ LRG_PSTN1 を設定して、メンバーとしてゲートウェイ トランクを含めます。
3. ローカル ルート グループ LRG_PSTN1 を設定します。
4. デフォルト ローカル ルート グループと LRG_PSTN1 を含むルート リストを設定します。
5. デバイス プールごとに、LRG_PSTN1 を Trunk_to_SiteID_GW に設定します。この設定では、推奨されているように、サイトごとにデバイス プール SiteIDPhone が存在することを想定しています。

ローカル ルート グループ設定を使用することによって、PSTN アクセスの認識が容易になります。たとえば、Unified Border Element を PSTN への集中型アクセスに使用し、ローカル PSTN 接続をバックアップとして使用することができます。この場合は、デバイス プールによって Unified Border Element ルート グループが LRG_PSTN1 に指定され、LRG_PSTN2 にローカル ゲートウェイへのトランク（Trunk_to_SiteID_GW）が含まれます。

Cisco ISDN Video Gateway を展開する

Cisco TelePresence ISDN GW 3241 または Cisco TelePresence ISDN MSE 8321 の展開は実に簡単なプロセスです。

1. Web インターフェイスにログインします。
2. ポート ライセンスを割り当てます。ポート ライセンスごとに PRI インターフェイスがアクティブになります。8321 ISDN ゲートウェイ用のポート ライセンスはスーパーバイザ MSE 8050 上で設定され、ISDN GW 3241 用のポート ライセンスはオンボックスで設定されます。
3. ISDN インターフェイスをセットアップします。この操作は、[設定（Settings）] > [ISDN] で実行します。これらの設定は、ISDN のタイプとフォームを配信するためにサービス プロバイダーから受信された通常の設定です。
4. ISDN ポートを設定します。この操作は、[設定（Settings）] > [ISDNポート（ISDN ports）] で実行します。ここで、ディレクトリ番号、チャネル範囲、およびチャネル検索順序のすべてが設定されます。また、使用する ISDN ポートを有効にするために各ポートの [有効（Enabled）] ボックスをオンにする必要があります。
5. コール制御を設定します。この操作は、[設定（Settings）] > [SIP] で実行します。これらは、Unified CM に使用されるホスト名と SIP ドメインを含む ISDN ゲートウェイ上の SIP 設定です。
6. ダイヤル プランを設定します。この操作は、ダイヤル プラン見出しの 2 つのタブ（[IPからISDNへ（IP to ISDN）] と [ISDNからIPへ（ISDN to IP）]）で実行します。[ISDNからIPへ（ISDN to IP）] ダイヤル プラン タブで、着信 ISDN 番号範囲が正しく IP 番号範囲に変換されていることを確認します。

ゲートウェイの設置と初期設定の詳細については、次の URL で Cisco TelePresence ISDN Gateway のインストレーション ガイドとアップグレード ガイドを参照してください。

http://www.cisco.com/c/en/us/support/conferencing/telepresence-isdn-gateway/products-installation-guides-list.html

コア アプリケーション

改訂日：2015 年 1 月 22 日

この章では、エンタープライズ コラボレーションのプリファード アーキテクチャに含まれるコア アプリケーションについて説明します。シスコとそのエコシステム パートナーからは多くのアプリケーションが提供されていますが、この章では、ほとんどのコラボレーション環境に必要なコア アプリケーションのサブセットを中心に説明します。プリファード アーキテクチャは、アプリケーションの導入を簡素化し、不必要な設定の変更を防ぐために、利用可能なすべてのアプリケーションを考慮して構築されています。

この章の主要な 2 つの項では、Cisco Unity Connection によるユニファイド メッセージングと Cisco TelePresence Management Suite（TMS）による会議スケジュールの実装方法を説明します。それぞれの項では、コア アーキテクチャと導入プロセスの詳細について説明します。

この章の第 3 項では、アプリケーション導入ツール（Cisco Prime Collaboration Deployment（PCD）およびCisco Prime License Manager（PLM））について説明します。また、この章の終わりに追加のアプリケーションのリストがあります。

この章の変更点

表 5-1に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 5-1　　本リリースで追加または変更された情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
Cisco TelePresence Conductor	「Cisco TelePresence Management Suite（TMS）による会議スケジュール」（P.5-37）	2015 年 1 月 22 日

前提条件

コア アプリケーションをプリファード アーキテクチャに導入する前に、以下の点を確認してください。

- Cisco Unified Communications Manager（Unified CM）が導入されており、機能している。
- Microsoft Active Directory がインストールされており、各アプリケーションの統合について理解している。
- このマニュアルのコール制御の章の内容を理解しており、この機能を実装している。
- このマニュアルの会議の章の内容を理解しており、スケジュールされている会議に必要なコンポーネントが導入されている。
- 会議ソリューションのサイジングとライセンスについて理解している。

コア アプリケーションのリスト

プリファード アーキテクチャのコア アプリケーションには次の要素が含まれています。

- Cisco Unity Connection：ユニファイド メッセージング機能を提供します（Cisco Unity Connection によるユニファイド メッセージングの項を参照）。
- Cisco TelePresence Management Suite：Collaboration Meeting Room（CMR）のプロビジョニングおよび会議スケジュール機能を提供します（Cisco TelePresence Management Suite（TMS）による会議スケジュールの項を参照）。

コラボレーション導入で使用するツールのリスト

エンタープライズ コラボレーション向けプリファード アーキテクチャの導入時に管理者にとって役立つソフトウェア ツールを次に示します。

- Cisco Prime License Manager（PLM）
- Cisco Prime Collaboration Deployment（PCD）

主な利点

- 複数のエンドユーザ プラットフォームでユニファイド メッセージングが使用可能になる
- 個々のエンドユーザ Collaboration Meeting Room（CRM）の作成とプロビジョニング
- 会議のスケジュールとワンボタン機能の導入
- 新規インフラストラクチャ コンポーネントの導入の簡素化
- 各種製品のライセンスを管理するための単一ツール

Cisco Unity Connection によるユニファイド メッセージング

Cisco Unity Connection により、エンタープライズ コラボレーション向けシスコ プリファード アーキテクチャのユニファイド メッセージングが有効になります。この項では、ボイス メッセージングとユニファイド メッセージングのための Unity Connection と、シングル インボックスおよびビジュアル ボイスメールなどの機能の導入に関する情報と手順を説明します。この項では、2 つの Unity Connection クラスタ間のネットワークについても説明します。

コア コンポーネント

コア アーキテクチャに含まれている要素を次に示します。

- Cisco Unified Communications Manager（Unified CM）
- Cisco Unity Connection
- Microsoft Exchange

主な利点

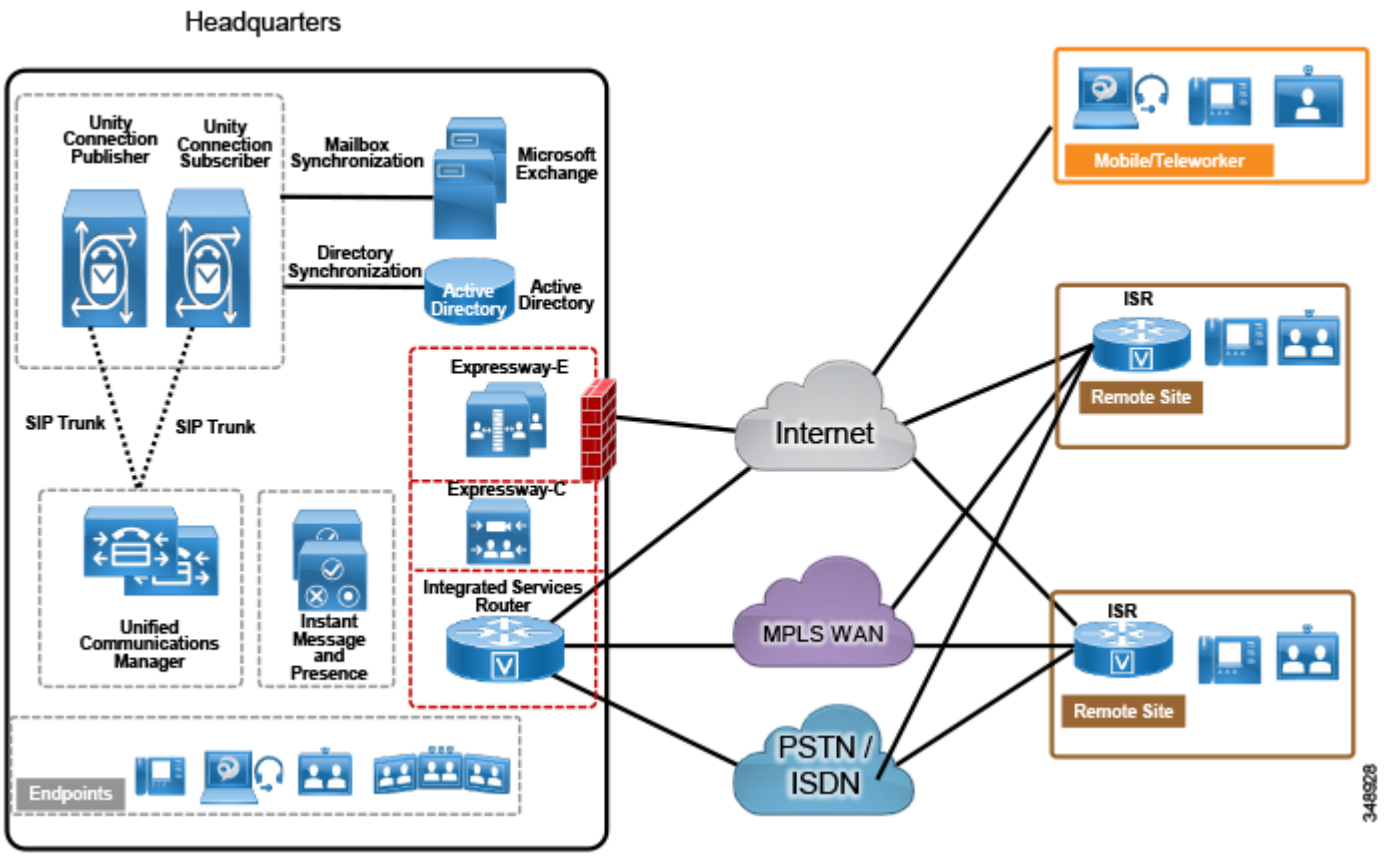
- ユーザは次のいずれかを使用してボイスメール システムにアクセスし、ボイス メッセージを取得できます。
  - Cisco Unified IP Phone、TelePresence エンドポイント、Jabber、およびモバイル デバイス
  - PC または Mac の Web インターフェイス
  - 電子メール クライアント アプリケーション（Microsoft Outlook など）
- ビジュアル ボイスメールにより、Jabber クライアントのボイス メッセージのビジュアル表示にアクセスできます。この表示には、送信者の名前、日付、メッセージの長さも示されます。

コア アーキテクチャ

集中型メッセージングと集中型呼処理

図 5-1 に示すように、集中型メッセージングではUnity Connection は Unified CM クラスタと同じサイトに配置されています。中央サイトから WAN 経由で接続しているリモート ブランチ サイトは、ユニファイド メッセージング サービスについて集中型 Unity Connection に依存しています。Unity Connection は、コール制御に SIP を使用し、メディア パスに RTP を使用して、Unified CM と統合しています。各 Unity Connection クラスタは 2 つのサーバ ノードで構成されており、高可用性と冗長性を備えています。

図 5-1　　アーキテクチャの概要



リモート ブランチ サイトでは、Cisco Unified Survivable Remote Site Telephony（SRST）がバックアップ コール エージェントとしてインストールされており、これは中央の Unity Connection サーバと統合しています。IP WAN の停止時には、リモート ブランチのすべての電話が SRST に登録されます。SRST は、無応答コールと話中コールを PSTN 経由で中央の Unity Connection サーバに送信するように事前に設定されています。

Unified CM の役割

Unified CM は、コール制御機能を備えており、着信側電話が話中または無応答の場合にコールを Unity Connection に転送します。ユーザが電話のメッセージ ボタンを押すか、または外部ネットワークからボイスメール パイロット番号にダイヤルすると、Unified CM はそのコールを Unity Connection にルーティングします。

Unity Connection の役割

集中型メッセージング環境では、Unity Connection によりユーザがボイスメールを保存および取得できます。一般に、Unity Connection に転送されるコールは直接コールであるか、または話中または無応答であった内線コールによるものです。ユーザに対し新しいメッセージが保存されている場合は、エンドポイントにメッセージ受信インジケータ（MWI）が表示されます。通常、電話システムと Unity Connection の間でコールごとに次のコール情報が渡されます。

- 着信側の内線番号
- 発信側の内線番号（内線の場合）、または発信側の電話番号（外線であり、電話システムが発信者 ID をサポートしている場合）
- 転送の理由（内線が通話中である、応答しない、またはすべてのコールを転送するように設定されている）

着信側が応答しないためにコールが転送された場合、Unity Connection は着信側ユーザの標準グリーティングを再生します。着信側電話が通話中であるためにコールが転送された場合、Unity Connection は着信側ユーザの通話中グリーティングを再生します。

Unity Connection は、直接コールと転送コールを異なる方法で処理します。Unity Connection は、コールを受信すると最初に発信者がユーザであるかどうかを判別します。このために、発信者 ID がユーザのプライマリ内線番号または代行内線番号に一致するかどうかを特定します。Unity Connection は一致を検出すると、ユーザが発信していると想定し、そのユーザのボイスメール PIN を入力するよう求めます。発信者 ID がユーザに関連付けられていないと Unity Connection が判断した場合、コールはガイダンスに送信されます。ガイダンスとは、外部の発信者が Unity Connection 自動応答に接続すると再生されるメイン グリーティングです。

Microsoft Exchange の役割

シングル インボックス機能を有効にするため、Unity Connection は Microsoft Exchange と統合されています。Unity Connection のシングル インボックスにより、ユニファイド メッセージングが有効になり、Unity Connection と Microsoft Exchange の間でボイス メッセージが同期されます。これにより、ユーザは電子メール クライアントを使用してボイスメールを取得できます。

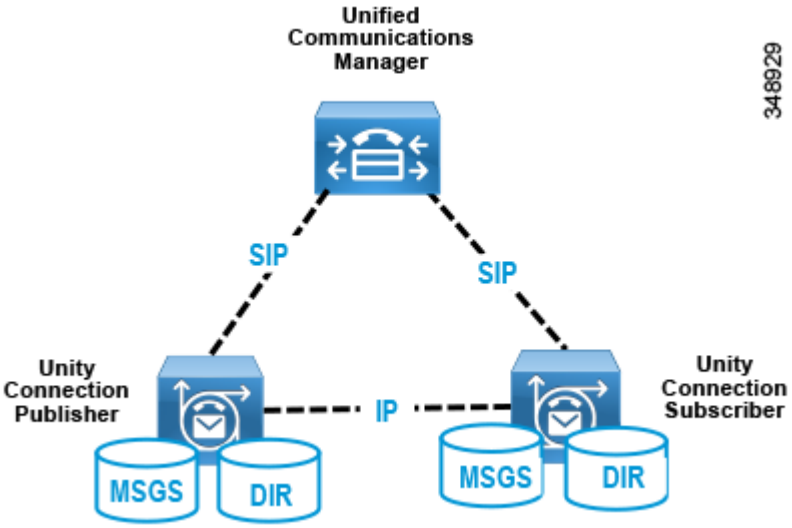
この章では、Microsoft Exchange が統合されている Unified Messaging を中心に説明します。Unity Connection は IBM Lotus Sametime インスタント メッセージング アプリケーションとも統合できます。この統合では、ユーザが Lotus Sametime を使用してボイス メッセージを再生できます。このトピックの詳細については、次の URL から入手可能な Unity Connection のマニュアルを参照してください。

http://www.cisco.com/en/US/products/ps6509/index.html

ユニファイド メッセージングの高可用性

図 5-2 に、アクティブ/アクティブ ペアの Unity Connection を示します。この場合、Unity Connection サーバを同じ建物または異なる建物に設置でき、高可用性と冗長性が実現します。アクティブ/アクティブ ペアの両方のサーバで Unity Connection が稼働しており、この両方のサーバでコールと HTTP 要求が受け入れられ、ユーザ情報とメッセージが保存されます。クラスタ ペアの 1 つのサーバだけがアクティブな場合、Unity Connection は完全なエンドユーザ機能（ボイス コールと HTTP 要求を含む）を維持します。ただし、コールに対する Unity Connection ポート キャパシティは半減し、単一サーバのキャパシティと同様になります。

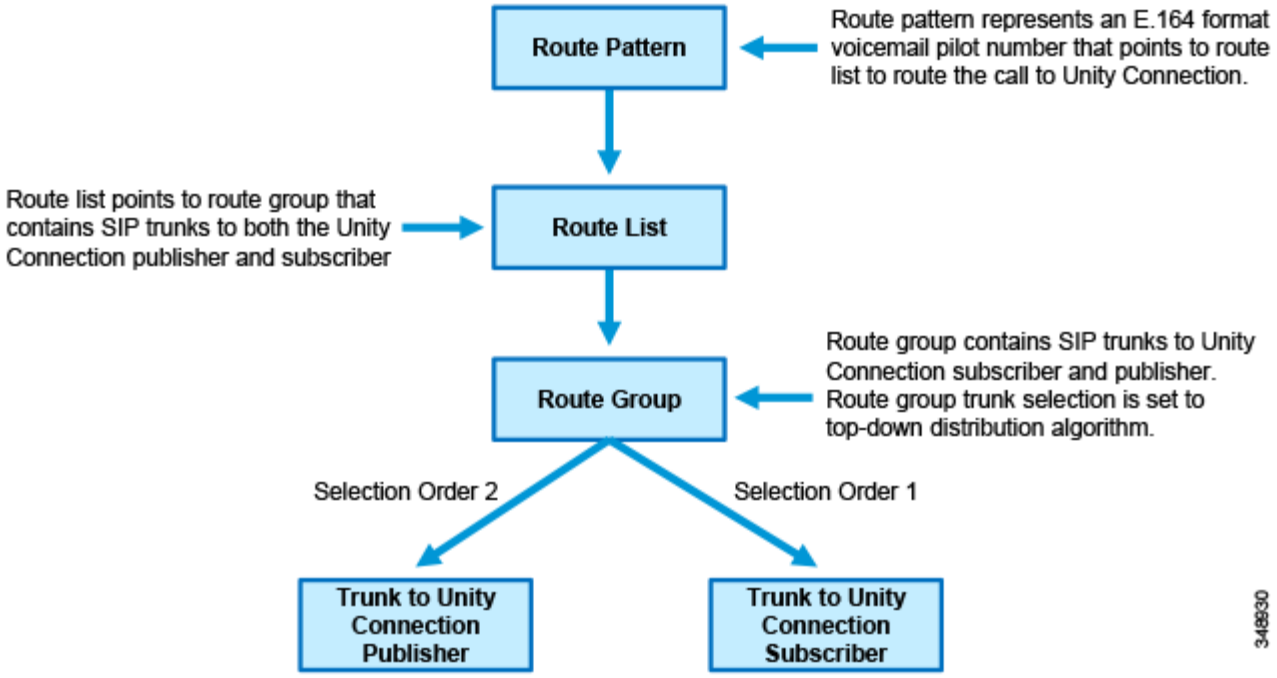
図 5-2　　Unity Connection クラスタ



すべてのユーザ クライアント セッションおよび管理者セッション（IMAP および Cisco Personal Communications Assistant など）と管理トラフィック（Cisco Unity Connection の管理、一括管理ツール、バックアップ操作など）は、Unity Connection パブリッシャ サーバに接続します。パブリッシャ サーバが機能しなくなった場合、ユーザ クライアント セッションと管理者セッションは、Unity Connection サブスクライバ サーバに接続できます。

このトポロジでは、クラスタ内の各 Unity Connection サーバ ノードを指し示す 2 つの個別の Unified CM SIP トランクが必要です。この構成では、高可用性と冗長性の両方が実現します。すべてのコールを最初に Unity Connection サブスクライバ ノードにルーティングするように Unified CM を設定する必要があります。サブスクライバ サーバが使用不可であるか、またはサブスクライバのすべてのポートが使用中の場合、コールはパブリッシャ ノードにルーティングされます。Unified CM と Unity Connection 間で SIP が統合されている場合、トランクの選択は Unified CM ルート パターン、ルート リスト、およびルート グループ構成によって決まります。（図 5-3を参照）。両方のトランクは同じルート グループに属し、同じルート リストに割り当てられています。ルート グループ内のトランクは、優先度順のトランク分配アルゴリズムを使用して並べ替えられます。この方法では、通常の運用時とフェールオーバー時の Unity Connection サーバ ノードの選択設定を Unified CM が制御できます。

図 5-3　　Unity Connection SIP トランクの選択



Unity Connection では、Microsoft Exchange 2010 または Exchange 2013 Database Availability Group（DAG）でのシングル インボックスの使用がサポートされています。DAG は、Microsoft の推奨事項に基づいて導入されます。高可用性を実現するため、Unity Connection ではクライアント アクセス サーバ（CAS）アレイへの接続もサポートされています。この項では、Microsoft Exchange の高可用性展開については説明しません。Exchange の高可用性展開については、http://www.microsoft.com/ から入手できる Microsoft Exchange 製品情報を参照してください。

ライセンスの要件

Unity Connection のライセンスは Cisco Prime License Manager（PLM）により管理されます。Unity Connection のライセンス済み機能を使用するには、その機能の有効なライセンスが PLM サーバにインストールされており、Unity Connection が PLM サーバと通信してライセンスを取得する必要があります。PLM サーバは、企業全体にわたるユーザ ベースのライセンスのシンプルな集中型管理を提供します。

ユニファイド メッセージングの要件

- Unity Connection では、シングル インボックスのために Microsoft Exchange 2003、2007、2010、および 2013 Server がサポートされています。Unity Connection では、Microsoft Business Productivity Online Suite（BPOS）Dedicated Services および Microsoft Office 365 クラウドベース Exchange サーバもサポートされています。
- Exchange サーバと Active Directory ドメイン コントローラ/グローバル カタログ サーバ（DC/GC）は、Microsoft がサポートする任意のハードウェア仮想環境にインストールできます。サポートされているハードウェア プラットフォームの詳細については、http://www.microsoft.com/ から入手できる Microsoft Exchange の製品情報を参照してください。
- Microsoft Exchange メッセージ ストアは、Microsoft がサポートする任意のストレージ エリア ネットワーク コンフィギュレーションに格納できます。サポートされているストレージ エリア ネットワークの詳細については、http://www.microsoft.com/ から入手できる Microsoft Exchange の製品情報を参照してください。
- 各サーバで 50 個のボイス メッセージング ポートごとに、Unity Connection と Microsoft Exchange の間でメッセージ同期のために 7 Mbps の帯域幅が必要となります。
- Unity Connection のデフォルト設定は、最大 2,000 ユーザと、Unity Connection と Microsoft Exchange サーバの間での最大 80 ミリ秒のラウンドトリップ遅延に十分に対応できます。2,000 を超えるユーザや 80 ミリ秒を超える遅延に対応する場合は、デフォルト設定を変更できます。詳細については、次の場所にある『*Design Guide for Cisco Unity Connection*』で遅延に関する情報を参照してください。

  http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-implementation-design-guides-list.html

Unity Connection のスケーリング

Unity Connection クラスタは、最大 2 つのノード（アクティブ/アクティブ展開の 1 つのパブリッシャと 1 つのサブスクライバ）で構成されます。通常の運用時には、アクティブ/アクティブ展開では呼処理負荷分散は発生しません。Unified CM は、すべてのコールを最初に Unity Connection サブスクライバ サーバにルーティングするように設定されています。すべてのポートが使用中であるか、またはサブスクライバ サーバが使用不可の場合、コールはパブリッシャにルーティングされます。Unity Connection のサイジングでは、次のパラメータを考慮してください。

- 現在および将来のユーザの合計数。
- ボイス メッセージング用の必要ストレージ容量。
- 各プラットフォームでサポートされるボイスメール ポートの数。

Unity Connection のスケーリングの詳細については、サイジングの章を参照してください。

Cisco Unity Connection 導入プロセス

前提条件

ユニファイド メッセージング アーキテクチャを導入する前に、次の点を確認してください。

- Unified CM がインストールされており、コール制御向けに設定されている（コール制御の章を参照）。
- Microsoft Exchange がインストールされており、電子メール サーバとして設定されている。サポートされている Exchange のバージョンについては、ユニファイド メッセージングの要件の項を参照してください。

導入環境の概要

このプリファード アーキテクチャの目的上、米国内の 3 か所のサイト（SJC、RCD、RTP）に対応する集中型メッセージング導入モデルを想定します。集中型メッセージングの導入では最初に、Unity Connection クラスタをインストールし、続いてプロビジョニングと設定を行います。Cisco Unity Connection で集中型メッセージングを導入するには、次のタスクを記載の順に行います。

1. Unity Connection クラスタのプロビジョニング
2. Unity Connection 統合のための Unified CM の設定
3. Unity Connection の基本設定
4. シングル インボックスの有効化
5. ビジュアル ボイスメールの有効化
6. SRST モードでのボイスメール
7. 2 つの Unity Connection クラスタの HTTPS インターネットワーキング

（注）　このマニュアルでは、非デフォルト値およびその他の設定フィールド値だけが示されています。フィールド設定値が示されていない場合は、デフォルト値が想定されます。

1. Unity Connection クラスタのプロビジョニング

Unity Connection サーバ ノードをクラスタリングする場合、サーバ ペアの 1 方がパブリッシャ サーバ、もう 1 方がサブスクライバ サーバとして指定されます。

パブリッシャ

Unity Connection では、アクティブ/アクティブの高可用性を実現するために 2 つのサーバのみがクラスタでサポートされています。パブリッシャ サーバは最初にインストールするサーバであり、データベースとメッセージ ストアをパブリッシュし、クラスタ内のもう一方のサブスクライバ サーバにこの情報をレプリケートします。

サブスクライバ

ソフトウェアをインストールしたら、サブスクライバ サーバ ノードをパブリッシャに登録して、データベースとメッセージ ストアのコピーを取得します。

Unity Connection メールボックス ストア

インストール時に、Unity Connection により次のものが自動的に作成されます。

- ディレクトリ データベース：システム設定情報（ユーザ データ、テンプレート、サービス クラスなど）に使用されます。
- メールボックス ストア データベース：ボイス メッセージに関する情報（メッセージの送信先、送信時刻、ハードディスク上の WAV ファイルの場所など）に使用されます。
- オペレーティング システム ディレクトリ：ボイス メッセージの WAV ファイルに使用されます。

サーバを同じ建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection での着信コールと発信コールのため、ファイアウォールの TCP ポートと UDP ポートがオープンである必要があります。これについては、『*Security Guide for Cisco Unity Connection*』の「*IP Communications Required by Cisco Unity Connection*」の章を参照してください。
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- サーバはファイアウォールによって隔離されてはなりません。
- 両方の Unity Connection サーバが同一のタイム ゾーンに位置している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。

サーバを異なる建物に設置する場合の Unity Connection クラスタ導入の前提条件

- Unity Connection での着信コールと発信コールのため、ファイアウォールの TCP ポートと UDP ポートがオープンである必要があります。これについては、『*Security Guide for Cisco Unity Connection*』の「*IP Communications Required by Cisco Unity Connection*」の章を参照してください。
- 2 つの仮想マシンが含まれているクラスタでは、この両方のマシンが同一の仮想プラットフォーム オーバーレイに属している必要があります。
- 両方の Unity Connection サーバ ノードは同一の電話システムに統合されている必要があります。
- 両方の Unity Connection サーバで、同じ機能と構成が有効である必要があります。
- 各 Unity Connection サーバ ノードのボイス メッセージング ポートの数に応じて、サーバ ノード間の接続に、次に示す定常輻輳のない保証帯域幅が必要です。
  - 各サーバで 50 個のボイス メッセージング ポートごとに、7 Mbps の帯域幅が必要となります。
  - 最大往復遅延は、150 ミリ秒（ms）以下でなければなりません。

Unity Connection クラスタを導入するには

- ポートの最大数とユーザの最大数に基づいて、Unity Connection ノードに導入する VMware Open Virtual Archive（OVA）テンプレートを決定します。Unity Connection のスケーリングの項を参照してください。
- 両方の Unity Connection ノードをホスト A レコードとして企業のドメイン ネーム サービス（DNS）サーバに追加します。たとえば、パブリッシャ Unity Connection ホスト名を US-CUC1.ent-pa.com と設定し、サブスクライバ ホスト名を US-CUC2.ent-pa.com と設定します。
- インストールに必要なネットワーク パラメータを判別します。
  - サーバのタイム ゾーン
  - ホスト名、IP アドレス、ネットワーク マスク、およびデフォルト ゲートウェイ。ホスト名と IP アドレスが前の DNS 設定に一致していることを確認します。
  - DNS IP アドレス
  - ネットワーク タイム プロトコル（NTP）サーバの IP アドレス
- 前述の OVA ファイルを Cisco Web サイトからダウンロードします。
- VMware vSphere Client を使用して Unity Connection パブリッシャ サーバ ノードを導入します。
- Unity Connection パブリッシャのインストールが完了したら、プライマリ サーバのクラスタ設定にサブスクライバの詳細を追加します。
- VMware vSphere Client を使用して Unity Connection サブスクライバ サーバ ノードを導入します。

2. Unity Connection 統合のための Unified CM の設定

Unity Connection が Unified CM と通信する前に、Unified CM で実行する必要があるタスクがあります。Unity Connection は SIP トランクを介して Unified CM と通信します。この項では、Unified CM を Unity Connection と統合するために必要なタスクの概要を説明します。

SIP トランク セキュリティ プロファイル

メディアおよびシグナリングの暗号化に関して、このマニュアルではこれらの暗号化は使用されず、代わりに Unified CM と Unity Connection サーバ ノードの間には非セキュアな SIP トランクが実装されていることを前提としています。デバイス セキュリティ モードが [非セキュア（Non Secure）] に設定された状態で、Unity Connection に新規 SIP トランク セキュリティ プロファイルを作成します。表 5-2に、SIP トランク セキュリティ プロファイルの設定を示します。

表 5-2　SIP トランク セキュリティ プロファイルの設定

パラメータ	値	コメント
[名前（Name）]	Unit Connection SIP トランク セキュリティ プロファイル	セキュリティ プロファイルの名前を入力します。
[説明（Description）]	Unit Connection SIP トランク セキュリティ プロファイル	プロファイルの説明を入力します。

表 5-2　SIP トランク セキュリティ プロファイルの設定（続き）

パラメータ	値	コメント
[デバイスセキュリティモード（Device Security Mode）]	[非セキュア（Non Secure）]	SIP トランクのセキュリティ モード。
[ダイアログ外 REFER の許可（Accept Out-of-Dialog refer）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの ダイアログ外 REFER メッセージを受け入れることを指定します。
[未承諾 NOTIFYの許可（Accept unsolicited notification）]	オン	Unified CM が、SIP トランク経由で着信する非インバイトの未承諾 NOTIFY メッセージを受け入れることを指定します。Unity Connection から MWI メッセージを受け入れるには、このパラメータをオンにする必要があります。
[REPLACE ヘッダの許可（Accept replaces header）]	オン	Unified CM が、既存の SIP ダイアログを置き換える新しい SIP ダイアログを受け入れることを指定します。これにより、Cisco Unity Connection が開始する監視転送に使用される "REFER w/replaces" を渡すことができるようになります。

SIP プロファイル

Unity Connection への SIP トランクの SIP プロファイルを設定します。標準 SIP プロファイルをコピーし、その名前を **Unity Connection SIP Profile** に変更します。Unified CM サーバの IP アドレスが、Unified CM により送信される SIP 発呼側情報に含まれないようにするには、[SIP要求で完全修飾ドメイン名を使用（Use Fully Qualified Domain Name in SIP Requests）] チェックボックスをオンにします。[サービスタイプ「なし(デフォルト)」のトランクの接続先ステータスをモニタするためにOPTIONS Pingを有効にする（Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"）] チェックボックスがオンになっていることを確認します。これにより、システムが Unity Connection ノードへの接続の状況を追跡できます。

OPTIONS Ping が有効な場合、トランクの SIP デーモンを実行する各ノードは、トランクの各宛先 IP アドレスに対して OPTIONS 要求を定期的に送信して到達可能性を判断し、到達可能なノードにのみコールを送信します。宛先アドレスが OPTIONS 要求に応答しない場合、Service Unavailable（503）応答または Request Timeout（408）応答を送信する場合、または TCP 接続を確立できない場合、そのアドレスは「アウト オブ サービス」と見なされます。1 つ以上のノードが、1 つ以上の宛先アドレスから（408 または 503 以外の）応答を受信した場合、トランク全体の状態は「イン サービス」と見なされます。SIP トランク ノードは、トランクの設定済み宛先 IP アドレス、またはトランクの DNS SRV エントリの解決済み IP アドレスに対して OPTIONS 要求を送信できます。すべての SIP トランクで SIP OPTIONS Ping を有効にすることを推奨します。有効にすることで、Unified CM は、コールごとの状態、ノードごとの状態、およびタイムアウトに基づいて判別するのではなく、動的にトランクの状態を追跡することができるためです。

SIP トランク

クラスタ内の Unity Connection サーバ ノードごとに 1 つずつ、合計で 2 つの個別 SIP トランクを作成します。表 5-3 に SIP トランクの設定を示します。

表 5-3　Unity Connection サーバへの SIP トランクのパラメータ設定

パラメータ	値	説明
[名前（Name）]	US_CUC1_SIP_Trunk	Unity Connection への SIP トランクの固有名を入力します。
[説明（Description）]	Unity Connection パブリッシャ	SIP トランクの説明を入力します。
[デバイスプール（Device Pool）]	Trunks_and_Apps	Unity Connection のデバイス プールを入力します。（コール制御の章を参照。）
[すべてのアクティブな Unified CM ノードで実行（Run on All Active Unified CM Nodes）]	オン	SIP トランクを使用した発信コールでは、Unified CM 呼処理サブスクライバ間のクラスタ内制御シグナリングが必要ではないことを指定します。
[コールルーティング情報 - インバウンド コール（Call Routing Information - Inbound Calls）]		
[コーリング サーチ スペース（CSS）（Calling Search Space (CSS)）]	ボイスメール（CSS 設定の詳細については、コール制御の章を参照してください。）	割り当てられる CSS には、DID、DID 以外の番号、URI パーティションなどのすべてのネットワーク上の宛先が含まれています。CSS にこれらのすべてのパーティションが含まれていないと、Unity Connection からの MWI 未承認 NOTIFY メッセージがユーザの電話に到達しません。
[Diversion ヘッダー配信のリダイレクト - インバウンド（Redirecting Diversion Header Delivery - Inbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[コールルーティング情報 - アウトバウンド コール（Call Routing Information - Outbound Calls）]		
[発呼側および接続側情報形式（Calling and Connected Party Info Format）]	[接続側にのみ URI および DN を配信（使用可能な場合）（Deliver URI and DN in connected party, if available）]	このオプションは、Unified CM がディレクトリ番号、ディレクトリ URI、またはディレクトリ番号とディレクトリ URI の両方を含むアドレスを、発信 SIP メッセージの SIP ID ヘッダーに挿入するかどうかを決定します。
[Diversion ヘッダー配信のリダイレクト - アウトバウンド（Redirecting Diversion Header Delivery - Outbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[SIP 宛先情報（SIP Destination Information）]		
[宛先アドレス（Destination Address）]	10.195.100.20	Unity Connection サーバの IP アドレスを入力します。

表 5-3　Unity Connection サーバへの SIP トランクのパラメータ設定（続き）

パラメータ	値	説明
[SIP トランク セキュリティ プロファイル（SIP Trunk Security Profile）]	Unit Connection SIP トランク セキュリティ プロファイル	表 5-2を参照してください。
[SIPプロファイル（SIP Profile）]	Unity Connection SIP プロファイル	SIP プロファイルを参照してください。

ルート グループ

Unity Connection クラスタに対し、別のルート グループ RG_CUC を作成します。このルート グループには、Unity Connection サブスクライバ ノードとパブリッシャ ノードへの SIP トランクが含まれています。リストに、サブスクライバ ノードに接続する SIP トランク（US_CUC2_SIP_Trunk）が最初に示され、続いてパブリッシャ ノードに接続する SIP トランク（US_CUC1_SIP_Trunk）が示されていることを確認してください。ルート グループ分配アルゴリズムとして、[優先度順（Top Down）] トランク選択方式を設定する必要があります。[優先度順（Top Down）] 分配アルゴリズムが設定されているルート グループでは常に、コールが最初に Unity Connection サブスクライバ サーバ ノード（US-CUC2）に送信されます。Unity Connection サブスクライバ サーバ ノードがビジーまたは使用不可の場合、コールはパブリッシャ サーバ ノード（US-CUC1）に送信されます。

ルート リスト

Unity Connection クラスタに対し、別のルート リスト RL_CUC を作成します。このルート リストには、前述の説明で作成した Unity Connection ルート グループ（RG_CUC）だけが含まれている必要があります。[このルートリストを有効にする（Enable this Route List）] と [すべてのアクティブなUnified CM ノードで実行（Run on all Active Unified CM Nodes）] オプションが選択されていることを確認してください。

ルート パターン

前述の説明で作成した Unity Connection ルート リストを指し示すボイスメール パイロット番号の別のルート パターンを作成します。この番号はボイスメール パイロット番号に一致している必要があります。表 5-4に、ルート パターンの設定例を示します。

表 5-4　Unity Connection パイロット番号:ルート パターンの例

パラメータ	値
[ルートパターン（Route Pattern）]	+14085554999
[ルートパーティション（Route Partition）]	DN
[ゲートウェイ/ルートリスト（Gateway/Route List）]	RL_CUC
[コールの分類（Call Classification）]	OnNet
[外部ダイヤルトーンの提供（Provide Outside Dial Tone）]	オフ

ボイスメールパイロット

ボイスメール パイロット番号は、ユーザがボイス メッセージにアクセスするための電話番号を指定します。Unified CM は、ユーザが IP エンドポイントの [メッセージ（Messages）] ボタンを押すと、自動的にボイスメール パイロット番号にダイヤルします。3 つのサイトすべてに対して 1 つのボイスメール パイロット番号が作成されます。表 5-5に、ボイスメール パイロットの設定例を示します。

表 5-5　　ボイスメール パイロットの例

パラメータ	値
[ボイスメールパイロット番号（Voice Mail Pilot Number）]	+14085554999
[コーリングサーチスペース（Calling Search Space）]	DN
[説明（Description）]	VM パイロット
[システムのデフォルトボイスメールパイロットに設定（Make this the default Voice Mail Pilot for the system）]	オン

リモート サイトのボイスメール ユーザは、各自の DID 範囲からボイスメール アクセス番号にダイヤルして、PSTN からメッセージを確認できます。ボイスメール PSTN アクセス番号をボイスメール パイロット番号に変換するためのトランスレーション パターンが個別に作成されます。表 6 に、ボイスメール パイロットのトランスレーション パターンの設定を示します。

表 5-6　　ボイスメール パイロットのトランスレーション パターンの例

パラメータ	値
[トランスレーションパターン（Translation Pattern）]	+19195551999
[パーティション（Partition）]	DN
[発信側コーリングサーチスペースを使用（Use Originators Calling Search Space）]	オン
[ルートオプション（Route Option）]	[このパターンをルーティング（Route this pattern）]
[着信側トランスフォーメーション（Called Party Transformations）]	
[着信側トランスフォーメーションマスク（Called Party Transform Mask）]	+14085554999

他のリモート サイト向けに追加のトランスレーション パターンが作成されます。

ボイスメール プロファイル

すべてのエンドポイント デバイスとエクステンション モビリティ プロファイルで、各ユーザの電話回線に対してボイスメール プロファイルが割り当てられます。このプロファイルにより、ユーザはエンドポイントの [メッセージ（Messages）] ボタンを押すだけで、ボイスメール システムにワンタッチでアクセスできます。Unity Connection が単一電話システムに統合されている場合は、デフォルトのボイスメール プロフィルを使用することを推奨します。エンドポイント デバイスでの回線の初期プロビジョニング時に、デフォルトのボイスメール プロファイル（[なし（None）]）が電話番号に割り当てられます。ボイスメールにアクセスする必要がないユーザの場合、そのエンドポイント回線にボイスメール プロファイルが割り当てられません。表 5-7に、ボイスメール プロファイルの設定例を示します。

表 5-7　　ボイスメール プロファイルの例

パラメータ	値
[ボイスメールプロファイル名（Voice Mail Profile Name）]	デフォルト
[説明（Description）]	VM プロファイル
[ボイスメールパイロット（Voice Mail Pilot）]	+14085554999/DN
[ボイスメールマスク（Voice Mail Mask）]	空欄
[システムのデフォルトボイスメール プロファイルとして使用する（Make this the default Voice Mail Profile for the System）]	オン

3. Unity Connection の基本設定

サービスのアクティブ化

- Unity Connection のインストールが完了したら、Cisco Unified Serviceability にログインし、パブリッシャ サーバ ノードの **DirSync** サービスをアクティブにします。
- [ユニファイド サービスアビリティ（Unified Serviceability）] で [ツール（Tools）] –> [コントロールセンターの機能サービス（Control Centre-Feature Services）] に移動します。パブリッシャ サーバ ノードで Cisco DirSync サービスが開始していることを確認します。
- [Unity Connectionのサービスアビリティ（Unity Connection Serviceability）] で [ツール（Tools）] –> [サービス管理（Service Management）] に移動します。プライマリおよびセカンダリ Unity Connection サーバ ノードでサービスのステータスを確認します。表 5-8に、この導入環境のサービス ステータスを示します。

表 5-8　Unity Connection サービス ステータス

サービス	プライマリ Unity Connection	セカンダリ Unity Connection
ステータスのみのサービス（OS コマンド ライン インターフェイスから非アクティブにできます）		
このカテゴリのすべてのサービス	[はい（Yes）]	[はい（Yes）]
重要なサービス		
Connection Conversation Manager	[はい（Yes）]	[はい（Yes）]
Connection Mailbox Sync	[はい（Yes）]	[いいえ（No）]
Connection Message Transfer Agent	[はい（Yes）]	[いいえ（No）]
Connection Mixer	[はい（Yes）]	[はい（Yes）]
Connection Notifier	[はい（Yes）]	[いいえ（No）]
基本サービス		
このカテゴリのすべてのサービス	[はい（Yes）]	[はい（Yes）]
オプション サービス		
Connection Branch Sync Service	[いいえ（No）]	[いいえ（No）]
Connection Digital Networking Replication Agent	[いいえ（No）]	[いいえ（No）]
このカテゴリのその他のすべてのサービス	[はい（Yes）]	[はい（Yes）]

データベース レプリケーション

プライマリおよびセカンダリ両方の Unity Connection サーバ ノードでサービスをアクティブにした後で、サブスクライバ ノードがパブリッシャ ノードに接続できることを確認します。また、両方のノードで OS コマンド ライン インターフェイス（CLI）のコマンド **show perf query class "Number of Replicates Created and State of Replication"** を使用して、データベース レプリケーションのステータスを確認します。

Unified CM の統合

各 Unity Connection クラスタは、同じ場所に配置されている Unified CM クラスタと統合されます。これにより、Unified CM クラスタ専用の各 Unity Connection クラスタによる単純な統合モデルが実現します。Unified CM では Unity Connection クラスタとの相互接続のために SIP トランクが設定されますが、Unity Connection システムではキャパシティとライセンスの目的で、ボイスメール ポートが使用されます。この項では、設計時の考慮事項、キャパシティ プランニング、ボイスメール ポートの設定について説明します。

ボイスメール ポートのオーディオ コーデック設定

Unity Connection では、Unity Connection SIP シグナリングでサポートされるすべてのオーディオ コーデック形式（G.711 mu-law、G.711 a-law、G.722、G.729、および iLBC）でのコールは常に、PCM リニアにトランスコードされます。録音は、PCM リニアから、Unity Connection Administration 録音でシステム全体に設定されているシステム レベルの録音オーディオ コーデック（PCM linear、G.711 mu-law、G.711 a-law、G.729a、G.726-a）にエンコードされます。デフォルトは G.711 mu-law です。

この項では、発信側デバイスと Unity Connection の間でネゴシエートされるオーディオ コーデックを*回線コーデック*と呼び、システムレベルの録音用オーディオ コーデックとして設定されたオーディオ コーデックを*録音コーデック*と呼びます。

サポートされる回線コーデック（公表コーデック）

- G.711 mu-law
- G.711 a-law
- G.722
- G.729
- iLBC

サポートされる録音コーデック（システムレベルの録音オーディオ コーデック）

- PCM リニア
- G.711 mu-law（デフォルト）
- G.711 a-law
- G.729a
- G.726
- GSM 6.10

トランスコーディングは、本来すべての接続で発生するので、ライン コーデックと録音コーデックが違っても、システムへの影響にほとんど違いはありません。たとえば、G.729a を回線コーデックとして、G.711 mu-law を録音コーデックとして使用しても、Unity Connection サーバにはトランスコーディングに伴う大きな追加負荷はかかりません。しかし、iLBC コーデックまたは G.722 コーデックはトランスコーディングにより多くの計算を必要とするので、Unity Connection サーバに大きな追加負荷がかかります。そのため、Unity Connection サーバがサポートできる G.722 または iLBC 接続の数は、G.711 mu-law 接続の数の半分のみです。

このトポロジの例では、システム録音コーデックはデフォルト（G.711 mu-law）のままです。サポートされる回線コーデックは G.729 および G.711 mu-law に設定されます。このデフォルト設定を使用する場合、同一の Unity Connection サイトのユーザは G711 mu-law を使用します。中央の Unity Connection サーバに WAN 経由で接続するユーザの場合、選択される回線コーデックは G.729 です。

G.722 コーデックまたは iLBC コーデックを回線コーデック（アドバタイズされているコーデック）として使用すると、Cisco Unity Connection サーバでプロビジョニング可能なボイス ポートの数が減少します。G.722 または iLBC コーデックを使用する場合に各プラットフォーム オーバレイでサポートされるボイス ポートの数の詳細については、『Virtualization for Cisco Unity Connection』を参照してください。

電話システムの設定

電話システムの統合により、Unity Connection と Unified CM の間の通信が実現します。Unity Connection が 1 つの Unified CM クラスタと統合している場合は、デフォルトの **PhoneSystem** を使用することを推奨します。表 5-9に、電話システムの設定を示します。

表 5-9　　電話システムの設定

パラメータ	値	説明
[電話システムの名前（Phone System Name）]	PhoneSystem	電話システム
[デフォルトTRAP電話システム（Default TRAP Phone System）]	オン	電話システムにより TRAP 接続が有効になるので、ボイスメール ボックスを使用していない管理者とユーザが、Unity Connection Web アプリケーションで電話から録音、再生できます。

表 5-9　電話システムの設定（続き）

パラメータ	値	説明
[内線番号を使用したコールループの検出（Call Loop Detection by Using Extension）]		
[転送メッセージ通知コールに対して有効にする(内線番号を使用)（Enable for Forwarded Message Notification Calls (by Using Extension)）]	オン	（携帯電話などの）デバイスに送信される新規メッセージ通知、およびデバイスが応答しなかったために Unity Connection にデバイスが再転送した新規メッセージ通知を Unity Connection で内線番号を使用し検出して拒否します。コール ループが検出されず拒否されない場合、コールによってユーザ宛ての新しいボイス メッセージが作成され、Unity Connection が新規メッセージ通知のコールをデバイスに送信します。
[発信コール規制（Outgoing Call Restrictions）]		
[発信コールを有効にする（Enable outgoing calls）]	オン	Unity Connection は、必要に応じて電話システムを通じて発信コール（MWI の設定など）をかけます。

ポート グループの設定

ポート グループを使用して、Unified CM クラスタと Unity Connection クラスタの間の SIP 通信を制御します。ポート グループを使用することで、システムは Unity Connection サーバが受け入れる SIP メッセージの送信元 Unified CM と、Unity Connection サーバが発信コールを Unified CM サーバにルーティングするときに使用する設定と順序を制限および指定できます。Unity Connection サーバは、Unity Connection 向けの Unified CM SIP ルーティング設計をミラーするように設定されているため、Unity Connection サーバで発信ルーティングが1 番目に使用可能な Unified CM サブスクライバ ノードを選択するように設定する必要があります。表 5-10に、ポート グループの設定を示します。

表 5-10　ポート グループの設定

パラメータ	値	説明
[表示名（Display Name）]	PhoneSystem-1	電話システムの記述名
[連動方法（Integration Method）]	SIP	Unity Connection と Unified CM の接続に使用する連動方法。
[セッション開始プロトコル(SIP)の設定（Session Initiation Protocol (SIP) Settings）]		
[SIPサーバで登録する（Register with SIP Server）]	オン	これにより、Cisco Unity Connection が SIP サーバに登録されます。
[SIPサーバ（SIP Servers）]		
[順序0（Order 0）]	10.195.100.21	順序 0 に設定されている SIP サーバには高い優先度が設定されます。プライマリ Unified CM 呼処理ノードの IP アドレスを入力します。

表 5-10　ポート グループの設定（続き）

パラメータ	値	説明
[順序1（Order 1）]	10.195.100.20	順序 1 に設定されている SIP サーバには低い優先度が設定されます。セカンダリ Unified CM 呼処理ノードの IP アドレスを入力します。
[ポート（Port）]	5060	Unity Connection が使用する Unified CM サーバの TCP ポートを入力します。

ボイス メッセージング ポートのサイジングに関する考慮事項

クラスタ内の各 Unity Connection サーバでは、いずれかのサーバが停止した場合のために、次のダイヤルイン機能用のボイス メッセージング ポートが指定されている必要があります。

- コールへの応答

各 Unity Connection サーバではさらに、次の発信機能用のボイス メッセージング ポートが指定されている必要があります。

- メッセージ受信インジケータ（MWI）の送信
- メッセージ到着通知の実行
- 電話での録音および再生（TRAP）接続の許可

システムのボイスメール ポートの合計数の 20% を、メッセージ通知、MWI の発信、および TRAP 用に確保しておくことを推奨します。これにより、コールへの応答とポートでの発信のためにポートでコール ブロッキングが発生する可能性が低減します。

あるいは、以前のボイスメール トラフィック レポートを使用して応答ポートと発信ポートを選択することもできます。Port Usage Analyzer Tool を使用して過去 1 ～ 2 週間のトラフィックを収集し、実際のポート トラフィックに基づいて調整できます。

ポート設定

前述の項で説明したように、ポートは着信ポートまたは発信ポートのいずれかになります。表 5-11に、ボイスメール ポート割り当ての設定例を示し、表 5-12に、応答ポートの設定のための設定テンプレートを示します。

表 5-11　ボイスメール ポート割り当ての設定例

CUC サーバ	ポート範囲	機能
US-CUC1	1 ～ 80	応答
US-CUC2	1 ～ 80	応答
US-CUC1	81 ～ 100	発信
US-CUC2	81 ～ 100	発信

表 5-12　　ボイスメール応答ポートの設定例

パラメータ	値	説明
[有効（Enabled）]	オン	電話システム ポートを有効にするには、このボックスをオンにします。
[電話システムポート（Phone System Port）]		
[ポート名（Port Name）]	自動作成	Unity Connection によりポート名が自動的に作成されます。
[電話システム（Phone System）]	電話システム	適切な電話システムを選択します。
[ポートグループ（Port Group）]	PhoneSystem-1	適切なポート グループを選択します。
[サーバ（Server）]	US-CUC2/US-CUC1	Cisco Unity Connection（CUC）サブスクライバ ノードを最初に選択し、同様に CUC パブリッシャ ノードのポートを追加します。
[電話の動作（Phone behavior）]		
[呼び出しに応答（Answer Call）]	オン	この設定により、コールに応答するポートが指定されます。
[メッセージ通知を実行する（Perform Message Notification）]	オフ	この設定により、メッセージをユーザに通知するためのポートが指定されます。
[MWI要求を送信する（Send MWI Requests）]	オフ	この設定により、MWI オン/オフ要求を送信するためのポートが指定されます。
[TRAP接続を許可する（Allow TRAP Connections）]	オフ	この設定により、Telephony Recording and Playback（TRAP）接続のポートが指定されます。

表 5-12に示す設定は、ボイスメールの発信ポートを作成するときにも使用する必要があります。ただし発信ポートの場合は、[呼び出しに応答（Answer Call）] パラメータをオフにし、[メッセージ通知を実行する（Perform Message Notification）]、[MWI要求を送信する（Send MWI Requests）]、および [TRAP接続を許可する（Allow TRAP Connections）] パラメータをオンにします。

Active Directory の統合

Unity Connection では、Active Directory に対する認証を使用する Unity Web アプリケーション（エンドユーザ向けの Cisco Personal Communications Assistant（PCA）など）で、Microsoft Active Directory 同期および認証がサポートされています。同様に、Unity Connection ボイス メッセージへにアクセスするために使用する IMAP 電子メール アプリケーションは、Active Directory に対して認証されます。電話ユーザ インターフェイスまたはボイス ユーザ インターフェイスによる Unity Connection ボイス メッセージへのアクセスでは、引き続き Unity Connection データベースに対して数値パスワード（PIN）による認証が行われます。

Active Directory で、Unity Connection がユーザ検索ベースに指定されているサブツリーにアクセスするときに使用する管理者アカウントを作成する必要があります。検索ベースのすべてのユーザ オブジェクトを「読み取る」ための最小限の権限が設定されており、また、有効期限のないパスワードが設定されている Unity Connection 専用アカウントを使用することを推奨します。

Unified CM の [メールID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。統合プロセスでは、これにより LDAP のメール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。Unity Connection は Unified Messaging アカウントの [社内電子メールアドレス（Corporate Email Address）] を使用してシングル インボックスを有効にします。

Unity Connection と Active Directory の統合により、ユーザ情報のインポートが可能になります。Unity Connection と Active Directory の統合にはさまざまなメリットがあります。

- ユーザの作成：Active Directory からデータをインポートして Unity Connection ユーザを作成できます。
- データの同期：Unity Connection は、Unity Connection データベースのユーザ データと Active Directory のデータを自動的に同期するように設定されています。
- シングル サインオン：Unity Connection Web アプリケーションのユーザ名とパスワードを Active Directory に対して認証するように Unity Connection を設定します。これにより、ユーザが複数のアプリケーション パスワードを管理する必要がなくなります。

Active Directory の設定については、コール制御の章を参照してください。

Unity Connection のパーティションと CSS

この導入環境のすべてのユーザは、デフォルトのコーリング サーチ スペース（US-CUC1 サーチ スペース）で設定されています。このサーチ スペースにはデフォルトのパーティション（US-CUC1 パーティション）が含まれています。

規制テーブル

Unity Connection は、ボイスメール システムが未承認の電話番号を呼び出すことがないようにするため、規制テーブルを使用します。通常、これらのルールは許可されている番号またはブロックされている番号のいずれかに完全一致するように設定されています。この導入環境では、Unity Connection システムはボイスメール システムからのコール ブロックの規制ルールを使用せず、代わりに SIP トランク着信コーリング サーチ スペース（CSS）を使用して、Unity Connection からの不正なコールを防止します。SIP トランク CSS は、Unity Connection に対しネットワーク上の宛先のみへの発信を許可するように設定されています。表 5-13に、デフォルトの転送規制テーブルの設定を示します。

表 5-13　Unity Connection の規制テーブル

順序	ブロック	パターン
0	このチェックボックスをオフにします。	+*
1	このチェックボックスをオフにします。	9+*
2	このチェックボックスをオフにします。	91???????*
3	このチェックボックスをオフにします。	9011???????*
4	このチェックボックスをオフにします。	9???????????*

表 5-13　Unity Connection の規制テーブル（続き）

順序	ブロック	パターン
5	このチェックボックスをオフにします。	900
6	このチェックボックスをオフにします。	*

Unity Connection には、この他に、デフォルトのファクス、デフォルトの発信ダイヤル、デフォルトのシステム転送、およびユーザ定義および自動追加の代行内線番号用の 4 つの規制テーブルがあります。これらの規制テーブルも、表 5-13で説明する設定を使用して無効にすることができます。

サービス クラス

サービス クラス（CoS）は、Unity Connection ボイスメールのユーザに対する制限と機能を定義します。サービス クラスは一般にユーザ テンプレートで定義され、このテンプレートがユーザ アカウントの作成時にアカウントに適用されます。この導入環境では、デフォルトのボイスメール ユーザ の COS がすべてのユーザに関連付けられています。

ユーザ プロビジョニング

ユーザを Unity Connection にインポートするには、Active Directory サーバのユーザ テンプレートを使用します。このユーザ テンプレートには、特定のユーザのグループに共通する設定が含まれています。ユーザ アカウントの作成時に、ユーザ テンプレートの共通設定がユーザに継承されます。ローカル タイム ゾーンの各サイトに個別のユーザ テンプレートを作成する必要があります。表 5-14に、ユーザ テンプレートの設定を示します。

表 5-14　ボイスメール ユーザ テンプレート

セクション	フィールド	値
[基本設定（Basics）]	[エイリアス（Alias）]	SJC_User_Template
	[表示名（Display Name）]	SJC_User_Template
	[表示名の生成（Display Name Generation）]	[名、姓の順（First name, then last name）]
	[電話システム（Phone System）]	電話システム
	[サービスクラス（Class of Service）]	[ボイスメールユーザの COS（Voice Mail User COS）]
	[次回ログイン時に自己登録を設定する（Set for Self-enrollment at Next Login）]	オン
	[ディレクトリに登録（List in Directory）]	オン
	[タイムゾーン（Time Zone）]	[(GMT-08:00)アメリカ/ロサンゼルス（(GMT-8:00) America/Los_Angeles）]
	[言語（Language）]	[英語(アメリカ合衆国)（English(United States)）]
	[社内電子メールアドレスからSMTP プロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）]	オン
[パスワード設定- VM（Password Settings - VM）]	[次回サインイン時に、ユーザによる変更が必要（User Must Change at Next Sign-In）]	オン
	[期限切れなし（Does Not Expire）]	オン
	[認証規則（Authentication Rule）]	[ボイスメール認証規則(推奨)（Recommended Voice Mail Authentication Rule）]
[パスワードの変更-ボイスメール（Change Password-Voicemail）]	[PIN]	30071982

テンプレートに基づいて新規ユーザ設定を行うことで、個々のユーザ アカウントで変更する必要がある設定の数を最小限に抑えるとともにユーザ追加作業にかかる時間も短縮され、エラーが発生しにくくなります。

これ以降（テンプレートを使用してユーザ アカウントを作成した後）に行うすべてのユーザ テンプレート変更は、既存のユーザ アカウントには適用されません。つまり、共通設定はユーザ アカウント作成時点でのみテンプレートから取得されます。テンプレートを使用して Unity Connection アカウントを作成した後で、テンプレートまたは他のユーザに影響を及ぼさずに個々のユーザの設定を変更できます。

ここでは Web アプリケーション パスワードを変更しないでください。これは、Unity Connection は LDAP と統合されており、Active Directory からユーザが認証されるためです。これらの PIN とパスワードをユーザに指定する必要があります。これにより、ユーザは Unity Connection システム電話ユーザ インターフェイス（TUI）と Cisco Personal Communications Assistant（PCA）にサインインできます。

[ボイスメールユーザCOSサービスクラス（Voice Mail User COS class of Service）] 下の [Messaging Assistantの使用をユーザに許可する（Allow Users to Use the Messaging Assistant）] オプションと [Web InboxとRSSフィードの使用をユーザに許可する（Allow Users to Use the Web Inbox and RSS Feeds）] オプションを選択して、ユーザが Cisco PCA を使用して Web Inbox にアクセスできるようにします。

前述の説明で作成したテンプレートを使用して LDAP からユーザをインポートします。

Unity Connection ユーザ自己登録

エンドユーザを Unity Connection ユーザとして登録する必要があります。Unity Connection 管理者は各ユーザの ID（通常はユーザのデスク電話の内線番号）と一時 PIN（ユーザ プロビジョニングで設定）を指定する必要があります。初回登録ガイダンスは、あらかじめ録音された一連のプロンプトであり、ユーザはこのガイダンスに従って次のタスクを実行します。

- ユーザ名を録音します。
- ユーザが電話に応答しないときに外部発信者に対して再生されるグリーティングを録音します。
- ユーザ PIN を変更します。
- 電話帳に登録するかどうかを選択します（ユーザが電話帳に登録されていると、発信者はユーザの内線番号を知らない場合でも、ユーザの名前のスペルを言うか、ユーザ名を言うことでユーザに電話をかけられます。）

Unity Connection ユーザは組織内の IP エンドポイントまたは外部ネットワークから、自己登録プロセスのためにボイスメール パイロット番号をダイヤルできます。ユーザは、組織内または外部の不明な内線番号から Unity Connection に発信している場合、Unity Connection が自己登録プロセスを続行するよう応答したら、*（スターキー）を押す必要があります。登録が完了する前にユーザが通話を切断すると、次回ユーザが Unity Connection にサインインしたときに、初回登録ガイダンスが再び再生されます。

4. シングル インボックスの有効化

シングル インボックスは、Unity Connection のユニファイド メッセージング機能の 1 つであり、Unity Connection のボイス メッセージと Microsoft Exchange メールボックスを同期します。ユーザがシングル インボックスを使用可能な場合、ユーザに送信されるすべての Unity Connection ボイス メッセージ（Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージを含む）は、最初に Unity Connection に保存され、直ちにユーザの Exchange メールボックスにレプリケートされます。この項では、Unity Connection を Microsoft Exchange 2013 および 2010 と統合してシングル インボックスを有効にするために必要な設定タスクについて説明します。

Unity Connection でのシングル インボックス有効化の前提条件

- シングル インボックス機能を有効にする前に、Microsoft Exchange が設定されており、ユーザが電子メールを送受信できることを確認してください。
- Unified Messaging サービス アカウント認証には Microsoft Active Directory が必要です。
- Unity Connection ユーザがインポートされ、基本ボイス メッセージング用に設定されます。ユーザ プロビジョニングを参照してください。

Unity Connection 証明書管理

Cisco Unity Connection をインストールすると、Cisco PCA と Unity Connection 間の通信、および IMAP 電子メール クライアントと Unity Connection 間の通信を保護するため、ローカル自己署名証明書が自動的に作成およびインストールされます。つまり、Cisco PCA と Unity Connection 間でのすべてのネットワーク トラフィック（ユーザ名、パスワード、その他のテキスト データ、ボイス メッセージを含む）は自動的に暗号化され、IMAP クライアントで暗号化を有効化している場合には IMAP 電子メール クライアントと Unity Connection 間のネットワーク トラフィックは自動的に暗号化されます。

もう 1 つのオプションは、認証局（CA）が発行した証明書を使用するオプションです。この場合、自己署名証明書は信頼できる CA により発行、署名された証明書に置き換わります。このプロセスの詳細については、Cisco Unified CM and IM and Presence の証明書管理を参照してください。

Unity Connection の Exchange 認証および SSL 設定の確認

必要な Web ベースの認証モード（基本、ダイジェスト、NT LAN Manager）と Web ベースのプロトコル（HTTPS または HTTP）用に Exchange サーバが設定されていることを確認します。Exchange と Unity Connection が通信するためには、この両方の認証モードが一致している必要があります。

Exchange サーバと Active Directory ドメイン コントローラのための外部 CA により署名された証明書を検証するオプションを選択する場合は、外部 CA により署名された証明書を取得し、Exchange サーバとドメイン コントローラ サーバの両方にインストールします。

Unity Connection での SMTP プロキシ アドレスの設定

シングル ボックスを設定すると、Unity Connection は SMTP プロキシ アドレスを使用して、Unity Connection ViewMail for Microsoft Outlook から送信されたメッセージの送信者を適切な Unity Connection ユーザにマップし、受信者を Unity Connection ユーザにマップします。

たとえば、電子メール クライアントが電子メール アドレス aross@ent-pa.com を使用して Unity Connection にアクセスするように設定されているとします。このユーザが ViewMail for Outlook でボイス メッセージを録音し、そのメッセージをユーザ ahall@ent-pa.com に送信します。Unity Connection は SMTP プロキシ アドレスのリストで aross@ent-pa.com と ahall@ent-pa.com を検索します。これらのアドレスがそれぞれ Unity Connection ユーザである ahall および aross の SMTP プロキシ アドレスとして定義されている場合、Unity Connection はメッセージを Unity Connection ユーザ aross からのボイス メッセージとしてUnity Connection ユーザ ahall に送信します。

ユーザ テンプレートを使用してユーザをインポートする場合、ユーザの SMTP プロキシ アドレスが自動的に作成されます。ユーザ テンプレートでは、SMTP プロキシ アドレスを作成するために [社内電子メールアドレスからSMTPプロキシアドレスを生成（Generate SMTP Proxy Address from the Corporate Email Address）] オプションを選択します。詳細については、ユーザ プロビジョニングを参照してください。

Active Directory での Unified Messaging サービス アカウントの作成および Unity Connection の権限の付与

シングル インボックスを使用するには、Active Directory のアカウント（ユニファイド メッセージング サービス アカウント）が必要です。このアカウントには、Unity Connection がユーザの代わりに操作を実行するために必要な権限が付与されている必要があります。Unity Connection は ユニファイド メッセージング サービス アカウントを使用して Exchange メールボックスにアクセスします。ユニファイド メッセージング サービス アカウントを作成する際には、次のガイドラインに従ってください。

- アカウントには Exchange メールボックスを作成しません。
- 管理者グループにはアカウントを追加しません。
- アカウントを無効にしないでください。無効にすると、Unity Connection がアカウントを使用して Exchange メールボックスにアクセスできなくなります。

Exchange Management Shell がインストールされているサーバにサインインし、次のコマンドを使用して、[アプリケーション偽装管理（ApplicationImpersonation Management）] ロールを Unity Connection のユニファイド メッセージング サービス アカウントに割り当てます。

new-ManagementRoleAssignment -Name: *RoleName* **-Role:ApplicationImpersonation -User:'** *Account* **'**

ここで、

- *RoleName* は、割り当てるロールの名前です（Unity ConnectionUMServicesAcct など）。**get-ManagementRoleAssignment** コマンドを実行すると、RoleName に入力する名前が表示されます。
- *Account* は、domain\alias 形式のユニファイド メッセージング サービス アカウントの名前です。

SMTP スマート ホスト

Unity Connection は、SMTP スマート ホストを使用してメッセージをユーザの電子メール アドレスにリレーします。Unity Connection ユーザが新しいメッセージを受け取ると、Unity Connection がテキスト形式の到着通知を電子メール アドレスに送信できます このタイプの通知では、Cisco PCA へのリンクを電子メール メッセージの本文に組み込むように Unity Connection を設定できます。ユーザ設定で、ユーザの[通知デバイスの編集（Edit Notification Device）] ページに移動し、[メッセージテキストにCisco Unity Connection Web Inboxへのリンクを含める（Include a Link to the Cisco Unity Connection Web Inbox in Message Text）] オプションを選択します。表 5-15に、SMTP スマート ホストの設定を示します。

表 5-15　SMTP スマート ホストの詳細（[システム設定（System Settings）] > [SMTPの設定（SMTP Configuration）] > [スマートホスト（Smart Host）]）

パラメータ	値
[SmartHost]	US-EXCH1.ent-pa.com

ユニファイド メッセージング サービス

Cisco Unity Connection Administration で、[ユニファイド メッセージング（Unified Messaging）] を展開し、[ユニファイド メッセージング サービス（Unified Messaging Services）] を選択します。

- ユニファイド メッセージング サービスは、Unity Connection が Microsoft Exchange と通信するために使用する認証方式と Microsoft Exchange のタイプを定義します。
- FQDN を使用して特定の Exchange サーバと通信するようにユニファイド メッセージング サービスを設定します。
- Unity Connection ユニファイド メッセージング サービスで、Microsoft Exchange で設定されているものと同じ Web ベース認証モード（基本、ダイジェスト、または NT LAN Manager）および Web ベースのプロトコル（HTTPS または HTTP）を設定します。
- Active Directory での Unified Messaging サービス アカウントの作成および Unity Connection の権限の付与の項で作成した Active Directory アカウントのクレデンシャルを入力します。
- [Exchangeの予定表および連絡先にアクセス（Access Exchange Calendar and Contacts）] オプションと [ConnectionとExchangeのメールボックスを同期する(シングル インボックス)（Synchronize Connection and Exchange Mailboxes (Single Inbox)）] オプションを選択し、ユニファイド メッセージング機能を有効にします。
- 自己署名証明書は検証できません。Unity Connection サーバで Exchange からの SSL 証明書を検証するには、自己署名証明書の代わりに認証局（CA）の公開証明書を使用します。詳細については、Unity Connection 証明書管理を参照してください。

ユニファイド メッセージング アカウント

Unity Connection Administration で、[ユーザ（Users）] を展開し、次に [ユーザ（Users）] を選択します。[ユーザの基本設定の編集（Edit User Basics）] ページの [編集（Edit）] メニューで、[ユニファイド メッセージング アカウント（Unified Messaging Accounts）] を選択します。

- ユーザ アカウントを作成する際、Unity Connection はそのユーザのユニファイド メッセージング アカウントを自動的には作成しません。ユニファイド メッセージング アカウントは、1人のユーザまたは複数のユーザに対して作成できます。多数のユーザを対象にユニファイド メッセージング アカウントを作成するには、一括管理ツール（BAT）を使用します。
- ユニファイド メッセージングでは、各 Unity Connection ユーザの Exchange メール アドレスを入力する必要があります。[ユニファイド メッセージング アカウント（Unified Messaging Account）] ページで、[社内電子メールアドレスを使用:指定なし（Use Corporate Email Address: None Specified）] を選択します。これにより、Unity Connection は [ユーザの基本設定の編集（Edit User Basics）] ページで指定した社内電子メール アドレスを Exchange 電子メール アドレスとして使用します。
- Active Directory 統合では、Unified CM の [メールID（Mail ID）] フィールドが、Active Directory のメール フィールドと同期されます。これにより、LDAP メール フィールドが Unity Connection の [社内電子メールアドレス（Corporate Email Address）] フィールドに表示されます。

一括管理ツールを使用した複数ユーザのユニファイド メッセージング アカウントの作成の詳細については、『*User Moves, Adds, and Changes Guide for Cisco Unity Connection*』でユニファイド メッセージング アカウントの作成に関する情報を参照してください。

ボイスメールユーザのCOS

ユーザがシングル インボックスを使用できるようにするため、ボイスメール ユーザのサービス クラスを編集します（[サービスクラス（Class of Service）] -> [ボイスメールユーザのCOS（Voice Mail User COS）] ）。[ライセンス済み機能（Licensed Features）] で [IMAPクライアントやシングル インボックスを使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Access Voicemail Using an IMAP Client and/or Single Inbox）] オプションを選択します。また、[メッセージ本文へのアクセスをIMAPユーザに許可する（Allow IMAP Users to Access Message Bodies）] オプションも選択します。

ユーザ ワークステーションへの ViewMail for Outlook のインストール

Cisco ViewMail for Microsoft Outlook のビジュアル インターフェイスにより、ユーザは Outlook 内で各自の Unity Connection ボイス メッセージを送信、再生、管理できます。ViewMail for Outlook を Cisco の Web サイト（http://www.cisco.com）からダウンロードし、各ユーザ ワークステーションにインストールします。ViewMail のインストールが完了したら、ViewMail の設定または [オプション（Options）] タブを開き、Unity Connection サーバに電子メール アカウントを関連付けます。ユーザ情報と Unity Connection サーバの詳細情報を入力します。

他の電子メール クライアントを使用して Exchange の Unity Connection ボイス メッセージにアクセスする場合、または ViewMail for Outlook がインストールされていない場合は、次の点に注意してください。

- メール クライアントは、Unity Connection ボイス メッセージを .wav ファイルが添付された電子メールとして処理します。
- ユーザが Unity Connection ボイス メッセージに返信またはボイス メッセージを転送すると、ユーザが .wav ファイルを添付した場合でも、返答または転送は電子メールとして処理されます。メッセージ ルーティングは、Unity Connection ではなく Exchange によって処理されます。したがって、メッセージは受信者の Unity Connection メールボックスに送信されません。

5. ビジュアル ボイスメールの有効化

ビジュアル ボイスメールにより、Jabber クライアントのボイスメール タブから Unity Connection に直接アクセスできます。ユーザは Jabber からボイス メッセージのリストを確認し、メッセージを再生できます。また、ユーザはボイス メッセージの作成、返信、削除もできます。

Unity Connection の設定

- Unity Connection ユーザがインポートされ、基本ボイス メッセージング向けに設定されていることを確認します。ユーザ プロビジョニングの項を参照してください。
- Unity Connection の **Connection Jetty** サービスと **Connection REST Service** が稼働していることを確認します。これらのサービスはいずれもサービスのアクティブ化で [オプション サービス（Optional Services）] の下でアクティブ化されます。
- IMAP クライアントからボイスメールにアクセスできるように、[サービスクラス（Class of Service）] が有効になっていることを確認してください。ボイスメールユーザのCOSの項を参照してください。
- Unity Connection ボイスメール サービス クラス（CoS）を編集し、ユーザが Web インボックスを使用できるようにします。[機能（Features）] タブで [Unified Personal Communicatorを使用したボイスメールへのアクセスをユーザに許可する（Allow Users to Use Unified Client to Access Voicemail）] オプションを選択します。

- [API設定（API settings）]（[システム設定（System Settings）] > [詳細設定（Advanced）]）で、次のオプションを選択します。
  - [CUMIを介したセキュアメッセージ録音へのアクセスを許可する（Allow Access to Secure Message Recordings through CUMI）]
  - [CUMIを介してセキュアメッセージのメッセージヘッダー情報を表示する（Display Message Header Information of Secure Messages through CUMI）]
  - [CUMI経由のメッセージ添付ファイルを許可する（Allow Message Attachments through CUMI）]

Unified CMの設定

各 Unity Connection サーバ ノードに**ボイスメール** UC サービスを追加します。表 5-16に、ボイスメール UC サービスの設定を示します。

表 5-16　ボイスメール サービスの設定（[ユーザ管理（User Management）] > [ユーザ設定（User Settings）] > [UCサービス（UC Service）]）

パラメータ	値	コメント
[製品のタイプ（Product Type）]	Unity Connection	ボイスメール システムの製品名を入力します。
[名前（Name）]	us-cuc1	ボイスメール サービスの名前を入力します。パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を選択します。
[説明（Description）]	us-cuc1	パブリッシャ ボイスメール サービスとサブスクライバ ボイスメール サービスを区別できる表示名を入力します。
[ホスト名/IPアドレス（Host Name/IP address）]	us-cuc1.ent.pa.com	ボイスメール サービスのアドレスを IP アドレス形式または FQDN 形式で入力します。
[ポート（Port）]	443	ボイスメール サービスに接続するポートを入力します。
[プロトコル（Protocol）]	HTTPS	ボイス メッセージを安全にルーティングするためのプロトコルを選択します。

以前に作成した**ボイスメール** UC サービスを**標準**サービス プロファイル（[ユーザ管理（User Management）] –> [ユーザ設定（User Settings）] –> [サービスプロファイル（Service Profile）]）に適用します。Unity Connection パブリッシャ（us-cuc1.ent.pa.com）に対して作成したボイスメール UC サービスがプライマリ プロファイルに設定されており、Unity Connection サブスクライバ（us-cuc2.ent.pa.com）に対して作成したボイスメール UC サービスがセカンダリ プロファイルに設定されていることを確認してください。ボイスメール サービスのクレデンシャルを同期する場合は、[ボイスメールサービスのクレデンシャルソース（Credentials source for voicemail service）] ドロップダウン リストから [Unified CM - IM/Presence（Unified CM - IM and Presence）] を選択します。

6. SRST モードでのボイスメール

集中型メッセージング導入モデルでは、WAN の停止中にブランチ サイトの Survivable Remote Site Telephony（SRST）が無応答コールおよび話中コールを中央の Unity Connection にルーティングします。ビジー信号を受けた着信コール、無応答コール、およびメッセージ ボタンを押して開始されたコールは、Unity Connection に転送されます。この設定では、電話のメッセージ ボタンをアクティブなままにできます。この機能を有効にするには、PRI を介した Unity Connection への POTS ダイヤル ピア アクセスを設定します。

ただし、PSTN を介してコールがルーティングされる場合、Redirected Dialed Number Information Service（RDNIS）が損なわれることがあります。RDNIS 情報が誤っている場合、PSTN 経由でルーティングされるボイスメール コールに影響することがあります。RDNIS 情報が誤っている場合、通話はダイヤル先のユーザのボイスメール ボックスに到達せず、代わりに自動応答プロンプトを受信します。その場合、発信者に対し、到達先の内線番号を再入力するように要求されることがあります。この動作は主に、電話通信事業者がネットワークを介した RDNIS を保証できない場合の問題です。通信事業者が RDNIS の正常な送信を保証できない理由は数多くあります。通信事業者に問い合わせて、回線のエンドツーエンドで RDNIS の送信を保証しているかどうかを確認してください。

Unified CM の設定

表 5-17で説明する設定が、中央サイトの PSTN ゲートウェイへの SIP トランクの Unified CM 設定で有効になっていることを確認します。

表 5-17　SRST モードでのボイスメール向け PSTN ゲートウェイへの SIP トランクの設定

パラメータ	値	コメント
[コールルーティング情報 - インバウンドコール（Call Routing Information - Inbound Calls）]		
[Diversionヘッダー配信のリダイレクト - インバウンド（Redirecting Diversion Header Delivery - Inbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が着信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。
[コールルーティング情報 - アウトバウンドコール（Call Routing Information - Outbound Calls）]		
[Diversionヘッダー配信のリダイレクト - アウトバウンド（Redirecting Diversion Header Delivery - Outbound）]	オン	リダイレクト情報要素、最初のリダイレクト番号、およびコール転送理由が発信メッセージの一部として送信され、受け入れられることを指定します。Unity Connection は最初のリダイレクト番号を使用してコールに応答します。

ブランチ SRST ルータの設定

ブランチ サイトの SRST ルータで、PRI を介したボイスメール アクセスを有効にするため次のコマンドを設定します。

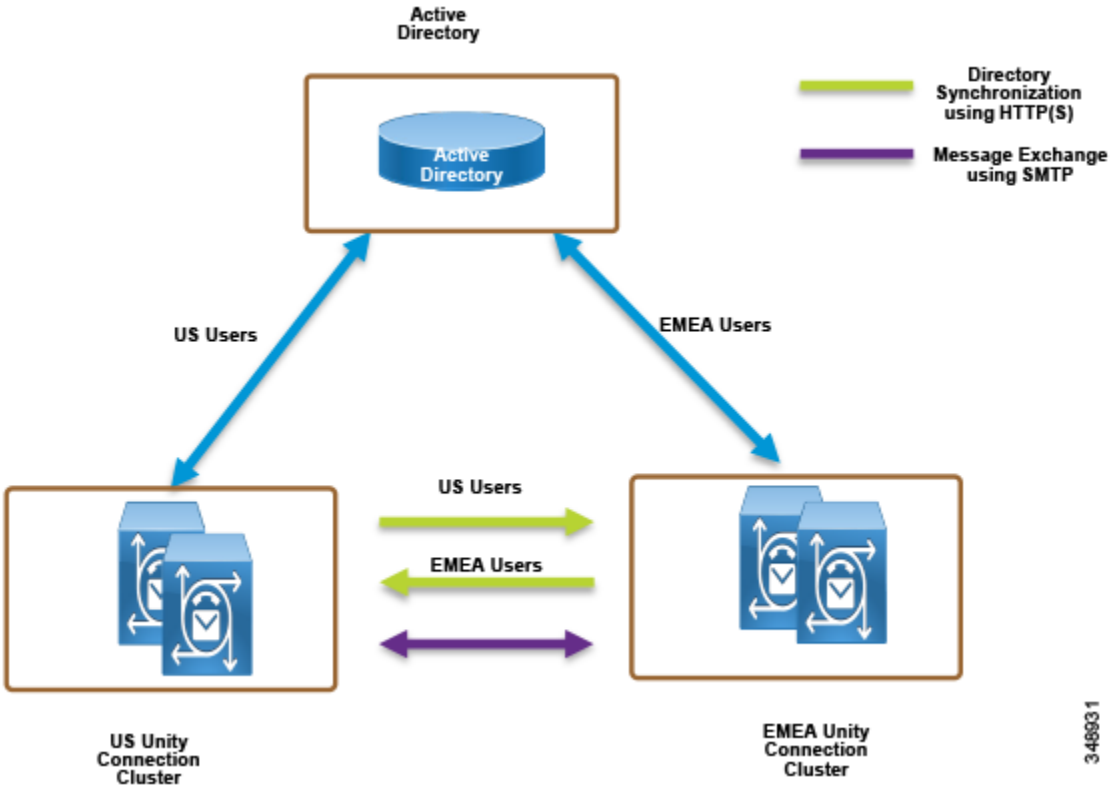
```
!
!
dial-peer voice 10 pots
destination-pattern +14085554999
direct-inward-dial
port 1/0:15
!
!
voice register pool 1
call-forward b2bua busy +14085554999
call-forward b2bua noan +14085554999 timeout 12
!
!
```

7. 2 つの Unity Connection クラスタの HTTPS インターネットワーキング

図 5-4に、2 つの Unity Connection クラスタの HTTPS インターネットワーキングを示します。HTTPS ネットワーキングにより複数の Unity Connection クラスタが接続されます。これにより、接続されたこれらのクラスタ間でディレクトリ情報を共有し、ボイス メッセージを交換できます。複数の Unity Connection サーバまたはクラスタを接続して、Unity Connection サイトと呼ばれる適切に接続されたネットワークを形成できます。サイトに接続するサーバは、*ロケーション*と呼ばれます。サイト内の各ロケーション間のディレクトリ情報の交換には HTTPS プロトコルが使用され、ボイス メッセージの交換には SMTP プロトコルが使用されます。

サイト内の Unity Connection ロケーションはディレクトリ情報を自動的に交換するため、受信側/送信先ユーザが発信側/送信元ユーザの検索範囲内で到達できる場合は、あるロケーションの受信側/送信先ユーザが別のシステムの発信側/送信元ユーザに対し、名前または内線番号を使用して発信するか、またはメッセージを送信できます。ネットワーク接続されたシステムは、1 つのディレクトリを共有しているかのように機能します。

図 5-4　　2 つの Unity Connection クラスタの HTTPS インターネットワーキング



HTTPS ネットワーキングでは、ハブアンドスポーク トポロジを使用して Unity Connection クラスタが相互に接続します。このトポロジでは、スポーク間のすべてのディレクトリ情報が、スポークに接続するハブを介して共有されます。HTTPS ネットワークで接続できる Unity Connection ロケーションの数と、HTTPS ネットワーキングの最大ユーザ数は、導入されている OVA テンプレートに応じて異なります。サポートされるロケーションの最大数とディレクトリの最大サイズの詳細については、『*System Requirements for Cisco Unity Connection*』で*ディレクトリ オブジェクト制限*に関する情報を参照してください。

HTTPS ネットワーキングでは、ネットワーク内の各ロケーションで稼働しているリーダー サービスとフィーダー サービスによって、ディレクトリ レプリケーションが行われます。リーダー サービスは、リモート ロケーションを定期的にポーリングして、前回のポーリング間隔以降に行われたディレクトリ変更情報を収集します。フィーダー サービスは、変更トラッキング データベースを調べてディレクトリ変更が行われたかどうかを確認し、必要な情報を使用してポーリング要求に応答します。

HTTPS ネットワーキングでは、クラスタ ロケーションのパブリッシャ サーバが稼働している場合、このサーバがディレクトリ情報の同期化を行います。ただしパブリッシャ サーバがダウンしている場合は、サブスクライバ サーバがディレクトリ情報を同期します。

ディレクトリ同期が実行されるクラスタのサーバ（パブリッシャまたはサブスクライバ）に応じて、ディレクトリ同期は次のいずれかのタイプになります。

- [標準（Standard）]：ディレクトリ同期が、パブリッシャ サーバにより接続ロケーションとの間で実行されることを示します。
- [アラート（Alert）]：パブリッシャ サーバに接続できず、サブスクライバ サーバが接続ロケーションにディレクトリ情報を提供することを示します。ただし、サブスクライバ サーバに格納されているディレクトリ情報は、パブリッシャ サーバの稼働時にパブリッシャ サーバとの間で最後に同期されたディレクトリ情報です。

パブリッシャで障害が発生すると、ディレクトリ同期はアラート モードで実行されます。アラート モードでは、HTTPS ネットワーク上の接続ノードに対し、サブスクライバとのディレクトリ同期へのアクセスが制限されます。制限付きアクセスとは、接続ノードが、パブリッシャの稼働時にパブリッシャとの間で最後に同期されたディレクトリ情報のみを取得できることを意味します。パブリッシャが復旧すると、パブリッシャに直接接続しているノードはパブリッシャを介して最新のディレクトリ情報を同期します。したがって、アラート モードの主要なメリットとしては、パブリッシャがダウンした場合でも接続ノードが引き続きサブスクライバ サーバと同期する点が挙げられます。

ネットワーク接続されているクラスタには、TCP/IP ポート 25（SMTP）を介して直接アクセスできます。また、両方のロケーションは、HTTP を介してポート 8081 で、または HTTPS を介してポート 8444 で互いにルーティングできる必要があります。

導入の解説という目的から、本書では US および EMEA Unity Connection クラスタ間に HTTPS ネットワークが存在することを前提としています。表 5-18 に、HTTPS ネットワークにより接続されるこの 2 つのクラスタのサーバ ノード情報を示します。

表 5-18　HTTPS ネットワークでの Unity Connection クラスタの詳細

	US Unity Connection クラスタ		EMEA Unity Connection クラスタ	
サーバ	**ホストネーム**	**IP アドレス**	**ホストネーム**	**IP アドレス**
パブリッシャ	US-CUC1	10.195.100.30	EMEA-CUC1	10.195.99.30
サブスクライバ	US-CUC2	10.195.100.31	EMEA-CUC2	10.195.99.31

2 つの Unity Connection クラスタ間で HTTPS ネットワークをセットアップするには、この項で説明する次のタスクを実行します。

各 Unity Connection サーバの表示名および SMTP ドメインの確認

- HTTPS ネットワークに接続する Unity Connection サーバには、一意の表示名と SMTP ドメインが設定されている必要があります。
- HTTPS ネットワークを有効にする前に、[ネットワーク（Networking）] –> [ロケーション（Locations）] の設定で、Unity Connection パブリッシャ サーバの表示名と SMTP ドメインを確認します。

Unity Connection クラスタ間の HTTPS ネットワークの作成

- Unity Connection サーバの HTTPS ネットワークを作成するには、最初に HTTPS リンクを作成して 2 つのクラスタをリンクし、その後各クラスタのサブスクライバが SMTP アクセスのために追加されていることを確認します。
- 各 Unity Connection パブリッシャで、新しい HTTPS リンクを追加します。表 5-19に、HTTPS リンクの設定を示します。

表 5-19　HTTPS リンクの設定（[ネットワーク（Networking）] > [HTTP(S) リンク（HTTP(s) Links）]）

パラメータ	値	コメント
[Cisco Unity Connectionのリモート ロケーションへのリンク（Link to Cisco Unity Connection Remote Location）]		
[パブリッシャ（IPアドレス/FQDN/ホスト名）（Publisher (IP address/FQDN/Hostname)）]	emea-cuc1.ent-pa.com	リモート Unity Connection パブリッシャ ノードの IP アドレス、完全修飾ドメイン名（FQDN）、またはホスト名を入力します。
[ユーザ名（Username）]	管理ユーザの名前	上記のパブリッシャ フィールドに指定したロケーションの管理者のユーザ名を入力します。管理者のユーザ アカウントには、システム管理者ロールを割り当てておく必要があります。
[パスワード（Password）]	管理ユーザのパスワード	[ユーザ名（Username）] フィールドに指定された管理者のパスワードを入力します。
[転送プロトコル（Transfer Protocol）]		
[Secure Sockets Layer(SSL)を使用する（Use Secure Sockets Layer (SSL)）]	オン	このオプションは、さまざまな HTTPS ロケーション間のディレクトリ同期トラフィックを SSL により暗号化できるようにします。
[自己署名の証明書を受け入れる（Accept Self-Signed Certificates）]	このチェックボックスは、自己署名の証明書を使用する場合にのみオンにします。	ネットワーク上のローカル ノードが自己署名の証明書を使用してこのロケーションと SSL をネゴシエートできるようにするには、このチェックボックスをオンにします。ネットワーク上のローカル ノードが認証局（CA）により署名された証明書を使用する場合は、このチェックボックスをオフにします。

クラスタ サブスクライバ サーバの SMTP アクセスの設定

Unity Connection クラスタ サーバ ペアを含む HTTPS ネットワークでは、ペアのパブリッシャ サーバだけをネットワークに接続できます。クラスタのサブスクライバがプライマリ サーバである場合に、ネットワーク上のすべてのロケーションがクラスタ サブスクライバ サーバ ノードと直接通信できるようにするには、すべてのネットワーク ロケーションで、サブスクライバ サーバからの SMTP 接続を許可するように設定する必要があります。

この例では、EMEA サブスクライバを US パブリッシャの SMTP 設定に追加し、US サブスクライバを EMEA パブリッシャの SMTP 設定に追加します。

- US パブリッシャの US クラスタで、EMEA サブスクライバを SMTP 設定（[システム設定（System Settings）]）に追加します。[編集（Edit）] メニューで [IPアドレスアクセスリストの検索（Search IP Address Access List）] を選択します。[IPアドレスの新規作成（New IP Address）] ページで、EMEA サブスクライバ サーバの IP アドレス（この例では 10.195.99.31）を入力します。[接続を許可する（Allow Connection）] オプションが選択されていることを確認します。
- EMEA クラスタのパブリッシャ（emea-cuc1.ent-pa.com）で上記の手順を繰り返し、US クラスタ サブスクライバの IP アドレスを追加します。

ロケーション間でのレプリケーション

HTTPS ネットワークの作成後に、ネットワークに追加された 2 つのロケーション間でデータベース全体がレプリケートされることを確認します。初回のレプリケーションが開始されると、データが全ロケーション間で完全にレプリケートされるまでには、ディレクトリのサイズによって数分間から数時間かかることがあります。

前述のステップで作成した **HTTP（S）リンク**を開き、次の値を確認します。

- [前回の同期時刻（Time of Last Synchronization）]

  ローカルのリーダー サービスが前回、リモート ロケーションのフィーダー サービスにポーリングしてリモート ロケーションのディレクトリ変更の確認を試みた時刻（応答の有無にかかわらず）のタイムスタンプを示します。

- [前回のエラー時刻（Time of Last Failure）]

  ローカルのリーダー サービスが前回リモート ロケーションのフィーダー サービスのポーリングを試行中にエラーが発生した時点のタイムスタンプを示します。このフィールドの値が 0 の場合、または [前回の同期時刻（Time of Last Synchronization）] の値が [前回のエラーの時刻（Time of Last Error）] の値よりも遅い場合、レプリケーションは問題なく進行している可能性が高くなります。

- [オブジェクト数（Object Count）]

  ローカル Unity Connection ロケーションが同期したリモート ロケーションのユーザの数を示します。

ローカル Unity Connection CSS へのリモート ロケーション パーティションの追加

ロケーション間のネットワークを初めてセットアップする場合、US クラスタでプロビジョニングされたユーザは、EMEA クラスタのユーザにボイス メッセージを送信できません。これは、各ロケーションのユーザは個別のパーティションに属しており、個々のユーザ検索スペースには他のロケーションのユーザのパーティションが含まれていないためです。

- US Unity Connection サーバの us-cuc1 コーリング サーチ スペース（CSS）を編集して、EMEA ロケーションの Unity Connection サーバ パーティション emea-cuc1 を追加します。
- EMEA Unity Connection サーバの emea-cuc1 コーリング サーチ スペース（CSS）を編集して、US ロケーションの Unity Connection サーバ パーティション us-cuc1 を追加します。

関連資料

- 『*Cisco Collaboration System SRND*』の「*Voice Messaging*」の章
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab10/collab10/vmessage.html
- 『*Design Guide for Cisco Unity Connection*』
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/design/guide/10xcucdgx.html
- 『*HTTPS Networking Guide for Cisco Unity Connection*』
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/https_networking/guide/10xcuchttpsnetx.html
- 『*Unified Messaging Guide for Cisco Unity Connection*』
  http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/unified_messaging/guide/10xcucumgx.html

Cisco TelePresence Management Suite（TMS）による会議スケジュール

この項では、TelePresence およびホスト型 Web 会議を使用してコラボレーション会議をスケジュールする機能について説明します。ユーザ向けの Collaboration Meeting Room（CMR）機能の他に、ユーザは既存の予定表ツール（Microsoft Outlook クライアントなど）を使用してルームを予約し、コラボレーション セッションに容易にエンドユーザ接続できます。この機能は、コラボレーションの必要性が事前に判明しており、組織内の特定の会議ロケーション（会議室）に TelePresence エンドポイントが装備されている場合に便利です。この場合、1 つのアプリケーション ワークフローで、会議主催者は参加者およびロケーションを予約し、会議用に設定されたテクノロジーを使用できる状態にしておくことができます。

前提条件

スケジューリング アーキテクチャを導入する前に、次の点を確認してください。

- 本書のコール制御と会議の章を読み、その内容を実装している。
- コール制御のためにルームのエンドポイントが Unified CM に登録されており、ポイントツーポイント コールが機能している。
- スケジューリング ソリューションのサイジングとライセンスについて理解している。

コア コンポーネント

コア アーキテクチャを構成する主要製品を次に示します。

- Cisco TelePresence Conductor
- Cisco TelePresence Server
- Cisco TelePresence Management Suite（TMS）：会議のプロビジョニング、監視、スケジュール
- Cisco TelePresence Suite Provisioning Extensions（TMSPE）：CMR の設定（会議の章を参照）
- Cisco TelePresence Management Suite Extension for Microsoft Exchange（TMSXE）：Microsoft Exchange のルーム/リソース カレンダーとのインターフェイス
- Cisco WebEx Software as a Service（SaaS）

このアーキテクチャには、次のシスコ製品以外のコンポーネントも含まれています。

- Microsoft SQL データベース
- Microsoft Active Directory
- Microsoft Exchange or Microsoft Office 365
- ネットワーク ロード バランサ

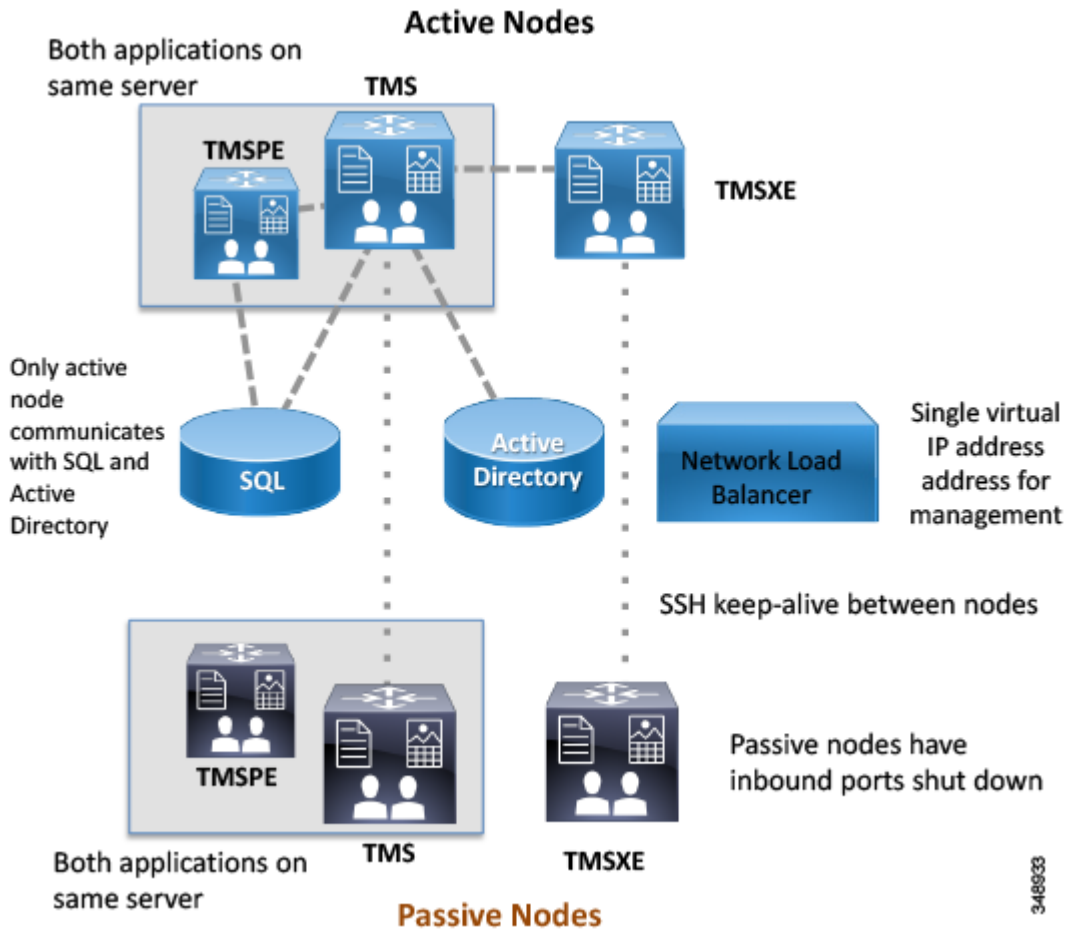
主な利点

- 参加者とロケーションをスケジュールする場合と同じツールを使用してテクノロジーをスケジュール
- 会議開始時にエンドユーザ操作なしで Web 会議参加者を統合
- スケジュールされている会議リソースとプロセスの高い可用性
- ビデオ ネットワークの復元性によりコンポーネントを保守のためにオフラインにすることが可能

コア アーキテクチャ

スケジューリング アーキテクチャは、Cisco TMS および TMSXE 両方のアクティブ ノードとパッシブ ノードで構成されています。これらは、ネットワーク ロード バランサの後ろに導入されています。一部の導入環境では、Cisco TMS、TMSPE、および TMSXE を同じ仮想マシンにインストールできますが、大規模な導入環境では TMSXE を個別の仮想マシンにインストールする必要があります（図 5-5を参照）。（サイジングの詳細については、サイジングの章を参照）。TMS サーバは顧客データセンターにインストールされます。このデータセンターは、組織の SQL 導入環境もホストします。すべてのサーバ ノードは、1 つの外部 Microsoft SQL データベースから機能します。また、会議を適切にスケジュールするには、エンドポイント、TelePresence Conductor、TelePresence サーバ、および Unified CM が使用されます。（図 5-5を参照）。

図 5-5　　アーキテクチャの概要



Cisco TMS の役割

Cisco TMS は、スケジュールされている会議で一貫したエンドユーザ エクスペリエンスを提供できるように、会議室のエンドポイント、TelePresence Conductor、および WebEx クラウド接続を統合します。Unified CM はエンドポイントの設定管理を維持し、TMS はカレンダーをこれらのエンドポイントにプッシュできます。管理者は、組織のデフォルト会議のパラメータを設定できます。パラメータの設定後に、このテンプレートに基づいて個々の会議が作成されます。

TMS 機能の一部（電話帳、ソフトウェア管理、レポート機能など）はプリファード アーキテクチャでは使用されません。

CMR と TMS Provisioning Extensions（TMSPE）の詳細については、会議の章を参照してください。CMR は、特定のエンドポイントが指定されていない、未スケジュールの会議に使用され、ユーザは CMR 番号にダイヤルインします。

Cisco TMS Extensions for Microsoft Exchange の役割

エンドユーザが複数の会議室リソースを使用する会議を Microsoft Outlook でスケジュールすると、Exchange の Exchange Web Service（EWS）機能により、そのイベントが TMS にスケジュール済み会議として同期されます。この同期は双方向であるため、管理者またはサポート担当員が、会議主催者の Outlook イベントにアクセスせずに、会議を更新できます。組織内で会議に使用する予定のすべてのエンドポイント リソースが、1 つの Exchange 会議要求にリストされている必要があります。

スケジュール済み会議の会議ブリッジ

Unified CM に直接接続している会議リソースの割り当てのために、スケジュール済みの会議（Cisco WebEx ユーザが参加する CMR Hybrid 会議を含む）が TelePresence Conductor と連携します。TelePresence Conductor がクラスタ化されている場合、Cisco TMS は TelePresence Conductor クラスタ ノードのうち 1 つのノードだけを認識するため、スケジュール済み会議のために Cisco TMS に 1 つの TelePresence Conductor ノードだけを追加します。スケジュール済み会議の詳細については、会議の章を参照してください。

復元性

Cisco TMS の導入環境には、TMS Provisioning Extension（TMSPE）アプリケーションもホストする 2 つの TMS フロントエンド サーバ、TMSXE を実行する 2 つのサーバ、ネットワーク ロード バランサ、および 1 つの外部 Microsoft SQL データベースが含まれています。

TMS 復元性では、2 つのサーバ（1 つのアクティブ ノードと 1 つの パッシブ ノード）だけがサポートされており、またこのモデルでは、TMS 導入環境のキャパシティを増減することはできません。ただし、Cisco TMS が認識できる TelePresence Conductor クラスタ ノードは 1 つだけであり、そのクラスタ ノードで障害が発生した場合には、そのノードが復旧するか、Cisco TMS が更新されクラスタ内の別の TelePresence Conductor ノードと通信できるようになるまでは、Cisco TMS スケジューリング機能が使用できなくなります。

Cisco TMS 導入プロセス

導入環境の概要

この項では、エンタープライズ コラボレーション プリファード アーキテクチャに Cisco TelePresence Management Suite（TMS）を導入するために必要な設定タスクの概要を説明します。スケジュール済みアプリケーションの冗長構成で Cisco TMS を導入するには、次のタスクを記載されている順序で実行します。

1. 計画
2. アクティブ ノードとパッシブ ノードでの TelePresence Management Suite（TMS）のインストールと設定
3. ネットワーク ロード バランサ（NLB）のインストールと設定
4. アクティブ ノード サーバとパッシブ ノード サーバ間でのファイル共有の設定
5. 追加の TMS 設定
    a. ISDN および IP ゾーン
    b. Active Directory の統合、グループ構造、ユーザ
    c. システム ナビゲータ フォルダの構造
    d. WebEx 接続
    e. デフォルトの会議設定
6. TMS への管理対象デバイスの追加
    a. TelePresence Conductor のインストールとスケジュールのための設定
    b. TMS への Unified CM の追加
    c. TMS への会議室エンドポイントの追加
7. TMS Extension for Microsoft Exchange のインストールと設定

1. 計画

インストールと設定のプロセスを開始する前に、組織固有の構造と設定に合わせて各種アイテムを決定する必要があります。また、一部の設定は設定プロセス中に使用する必要があるため、インストール プロセス開始前にこれらの情報を収集しておく必要があります。

Microsoft SQL

Cisco TMS は、会議、ユーザ、システムに関するすべてのデータを外部 Microsoft SQL データベースを使用して保存します。インストール プロセスでは、TMS と関連ソフトウェア拡張機能によって特定のデータベースがいくつか作成されます。TMS アプリケーションでは、tmsng データベースとの通信がアクティブでない場合には、ユーザは Web ページにログインできません。このように SQL データベースとの継続的な通信に依存しているため、SQL データベースでは、Microsoft によるデータベースの復元性を実現する手法も使用する必要があります。データベースのサイズは、導入の規模とスケジューリング イベントの数に応じて異なりますが、一般的な指針として、ほとんどの組織では初期ストレージとして 1 GB あれば十分です。

表 5-20に、Cisco TMS、TMSXE、および TMSPE をサポートするための Microsoft SQL 2012 の要件を示します。

表 5-20　Cisco TMS、TMSXE、および　TMSPE をサポートするための Microsoft SQL 2012 の要件

要件	パラメータ
TMS が使用するアカウントの SQL ユーザ アカウント権限	**dbcreator** ロールと **security admin** ロール
認証	SQL Server および Windows 認証（混合モード）
デフォルト言語	英語
タイム ゾーン	TMS サーバのタイム ゾーンに一致している必要があります
作成されるデータベース	tmsng（CiscoTMS） tmspe（CiscoTMSPEmain） mspe_vmr（Cisco TMSPE Collaboration Meeting Room） tmspe_userportal（Cisco TMSPE セルフサービス ポータル）
復元性モデル	Windows Server フェールオーバー クラスタ（WSFC）による **AlwaysOn フェールオーバー クラスタ** インスタンス

（注）　その他の SQL 復元性モードが TMS でサポートされていますが、**AlwaysOn フェールオーバー クラスタ**以外の方法では、SQL の停止中に TMS 管理者が手動で調整を行う必要があります。

Active Directory

Cisco TMS は、Microsoft Active Directory のさまざまな機能を使用して動作するため、サーバを組織のドメインに追加する必要があります。すべての TMS ユーザは Active Directory からインポートされ、Active Directory に対して認証されます。

設定プロセスでは、TMS がユーザをインポートできるようにするため、**AD サービス アカウントのユーザ名とパスワード**を入力する必要があります。これは読み取り専用アカウントであり、TMS が Active Directory の情報を変更することはありません。このアカウントには、AD 構造の最上位レベルへのアクセス権限が必要です。このアクセス権限により、後続のすべてのエンドユーザがその機能にアクセスできるようになります。複数ドメインを使用する組織では、TMS ユーザ アカウントに最上位ドメインを関連付ける必要があります。エンドユーザが Exchange リソースを予約できるようにするため、TMSXE アプリケーションには追加のサービス アカウントが必要です。これも読み取り専用サービス アカウントである必要があります。また、実際のイベント予約にはエンドユーザのクレデンシャルが使用されます。TMSXE ユーザ アカウントでは、TMSXE アプリケーションだけが Exchange Web Service を介して Exchange Server で認証および Exchange Server と通信できます。

また、AD で、TMS のスケジュール機能へのアクセス権限を持つエンドユーザと TMS 管理者の同期に使用する既存のグループを指定するか、または新規のグループを作成します。

（注）　TMS サーバのローカル マシン アカウントは、フロントエンド サーバ間で複製されないため、使用しないでください。また他のノードがアクティブになるとユーザ クレデンシャルが使用できなくなります。

電子メールの統合

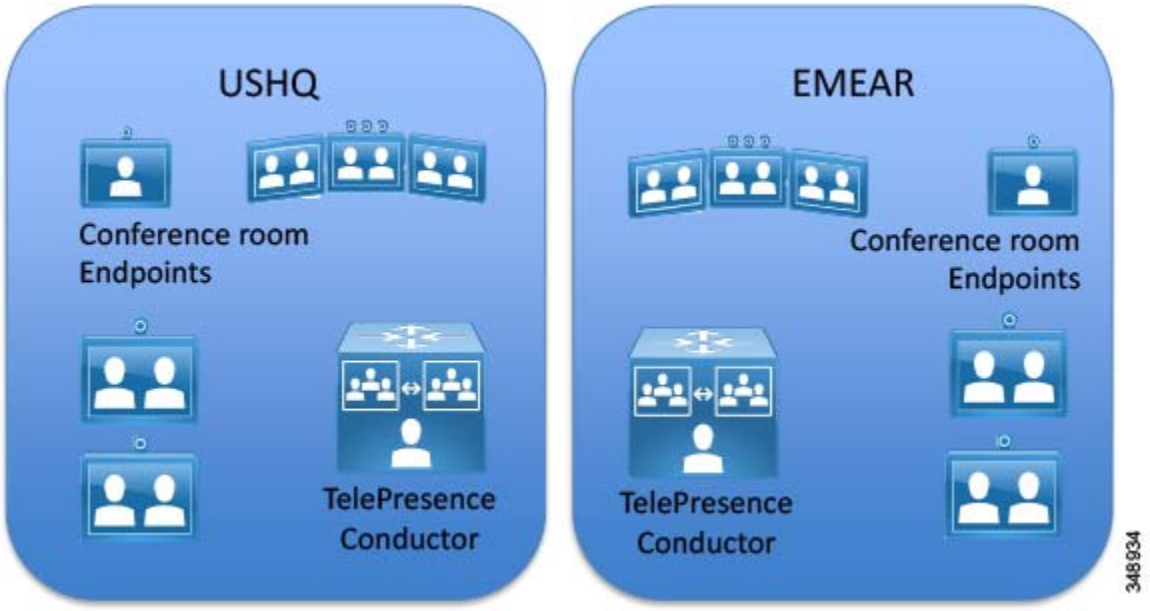
ユーザが会議をスケジュールすると、TMS は参加者のすべての接続情報を記載した自動メールをユーザに送信します。インストール プロセスで、この自動メールの送信元としてエンドユーザに対して表示される「from」アドレスを入力する必要があります。このため、collabconferencing@ent-pa.com のようなアドレス、または現在組織内で使用していない類似アドレスを選択します。

また、送信メール サーバの SMTP アドレスも入力する必要があります。

ゾーン

Cisco TMS はゾーンという概念を使用して、スケジューリング エンジンに対しコールの作成方法を指示し、トラフィックを可能な限りローカライズした状態で維持します。エンドポイント、会議リソース、および ISDN ゲートウェイはすべてゾーンに割り当てられます。ゾーンは、どのようなネットワーク接続をどこで使用するかを定義します。プリファード アーキテクチャは、すべてのエンドポイントが接続に 1 つの IP ネットワークを使用できることに基づいており、ISDN は組織外部に接続する場合にのみ使用されます。（図 5-6を参照）。

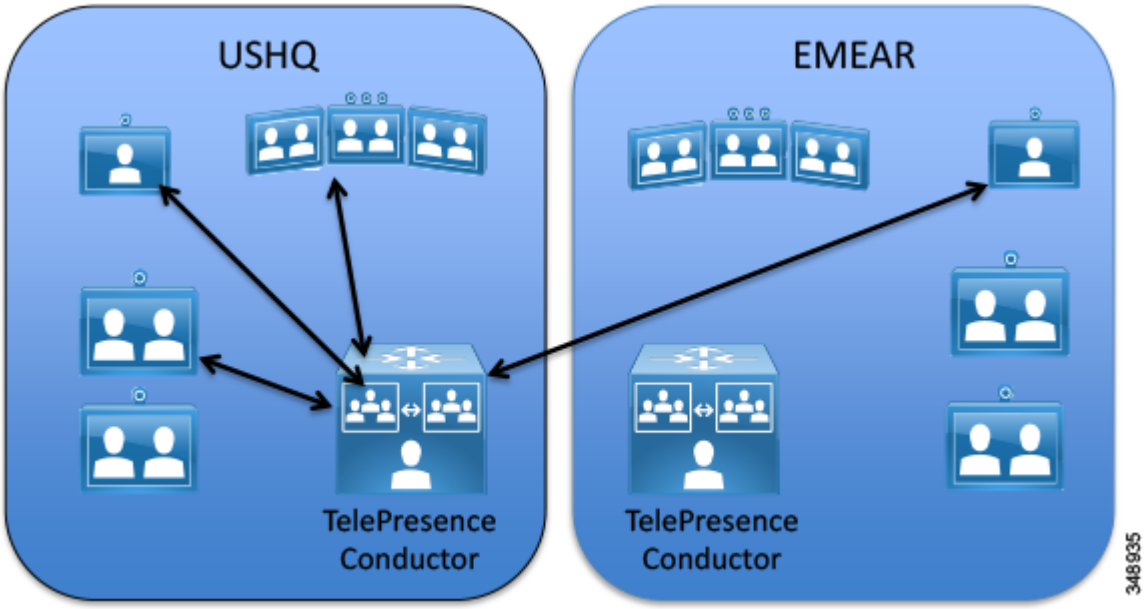
図 5-6　　Cisco TMS IP ゾーン



IP ゾーン

IP ゾーンは、共通するプライマリ データセンターを共有するネットワーク領域を指しており、主に「ローカル」の会議リソースを識別するために使用されます。設定プロセスでは、会議リソースが配置されるロケーションごとに IP ゾーンを追加する必要があります。（図 5-7を参照）。

図 5-7　　Cisco TMS による IP ゾーンを使用した会議用に最適な TelePresence サーバの選択



ISDN ゾーン

ISDN ゾーンは IP ゾーンと似ていますが、組織内に導入されている ISDN ゲートウェイ固有のゾーンです。ISDN 機能が不要な場合でも、インストール時にエンタープライズ全体に対して 1 つの ISDN ゾーンを設定する必要があります。

エンドポイントの命名規則

エンドポイントが Cisco TMS に追加される理由として、次の 2 つの理由があります。

- 会議リソースの割り当てのために Exchange リソースを関連付ける
- TMS がワンボタン機能の接続情報をエンドポイント ユーザ インターフェイスに提供できるようにする

TMS にエンドポイントが追加されると、Exchange でルーム名またはリソース名として同じ文字列が使用されます。これにより、エンドユーザに対して、コール履歴にシステム名が表示されるときに統一がとられます。また、画面上のラベルのテキストが会議リソースから取り込まれます。

TMS Systems Navigator のフォルダ構造の使用法について系統立った計画を立てることで、管理者が簡素化されたインターフェイスを使用できるようになります。

組織のデフォルト会議パラメータ

これは組織別にカスタマイズ可能な設定であり、各自のネットワークに関する考慮事項、会議の流れ、企業風土に基づいて使用する必要があります。デフォルトの会議設定は、エンドユーザが Outlook でスケジュールするすべての会議に使用されます。デフォルトの会議に対して設定可能なすべての設定については、『*Cisco TelePresence Management Suite Administrator Guide*』

（http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html より入手可能）を参照してください。

CMR Hybrid 向け WebEx サイト

WebEx サイトのホスト名とサイト名が分かっていることを確認してください。オンプレミス TelePresence 会議インフラストラクチャと WebEx クラウドを統合するため、この WebEx サイトを設定します。

CMR のプロビジョニング

会議の章で説明されているように、組織による Collaboration Meeting Room の使用計画を理解しておくことは、エンドユーザが会議に対して期待するワークフローを理解する基盤となります。一部の組織は特定のタイプの会議にスケジュールされたリソースではなく、アドホック CMR を利用することがあります。特に、ほとんどの従業員がそれぞれ離れた場所にいて、ローカル会議室に集合することがほとんどない場合に利用されます。

サーバのロケーション

冗長 TMS 導入環境のアクティブ ノードとパッシブ ノードの両方に対し、サーバ オペレーティング システムで同一タイム ゾーンを設定する必要があります。また、これは SQL サーバと同じタイム ゾーンである必要もあります。冗長 TMS のサポートは、アクティブ ノードとパッシブ ノードの両方と SQL サーバが同じローカル ネットワーク上に存在する場合に限定されています。

2. アクティブ ノードとパッシブ ノードでの TelePresence Management Suite（TMS）のインストールと設定

冗長環境を実現するには、『*Cisco TelePresence Management Suite Installation and Upgrade Guide*』

（http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html から入手可能）のガイドラインに従って、Cisco TelePresence Management Suite（TMS）をインストールする必要があります。

- プライマリ サーバにこのアプリケーションをインストールします。
- 計画段階で設定した外部 SQL リソースを指し示します。
- 暗号化キーをメモしておきます。
- Web ポータルにログインして TMS 冗長性を有効にし、基本的な操作を検証します。
- 1 番目のサーバの暗号化キーを使用し、1 番目のサーバと同じ SQL クレデンシャルを使用して、2 番目のサーバにアプリケーションをインストールします。

両方のサーバが、すべての会議データと設定データが保存されている 1 つの SQL データベースにアクセスします。アクティブ ノード設定とパッシブ ノード設定で、1 つの暗号化キーと証明書が両方のサーバに対して使用されます。この暗号化キーと証明書をそれぞれのサーバに配置しておくと、エンドユーザから TMS への通信と、TMS から管理対象デバイスへの通信に、セキュアプロトコルを使用できるようになります。

3. ネットワーク ロード バランサ（NLB）のインストールと設定

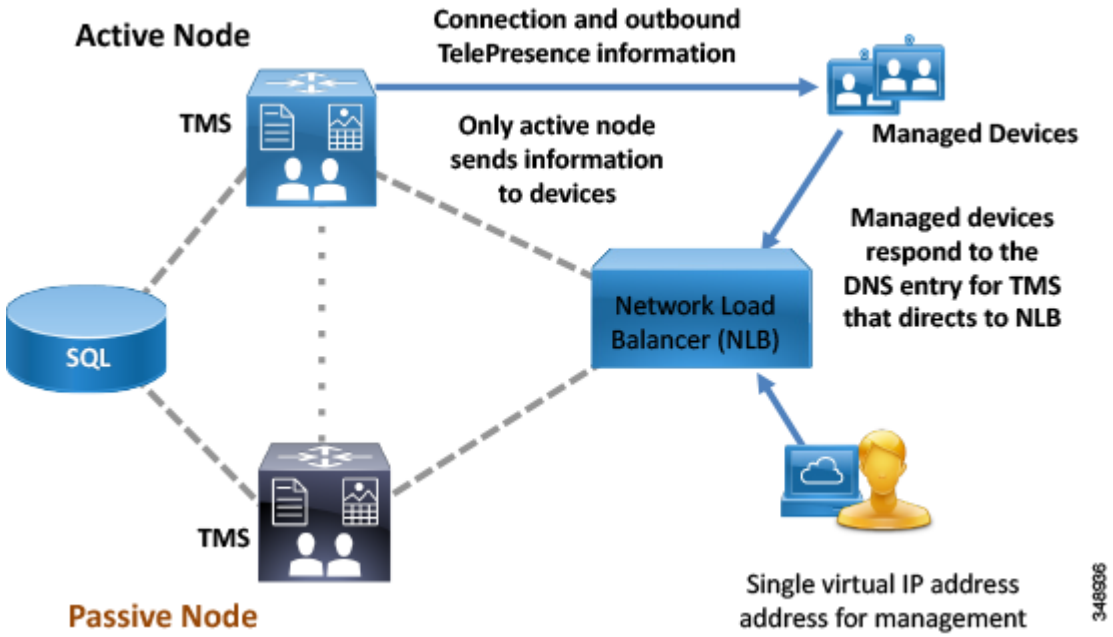
ネットワーク ロード負荷分散設定の詳細は、お客様が選ぶロード バランサの指示に応じて異なります。以下は、設定する必要がある機能要件です。

- HTTP、HTTPS、および SNMP トラフィックをアクティブ ノードに転送します。
- Cisco TMS 内で Probe URL へのネットワーク ロード バランサ プローブを設定します。
- すべてのトラフィックをアクティブ ノードにプッシュします。

Cisco TMS サーバは発信通信を管理対象デバイスに直接送信し、トラフィックを NLB 経由でルーティングしません。ただし、管理対象デバイスからのすべての戻り通信とすべての Web ポータル要求は、NLB 経由でルーティングされる必要があります。通信パスにより、エンドユーザとエンドポイントは、どの TMS サーバ ノードがアクティブ モードであるかに関係なく、1 つのアドレスを使用できます。

TMS ネットワーク設定を、ネットワーク ロード バランサで設定されている TMS アドレスの FQDN に設定します。TMS 内のこの設定が、管理対象デバイスが TMS との通信を開始するときに使用するアドレスに取り込まれます。ロード バランサに解決される tms.company.com の FQDN を使用することで、エンドポイントまたはエンドユーザ Web クライアントからのすべての着信トラフィックは NLB を経由して送信され、アクティブ ノードに解決されます。（図 5-8を参照）。

図 5-8　　NLB による管理対象デバイスからアクティブ TMS ノードへの通信の指示



4. アクティブ ノード サーバとパッシブ ノード サーバ間でのファイル共有の設定

すべての運用データは SQL データベースに保管されますが、一部のアプリケーション固有ファイルはホスト サーバのファイル ストラクチャ内に保存されます。これらのカスタマイズ可能なファイルは TMS アプリケーションにより追加され、冗長環境を使用する場合は 2 つのサーバ間でこれらのファイルを同期する必要があります。このようなファイルには、Cisco TMS にアップロード可能なソフトウェアおよびイメージ、Cisco TMS により作成されたイメージなどが含まれます。

デフォルトのインストールでのファイルの場所は次のとおりです。

C:\Program Files\TANDBERG\TMS\Config\System\

C:\Program Files\TANDBERG\TMS\Data\GenericEndpoint\

C:\Program Files\TANDBERG\TMS\Data\SystemTemplate\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\CompanyLogo\

C:\Program Files\TANDBERG\TMS\wwwTMS\Data\ExternalSourceFiles\

C:\Program Files\TANDBERG\TMS\wwwTMS\Public\Data\SystemSoftware\

Windows Server オペレーティング システムの分散ファイル システム（DFS）を使用して、2 つのサーバ間のレプリケーション プロセスを実行します。「フル メッシュ」設定が使用されている場合、DFS は 2 つのサーバ間でこれらのファイルを同期した状態で維持します。

5. 追加の TMS 設定

プリファード アーキテクチャで意図されているとおりに導入環境が機能するようにするには、Cisco TMS のインストール中に次の追加設定タスクを実行します。

- ISDN および IP ゾーン
- Active Directory の統合、グループ構造、ユーザ
- システム ナビゲータ フォルダの構造
- WebEx 接続
- デフォルトの会議設定
- TMS 内での電子メール テンプレートの変更

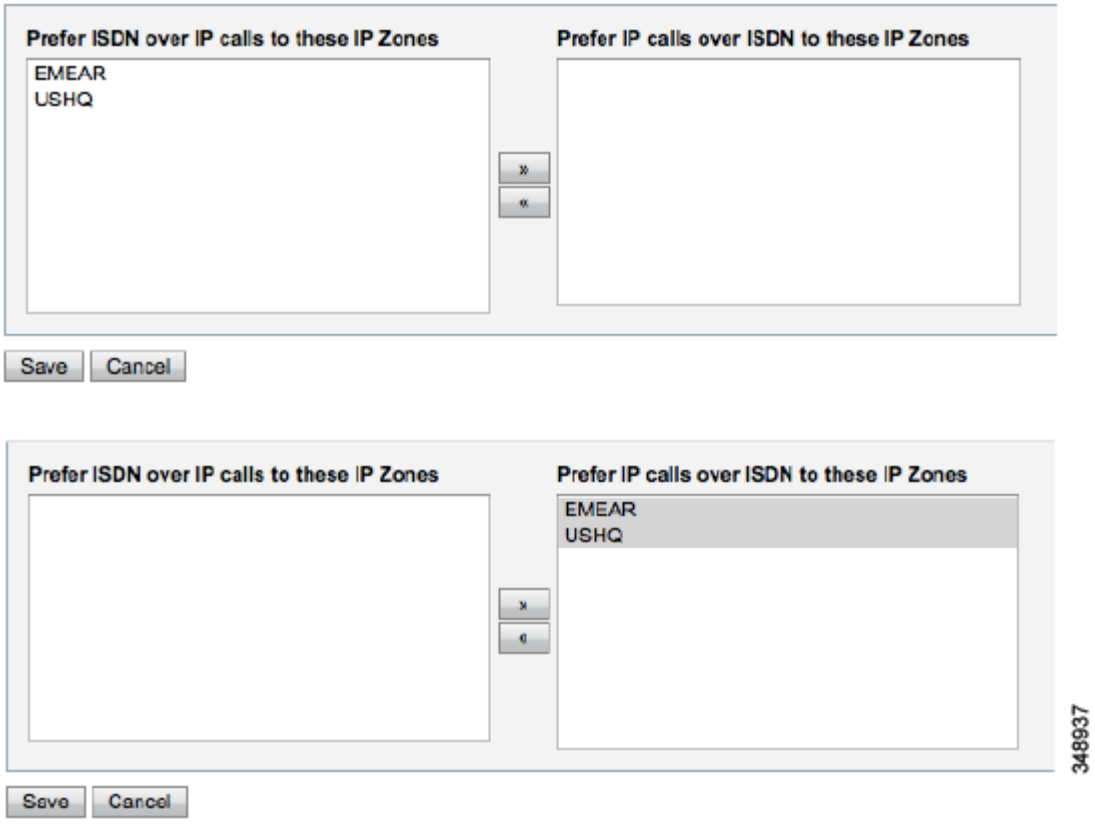
ISDN および IP ゾーン

会議リソースが配置されるロケーションごとに追加 IP ゾーンを設定します。

会議リソースが配置されている各ロケーションは、一意の IP ゾーンにより識別されます。

（注）　ネットワーク設定に基づいて [このIPゾーンでISDNよりもIPコールを優先する（Prefer IP calls over ISDN to these IP Zone）] に値を入力してください（図 5-9を参照）。デフォルトでは、すべての新規 IP ゾーンは、その他のすべての既存 IP ゾーンで IP よりも ISDN を「優先」します。この項目を選択しないと、TMS はゾーン間でコールをルーティングする方法を認識できないため、TMS による会議設定が失敗することがあります。

図 5-9　　ISDN よりも IP コールを優先する IP ゾーンの設定



追加の ISDN ゾーンを設定します。

使用する ISDN ゲートウェイごとに、TMS で ISDN ゾーンを追加作成します。これにより、コラボレーション エッジの章で定義しているように、エンドポイントはすべてのスケジュール済みコールに対し、目的の ISDN ゲートウェイを使用するようになります。各 ISDN ゲートウェイには、外部ダイヤルのためのプレフィックスがあり、そのプレフィックスが TMS で設定されている必要があります。

Active Directory の統合、グループ構造、ユーザ

Active Directory サービス アカウントのすべての情報が正しく入力されていることを確認します。

（注）　AD 接続のすべての設定が正しいことを確認し、接続をテストします。AD 同期が機能していない場合でも、TMS 内でその他の AD インターフェイス コマンドを実行すると、エラーが表示されないことがあります。

Active Directory Group を使用して、組織のニーズに対応するグループ構造を作成します。

デフォルトでは、TMS のインストール中に 3 種類のグループが作成されます。

- Users
- Video Unit Administrator
- Site Administrator

顧客のニーズに対応するようにこれらのグループを変更できますが、削除はできません。デフォルトでは、すべてのグループに Site Administrator と同じアクセス権限が付与されます。

これらのデフォルト グループでのユーザ入力は、手動での入力に制限されているため、グループを Active Directory からインポートし、既存の Active Directory グループを使用してエンドユーザによる TMS 機能へのアクセスを管理する必要があります。会議をスケジュールするエンドユーザ、サポート デスク担当者、および技術管理者のグループを検討してください。

グループに関する追加情報については、『*Cisco TelePresence Management Suite Administrator Guide*』

http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-maintenance-guides-list.html より入手可能）を参照してください。

[ADからインポート（Import from AD）] 機能を使用すると、エンドユーザの職務を一元的に管理できます。従業員を追加または削除するか、あるいは職務を変更して、組織的な Active Directory グループを変更すると、TMS 権限が自動的に更新されます。

Active Directory からグループをインポートしたら、各グループに適切な権限を割り当てます。表示される画面で、グループに設定しない権限をすべてオフにします。これらの権限を制限しないと、意図しない設定変更が発生する可能性があります。

また、すべてのユーザに対して適切なデフォルト グループを選択してください。

（注）　Cisco CMS にアクセスできるすべてのユーザは自動的に Users グループに追加されます。このグループをオフにすることはできません。管理者が組織内のすべてのユーザに対して付与しない権限があれば、それらをすべて選択解除します。

ユーザのインポート

グループの権限が設定されたら、[すべてのユーザをADと同期する（Synchronize All Users with AD）] 機能を使用してユーザをインポートします。組織の規模と関連するグループの数に応じて、同期が完了するまでに長時間かかることがあります。

（注）　ユーザは、初めて TMS にログインするまではユーザ リストに表示されません。

システム ナビゲータ フォルダの構造

TMS システム ナビゲータは、フォルダ構造を使用して管理者のためにデバイスを論理的にグループ化します。組織の物理的な環境に対応したフォルダ構造を作成します。これらのフォルダは管理者に対してだけ表示され、エンドユーザに対しては表示されません。組織の論理フローに基づいてフォルダを配置します。たとえば、地域ごとに 1 つのフォルダを作成し、続いてインフラストラクチャのサブフォルダと会議室エンドポイントのための別のフォルダを作成します。システム ナビゲータ内のフォルダには、TMS から接続の指示を受信するインフラストラクチャ デバイスまたはエンドポイント、あるいはこの両方を含めることができます。

WebEx 接続

Cisco CMR Hybrid を活用するには、組織の WebEx サイトに接続する必要があります。（CMR Hybrid の詳細については、会議の章を参照。）TMS 内で 表 5-21の設定が行われていることを確認してください。

表 5-21　WebEx 向け TMS 設定

パラメータ	値
[WebExを有効化（Enable WebEx）]	[はい（Yes）]
[すべての会議にWebExを追加（Add WebEx to All Conferences）]	[はい（Yes）]
[Active DirectoryからWebExユーザ名を取得する（Get WebEx Username from Active Directory）]	ユーザ名（samAccountName）
[WebExサイト（WebEx Site）]	顧客アカウント別に設定
[新規ユーザのデフォルトサイト（Default site for new users）]	[はい（Yes）]
[SSOを有効にする（Enable SSO）]	[はい（Yes）]

表 5-21の設定により、TMS はスケジュール中にエンドユーザの代わりに組織の WebEx サイトと通信できるようになります。WebEx をすべての会議に自動的に追加することで、管理者が WebEx 生産性ツール以外の方法で会議を生成する必要がある場合に、エンドユーザに対して WebEx リンクが使用可能になります。SSO 設定により、エンドユーザは 1 つのクレデンシャル セットですべてのコラボレーション サービスにアクセスできるようになります。これは、WebEx サービスはエンドユーザの AD クレデンシャルを使用して WebEx ツールにアクセスできるためです。

デフォルトの会議設定

会議をスケジュールする前に、管理者はエンドユーザ コミュニティの使用モデルと、エンドポイントの制限について理解しておく必要があります。検討すべき重要な Cisco TMS 設定には、次のものがあります。

- ワンボタン機能
- 帯域幅
- すべての会議にWebExを追加
- 参加者に対し5分前の接続を許可する

ワンボタン機能

ワンボタン機能により、エンドユーザは特定のルームで開催される当日の会議をカレンダーで確認し、会議への接続を開始できます。Cisco TMS はユーザに対し、1 要求あたり 72 時間分のカレンダー情報を提供します。

帯域幅

この設定はエンドポイントごとに行います。ネットワークに必要な設定にあわせて帯域幅を調整してください。HD メイン チャネルとコンテンツの最大解像度を有効にするには、非イマーシブ システムのデフォルト帯域幅を 2048 kbps に設定してください。最大帯域幅にこれよりも低い値が設定されているエンドポイントはすべて、その最大帯域幅で接続します。

すべての会議にWebExを追加

各会議で完全なコラボレーション エクスペリエンスを提供するには、この設定を選択する必要があります。[ユーザアクセス方式（Method of User Access）] を [WebEx（ユーザ名）（WebEx (Username)）] に設定するオプションを選択します。この設定により、会議をスケジュールする担当者のユーザ名が招待状の WebEx 部分に表示され、またそのエンドユーザの Jabber または WebEx モバイル クライアントの議題に会議のデータを取り込むことができます。

参加者に対し5分前の接続を許可する

エンドユーザの時間インターフェイスで多少の差異を許可するには、この設定を選択します。TMS サーバでの正確な時刻よりも前にユーザが接続できるようにすることで、より一貫性のあるエンドユーザ エクスペリエンスを提供し、また会議開始時刻の数分前にエンドユーザが会議に接続しようとしたときに「接続できない」というメッセージが表示されなくなります。

TMS 内での電子メール テンプレートの変更

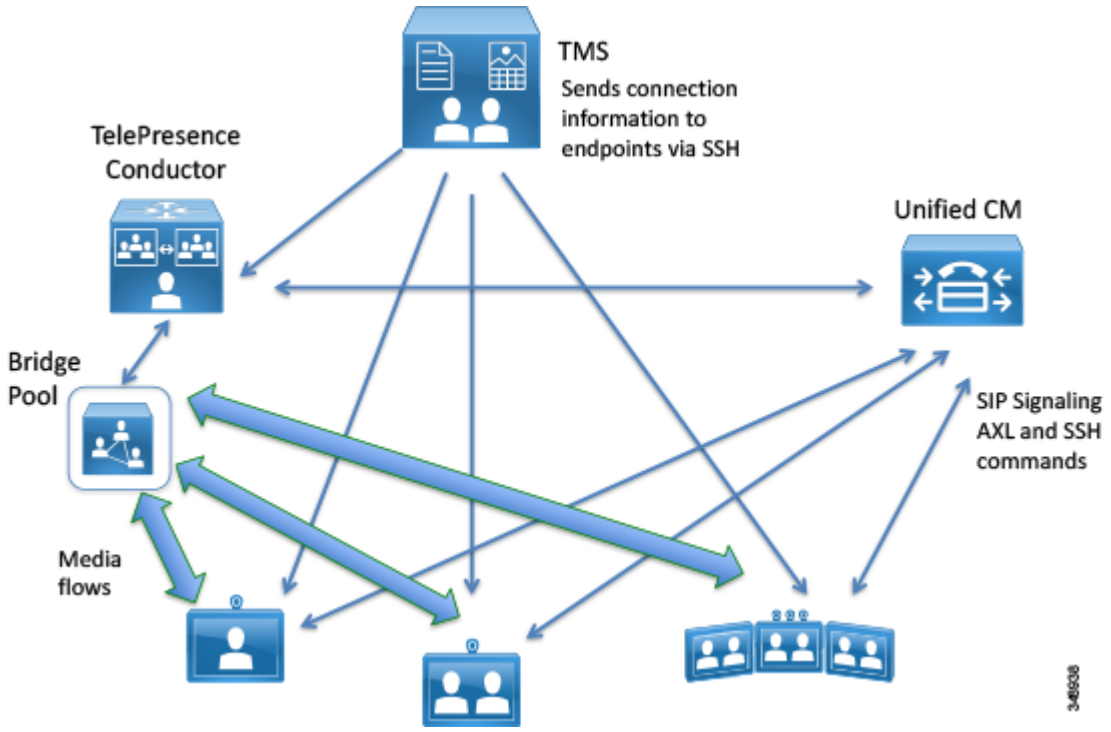
Cisco TMS には、会議主催者への通知に使用できるテンプレートがあります。ただし Cisco TMSXE では、Cisco TMS が送信する電子メールのメッセージにエラー、警告、および情報テキストが挿入されることがあります。管理者はこれらのメッセージを変更できます。{MEETING_TITLE}、{CONTACT_HOST} のように中カッコで囲まれたテキストは、スケジュール済みイベントの特定のコンテンツを組み込む変数であるため、これらのテキストを削除または変更しないようにしてください。

すべての電子メール テンプレートで、TMS により自動生成される通信内容が目的の手続きに対応していることを確認します。多くのテンプレートはシンプルに作られており、各組織がテンプレートを拡張することを前提としています。また、テンプレートは標準 HTML エディタを使用して変更できます。

6. TMS への管理対象デバイスの追加

Cisco TMS がスケジュール済み会議を作成できるようにするため、必要なコンポーネントを TMS にシステムとして追加する必要があります。TMS スケジューリング メカニズムがすべてのデバイスのコール制御エンティティを認識できるようにするため、Unified CM が TMS に追加されます。TMS は Unified CM の設定を制御しませんが、Unified CM が管理する会議室のエンドポイントと直接通信します。（図 5-10を参照）。

図 5-10　　Cisco TMS と Unified CM 管理対象エンドポイントの直接通信



TelePresence Conductor のインストールとスケジュールのための設定

この項では、TelePresence Conductor をインストールして導入し、Cisco TMS によるスケジュールが可能な状態にするために必要な作業について概説します。主要な導入タスクは次のとおりです。

- スケジューリングのための TMS への TelePresence Conductor および TelePresence Server の追加
- TelePresence Conductor とダイヤル プランの統合
- TMS チケット フィルタの調整によるゲートキーパーの警告の除去

TelePresence Server の物理的な位置を考慮することが重要です。これは、この位置と各参加者の間でメディア トラフィックが生じるためです。TelePresence Conductor を、その管理対象 TelePresence Server が導入される各リージョンで、管理対象 TelePresence Server に対して中央に配置してください。

Cisco TMS は、クラスタ内で 1 つの TelePresence Conductor ノードだけを認識します。複数の TelePresence Conductor（TelePresence Conductor クラスタごとに 1 つずつ）が設定されている場合、Cisco TMS はこれらをスケジュール済み会議用であると認識します。Cisco TMS は、予約の時点でスケジュールされているエンドポイントと TelePresence Conductor の IP ゾーン設定を使用して、予約でどの TelePresence Conductor を優先するかを決定します。

会議の章の情報に基づいて TelePresence Conductor をインストール、設定します。

スケジューリングのための TMS への TelePresence Conductor および TelePresence Server の追加

計画段階で策定され、設定プロセスで TMS システム ナビゲータに設定されたフォルダ構造を使用して、1 つの TelePresence Conductor ノードを管理用に TMS に追加します。インストールされている TelePresence Conductor ごとに適切な IP ゾーンを必ず選択してください。また TMS 内で、TelePresence Conductor と同じ IP ゾーンの同じフォルダに、TelePresence Conductor が管理する各 TelePresence Server を追加します。

（注）　TMS システム ナビゲータを介して TelePresence Conductor と TelePresence Server を追加する場合、これらは非 SNMP デバイスとして追加されます。

TelePresence Conductor とダイヤル プランの統合

スケジュール済みコールのために TelePresence Conductor をインストールする前の準備として、会議エイリアスを作成し、ダイヤル プランの一部として使用する TelePresence Conductor の数値範囲を特定し、SIP トランクで指定しました。表 5-22に、TelePresence Conductor ダイヤル プランのパラメータ設定を示します。

表 5-22　TelePresence Conductor ダイヤル プランの設定

パラメータ	値
[数字IDベース（Numeric ID Base）]	これは、ダイヤル プランのスケジュール会議範囲の 1 番目の数字です。
[数字IDステップ（Numeric ID Step）]	範囲内のすべての数字を使用するには、デフォルト値 1 のままにします。
[数字IDの桁数（Numeric ID Quantity）]	この TelePresence Conductor のダイヤル プランで使用可能な桁数を指定します。
[ゲートキーパーに登録する（Register with Gatekeeper）]	プリファード アーキテクチャでは H.323 ではなく SIP 接続が使用されるため、[オフ（off）] に設定してください。

その他のすべての設定はデフォルト値のままにして設定を保存します。これで TelePresence Conductor が TMS に追加されます。

TMS チケット フィルタの調整によるゲートキーパーの警告の除去

Cisco TMS は、E.164 エイリアスと SIP URI の両方に、前述のステップで指定したダイヤル プランの数値を取り込みます。ただし TMS 内での E.164 ロジックの実装は、プリファード アーキテクチャのその他の場所での E.164 の使用方法とは異なります。TMS は E.164 エイリアスを H.323 通信だけに関連付けます。したがって、TelePresence Conductor の特定の警告を無視するように TMS の統合チケット システムを調整する必要があります。

TelePresence Conductor が TMS に追加されたら、このエントリのチケット フィルタを調整するため、[ゲートキーパーモードオフ（Gatekeeper Mode Off）] のフィルタを追加します。

TMS への Unified CM の追加

Unified CM はその他のすべての設定および管理の面で会議室のエンドポイントを管理しますが、予約と接続開始を実行できるようにするため、Unified CM クラスタを TMS に追加する必要があります。Unified CM を TMS に追加するには、次のタスクを実行します。

- Unified CM 内でのCisco TMS のアプリケーション ユーザの作成
- ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

複数の Unified CM クラスタを追加する場合は、コール制御の章で説明するダイヤル プラン設定に準拠する必要があります。

Unified CM 内でのCisco TMS のアプリケーション ユーザの作成

このアプリケーション ユーザにより、Unified CM が制御するエンドポイントと TMS が通信できるようになります。このユーザには、Unified CM 内のスケジュール対象の会議室デバイスすべてを割り当てる必要があります。また、次のロールが設定されている Cisco TMS 専用のユーザ グループにこのユーザを追加する必要もあります。

- Standard AXL API Access
- Standard CTI Enabled
- Standard SERVICEABILITY
- Standard CCM Admin Users
- Standard RealtimeAndTraceCollection

詳細については、『*Cisco Unified Communication Manager Configuration Guide for the Cisco TelePresence System*』を参照してください。

ご使用の環境での各 Unified CM クラスタのパブリッシャの追加

Unified CM パブリッシャを TMS に追加すると、TMS はそのエンドポイントのコール制御権限を認識します。Unified CM を認識しない場合、TMS スケジューリング エンジンは導入環境の全機能を利用できず、接続が失敗することがあります。

パブリッシャは、他のデバイスの場合と同様の方法で、TMS からユーザ名とパスワードの入力を求められたら、前述のステップで作成したアプリケーション ユーザのユーザ名とパスワードを使用して追加します。

TMS への会議室エンドポイントの追加

IP アドレスまたは DNS 名でデバイスを追加する代わりに、[リストから（From List）] タブを使用して、Unified CM を選択します。TMS のスケジューリング インターフェイスから使用できるようにする会議室の TelePresence デバイスをすべて選択します。エンドポイントごとに適切な IP ゾーンを選択してください。この IP ゾーンは、すべての会議でのエンドポイントに使用可能な TelePresence Server の中から、最適なサーバを選択するために使用されます。Unified CM の各エンドポイントの DN が、コール制御の章に記載されている E.164 ガイドラインに準拠していることを確認します。

Exchange を介して TMS にリソースとしてスケジュールされることがないパーソナル TelePresence デバイス（Cisco TelePresence EX または DX シリーズのエンドポイントなど）は追加しないでください。

7. TMS Extension for Microsoft Exchange のインストールと設定

Cisco TelePresence Management Suite Extension for Microsoft Exchange（Cisco TMSXE）は、Microsoft Outlook からビデオ会議のスケジュールを可能にする Cisco TelePresence Management Suite の拡張機能であり、Cisco TMS 会議を Outlook の会議室予定表にレプリケートします。

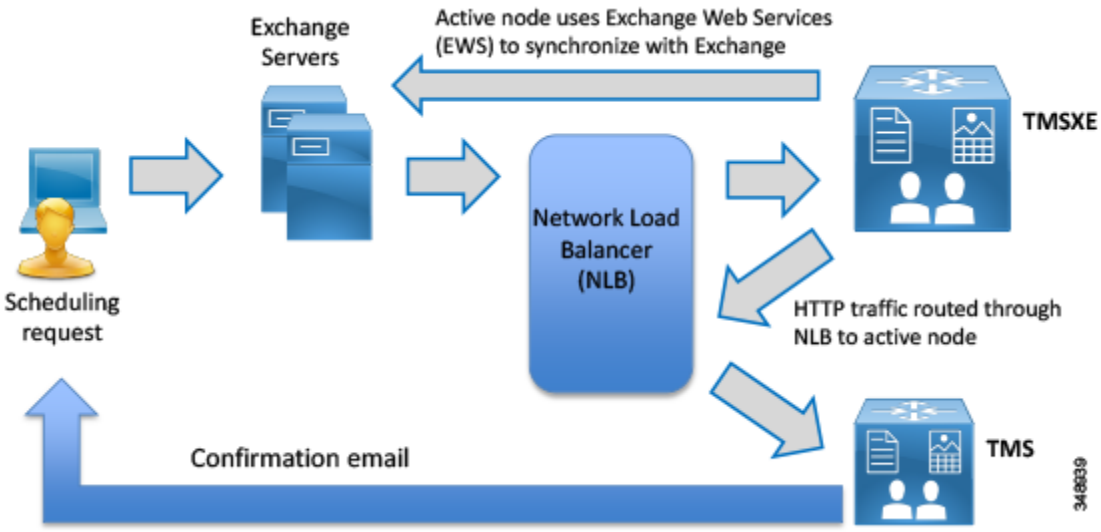
この TMS ソフトウェア拡張機能を使用するには、TMS 内で機能を有効にするためのライセンス キーが必要です。TMSXE ソフトウェアのインストール前に、このキーを TMS にインストールしておく必要があります。スケジュールされるエンドポイントの数が 50 を超える導入環境では、TMSXE を専用のサーバまたは仮想マシン インスタンスにインストールする必要があります。

前提条件

Cisco TMSXE をインストールする前に、Outlook と Exchange がすでにセットアップされており、ユーザがルーム メールボックスを含む会議を予約できることを確認してください（図 5-11を参照）。この統合は、エンドポイント グループによりライセンスされるか、または Application Integration ライセンス キーとしてライセンスされます。インストールを続行する前に、正しいキーを作成し、TMS に入力する必要があります。両方のオプション キーを追加した場合、Cisco TMS は Application Integration Package オプションのみを使用します。

Cisco TMSXE が使用できる Microsoft Exchange リソースは、オンプレミス、Office 365 ホスティング導入環境、または顧客のハイブリッド導入環境のいずれかです。お客様の特定の環境に適用される可能性のある推奨事項またはガイドラインについては、Microsoft Exchange の管理と導入に関する資料を参照してください。

図 5-11　　エンドユーザによる会議のスケジュール フローの例



システム別のオプション キーを Cisco TMS で有効化したら、[リモート予約を許可する（Allow Remote Bookings）] 設定により、各システムがライセンスを使用するかどうかが決定します。この設定により、エンドユーザが予約でき、個別のエンドポイント ライセンスの 1 つを使用できるエンドポイントを管理者が選択できます。Application Integration Package オプションを使用する場合は、この設定は無効であり非表示になります。

Cisco TMSXE にエンドポイントを追加するには、その前に、Exchange でこれらのエンドポイントがルーム メールボックスによって示されている必要があります。TMSXE のセットアップを簡素化するため、エンドポイントの Cisco TMS 表示名をメールボックス名として使用することを推奨します（スペースはすべて削除してください）。これにより、エンドユーザに対するシステム名の表示方法すべてで統一が図られます。

Exchange のプライバシー機能に関する特別な注意事項

Cisco TMSXE に追加されるすべてのルーム メールボックスが、予約件名とプライバシー設定を同一の方法で処理するように設定されている必要があります。つまり、以下の設定をすべてのメールボックスに適用するか、またはどのメールボックスにも適用しないかのいずれかになります。

- [件名の削除（Delete the subject）]

  サポート担当者が会議制御センターで特定の会議を識別できるようにするため、この機能を使用しないことを推奨します。また、これにより会議のタイトルが対応エンドポイントの One Button to Push インターフェイスに表示されるようになります。

- [開催者名を件名に追加する（Add the organizer's name to the subject）]

  この設定を使用する際には十分に注意し、組織の慣習に基づいて使用してください。あるユーザが複数グループの会議をスケジュールすると、スケジュールされた会議は会議の件名ではなくそのスケジュール担当者のユーザ名でリストされることに注意してください。会議の件名の方が便利である可能性があります。一方、会議がそれぞれ該当する主催者によってスケジュールされる場合、特定の会議の件名を覚えておくよりも、「ボブの会議」と確認できる方が容易なことがあります。ほとんどの組織ではこの設定を使用しないことを推奨します。

- [承諾した会議に設定されたプライベートフラグを削除する（Remove the private flag on an accepted meeting）]

  「プライベート」フラグは Outlook クライアント内では反映されますが、Cisco TMS ではサポートされていないため、会議の議題は以下の場所で制限なしで表示されます。

  - Cisco TMS 内
  - 組織内で件名を公開すべきではない会議に使用する会議室を、他の担当者も使用している場合は、会議室予定表をサポートしているエンドポイント。（たとえば、最高責任者による「合併会議」がスケジュールされている会議室を使用する、保留中の合併について知る必要がない下位レベルの従業員に対し、会議室システム予定表にこの会議が表示されることがあります。）
  - Exchange で「プライベート」フラグが設定されている予約の参加者または定例会議パターンが Cisco TMS で変更されると、この変更が Exchange にレプリケートされる時点で「プライベート」フラグが削除されます。

インストール プロセス

TMSXE ユーザの作成

- Active Directory で TMSXE ユーザを作成し、TMS にインポートします。
- TMS では、[予約（Booking）] の下で次の権限が有効な既存のグループまたは新規のグループにこのユーザが属している必要があります。
  - [読み取り（Read）]
  - [更新（Update）]
  - [代理予約（Book on Behalf of）]
  - [会議承認（Approve Meeting）]

証明書のインストール

Cisco TMSXE と TMS の通信には HTTPS が使用されます。TMSXE サーバと Exchange 環境間のセキュア通信は証明書でも可能です。TMS アプリケーション サーバと同様に、TMSXE のアクティブ ノードとパッシブ ノードの両方に同じ証明書がロードされ、証明書の DNS 項目は TMSXE に使用されるネットワーク ロード バランサのアドレスの項目を指し示します。

ソフトウェア インストーラの実行

- スケジューリングに WebEx 生産性ツールを使用できるようにするため、TMS Booking Service を選択してください。
- アクティブ ノードまたはパッシブ ノードに適切な冗長性オプションを選択します。
- アクティブ ノードとパッシブ ノードの両方でソフトウェア インストールを実行します。

アクティブ ノードとパッシブ ノードの両方でインストールが完了したら、各ノードのプローブ URL を使用してネットワーク ロード バランサを設定します。

Cisco TMSXE の設定

Cisco TMS 接続情報

TMSXE アプリケーションが TMS アプリケーションと通信できるようにするため、Active Directory で作成した TMSXE アカウントを使用して TMS 接続情報を設定します。

Exchange Web Services の設定

ユーザとリソース メールボックスのために TMSXE が Exchange サーバと通信できるように Exchange Web Services（EWS）を設定します。この接続に使用するクレデンシャルは、他の場所で使用されるものと同じ TMSXE クレデンシャルです。

Exchange と TMS リソースの調整

TMS システム ID に合わせて Exchange リソースを調整します。この操作は、『*Cisco TelePresence Management Suite Extension for Microsoft Exchange Deployment Guide*』で説明する .csv ファイルを使用した方法で行うか、または個別に行います。

エンドユーザ向けの WebEx 生産性ツールの使用

エンドユーザ コラボレーション ツールを最大限に活用できるようにするため、すべてのユーザに対して WebEx 生産性ツールを導入します。TelePresence を含む WebEx 生産性ツールにより、次に示す会議を同期的に予約および設定するための特殊なパネルが Outlook for Windows に追加されます。

- WebEx と TelePresence の両方を含む CMR Hybrid 会議
- WebEx のみの会議
- TelePresence のみの会議

このパネルから、WebEx と TelePresence の両方の簡易設定と詳細設定にアクセスできます。この設定には、TelePresence のコールインおよびコールアウト参加者を追加するオプションや、WebEx 参加者に対し開始時刻よりも前に会議に参加できるようにするオプションなどが含まれます。

TelePresence のみの会議を予約する場合でも、生産性ツールが機能するようにすべての主催者に対し WebEx ユーザをセットアップする必要があることに注意してください。

TelePresence を含む WebEx 生産性ツールの設定と導入の詳細な手順は、『*Cisco WebEx Site Administration User's Guide*』に記載されています。この資料は WebEx サイトから Web ヘルプまたはPDF ファイルとして入手することもできます。

アプリケーション導入ツール

この章で説明したコア アプリケーション以外に、エンタープライズ コラボレーション プリファード アーキテクチャを導入する管理者にとって役立つ 2 つのツールがあります。

- Cisco Prime Collaboration Deployment：IM および Presence Server からなる Unified CM クラスタのインストールに必要なステップの多くを自動化し、管理者を支援します。
- Cisco Prime License Manager：導入環境内で使用されるさまざまなライセンスの一元管理ポイントを提供するツールとして Cisco Unified CM に統合されています。

Cisco Prime Collaboration Deployment（PCD）

Prime Collaboration Deployment（PCD）は、Unified CM と IM および Presence サーバで構成される新しいクラスタの導入作業を行う管理者をサポートします。自動化によりクラスタのノードのすべての共通設定が処理され、管理者の作業が大きくサポートされます。

PCD は、他のインストール タスクを開始する前に専用の仮想マシンにインストールする必要があるスタンドアロン アプリケーションです。PCD を使用して新しいクラスタをインストールするには、次の手順を実行します。

1. ホスト ハードウェアを導入し、ESXi を設定します。
2. ターゲット リリースに必要な OVA テンプレートと Cisco ISO イメージをダウンロードします。
3. お客様の企業に適した推奨 OVA テンプレートを導入します。
   a. ESXi ホストでノードごとに仮想マシンを作成します（インストールするサーバごとに 1 つの仮想マシン）。
   b. 新しい仮想マシンでネットワーク設定を行います。
4. ESXi ホストを PCD ユーザ インターフェイスに追加します。
5. 作成するクラスタのタイプの新しいタスクを PCD 内で作成します。インストールするノードと、その関連仮想マシンを定義します。

Cisco PCD により仮想マシンへのアプリケーションのインストールが実行され、タスクが完了すると管理者に電子メールで通知が送信されます。

Cisco Prime License Manager（PLM）

Cisco Prime License Manager（PLM）は、社内全体でのユーザベースのライセンスを管理するシンプルな機能（ライセンス履行を含む）を提供します。Cisco Prime License Manager は、ライセンス履行を処理し、複数のサポート製品間でのライセンスの割り当ておよび調整をサポートし、使用と権限付与に関するエンタープライズ レベルのレポートを提供します。

1 つのエンタープライズに 1 つの仮想マシンが必要であり、アプリケーションは VMware ツールによりバックアップされる必要があります。PLM のスタンドアロン インスタンスとして、プリファード アーキテクチャのすべてのノードを効果的に管理できます。これはエンドユーザが直接使用するアプリケーションではなく、またリアルタイムの使用状況に影響しないため、クラスタリングは不要です。PLM には、追加ライセンスの電子履行をサポートする機能があるため、このサーバは新しいライセンス ファイルを取得するためにインターネットへのアクセスを必要とします。

プリファード アーキテクチャでは次の製品が PLM によりサポートされています。

- Cisco Unified CM
- Cisco Unity Connection

管理者に役立つ PLM の主な機能を次に示します。

- ライセンス使用履歴
- 新規ライセンスの電子履行

ライセンス使用履歴

管理者が一定期間のコラボレーション ポートフォリオ ライセンスの使用状況を追跡できる機能です。これにより、管理者は必要に応じた追加ライセンスをより適切に計画できます。このライセンス使用状況管理ツールを使用することで、管理者はすべてのライセンス使用ルールに準拠できます。

アプリケーションの非準拠状態は 60 日まで許容されます。この期間内には、ライセンスが不足している場合や、PLM ノードとアプリケーション ノードの間の通信が失われた場合に管理者が変更を行うことができます。非準拠状態で 60 日が経過した後は、Unified CM アプリケーションでは管理者による変更はできなくなりますが、アプリケーションはサービスを停止することなく引き続き機能（コール制御）します。非準拠状態で 60 日が経過した後でも、Unity Connection アプリケーションでは管理者による変更が可能ですが、アプリケーションは機能しなくなります（ユーザはボイス メッセージにアクセスできなくなります）。

新規ライセンスの電子履行

管理者が追加ライセンスを調達する必要がある場合には、PLM の電子履行ツールにより必要なステップが簡素化され、該当製品で使用されるライセンスがインポートされます。

追加のアプリケーション

Cisco およびエコシステム パートナーから、コラボレーション環境を強化するさまざまな追加アプリケーションが提供されています。表 5-23に、よく利用されるお客様の導入のためのアプリケーションを示します。ただしこの表にはすべてのツールがリストされているわけではありません。

表 5-23　プリファード アーキテクチャのためのその他の Cisco アプリケーション

アプリケーション	機能	連動方法
Unified Contact Center Enterprise（CCE）	内外のカスタマー コラボレーション テクノロジー（エージェント ログイン、コール ベクタリングのための音声自動応答（IVR）、アウトバウンド接続方式、マルチチャネル エージェント インタラクションなど）を提供します。	エンタープライズ コンタクト センターは、エンタープライズ Unified CM クラスタにトランキングしている専用の Unified CM クラスタ上で動作します。
Contact Center Express（CCX）	小規模なコンタクト センターまたは社内での使用に適したコンタクト センターのサブセットと名前によるダイヤル機能を提供します。	JTAPI を介して Unified CM と通信します。
TelePresence Content Server（TCS）	ビデオ、音声、およびコンテンツの録音機能を提供します。この機能は、TMS のチェックボックスを介してスケジュールされたコールに組み込むか、またはダイヤルすることで利用できます。これにより、エンドポイントが簡単に録音ステーションになります。	TCS はコール制御のために Cisco TelePresence Video Communication Server（VCS）Control に登録し、Unified CM と VCS Control 間の SIP トランクを介して Unified CM デバイスに接続します。
Show and Share	社内で保管されているビデオ コンテンツのポータルを提供します。	TCS はコンテンツを Show and Share に自動的にアップロードします。コール制御へのその他の統合は必要ありません。
Prime Collaboration Provisioning	「Day 2」運用のための管理ポータルを提供します。	インフラストラクチャ デバイスおよびエンドポイントの SSH および HTTPS インターフェイスを介して通信するスタンドアロン ソフトウェアです。
Prime Collaboration Assurance	コラボレーション導入管理者に品質および障害検出サービスを提供します。	インフラストラクチャ デバイスおよびエンドポイントの SSH および HTTPS インターフェイスを介して通信するスタンドアロン ソフトウェアです。
Prime Collaboration Analytics	コラボレーション導入管理者が使用状況と障害のトレンド分析に使用できる最長 1 年分の使用状況データを提供します。	Prime Collaboration Assurance とともに導入され、Prime Collaboration Assurance により収集されたデータを使用します。
Attendant Console	社内オペレータまたは受付担当者に対し、着信コールを処理するためのデスクトップ アプリケーションを提供します。	標準バージョンはエンドユーザの Windows コンピュータにインストールされ、Unified CM に接続します。 拡張バージョンは専用サーバで実行され、エンドユーザはこのアプリケーションにログインします。

表 5-23　プリファード アーキテクチャのためのその他の Cisco アプリケーション（続き）

アプリケーション	機能	連動方法
MediaSense	Unified CM で常時録音および選択録音の両方の状況に対応した録音機能を提供します。	録音プロファイルが Unified CM で設定され、MediaSense は SIP トランク経由で Unified CM と Cisco Unified Border Element に接続します。
Jabber Guest	Business-to-Consumer（B2C）コラボレーションのためのクリック接続機能を提供します。	専用の Expressway-C / Expressway-E ペアが必要です。モバイルおよびリモート アクセスと Business-to-Business（B2B）ビデオコール向けに使用するエンタープライズ Expressway-C および Expressway-E 実装の個別ドメインを使用します。Unified CM には、この専用 Expressway ペアへの SIP トランクがあります。

CHAPTER 6

サイジング

改訂日：2015 年 1 月 22 日

エンタープライズ コラボレーション向けプリファード アーキテクチャ ソリューションのコンポーネントのサイジングは、ソリューション設計全体の重要な部分です。

特定の展開におけるサイジング プロセスの目標は、以下の項目を決定することです。

- 各シスコ コラボレーション製品で使用されるプラットフォームのタイプ。ほとんどの製品は仮想化のみを使用して展開されますが、Cisco TelePresence Server などの一部の製品は、要件に応じてアプライアンスまたはブレードとして展開することもできます。
- 各シスコ コラボレーション製品に関して展開されるインスタンスの仕様と数。仮想化を使用して展開される製品では、これは Open Virtual Archive（OVA）テンプレートで定義される仮想マシンのハードウェア仕様と仮想マシンの数に相当します。仮想化を使用せずに展開される製品では、これはアプライアンスまたはブレードのタイプと数に相当します。

サイジングは、考慮すべきパラメータの数が多いため、複雑な作業になる可能性があります。サイジングの作業を簡略化するため、この章ではサイジングの例を対応する仮定条件とともにいくつか紹介します。ここでは、これらのサイジング例を *簡易サイジング展開* と呼びます。個々の展開の要件がこれらの仮定条件の範囲内である場合は、このマニュアルの簡易サイジング展開を参考として使用できます。それ以外の場合は、『*Cisco Collaboration SRND*』のサイジングに関する章および製品ドキュメント（http://www.cisco.com/go/ucsrnd）の記載内容に従って、通常のサイジング計算を行う必要があります。

仮想化を使用して展開された製品のサイジングを行った後は、仮想マシンを Cisco Unified Computing System（UCS）サーバに配置する方法を決定し、共存のルールを検討します。最終的には、この仮想マシンの配置プロセスによってソリューションに必要な UCS サーバの数が決まります。

この章では、このマニュアルで扱っているすべてのモジュール（つまり、コール制御、会議、コラボレーション エッジ、およびコア アプリケーション）のサイジングについて説明します。この章では、仮想マシンの配置とプラットフォームについても説明します。

このマニュアルでは、仮想マシンとして展開される製品の仮想マシン OVA テンプレートの詳しい仕様については説明しません。これについては、http://www.cisco.com/go/uc-virtualized にある『*Unified Communications in a Virtualized Environment*』のドキュメントを参照してください。

この章の変更点

表 6-1 に、この章に新しく追加されたトピック、またはこのマニュアルの以前のリリースから大幅に改訂されたトピックの一覧を示します。

表 6-1　本リリースで追加または変更された情報

新規トピックまたは改訂されたトピック	説明箇所	改訂日
推奨される TelePresence Server プラットフォームと容量	「TelePresence Server プラットフォームのサイジング」（P.6-8）	2015 年 1 月 22 日

コール制御

コール制御の章で説明したように、Cisco Unified Communications Manager（Unified CM）および IM and Presence サービスは Unified CM クラスタおよび IM and Presence クラスタを通じて提供されます。

Cisco Unified CM クラスタは、1 つのパブリッシャ ノード、2 つの専用 TFTP サーバ、および 1 つまたは複数のコール処理ノード ペアで構成されます。コール処理ペアの数は展開のサイズによって異なるため、後で説明します。コール処理ノードは、1:1 の冗長性を確保するためにペアで展開されます。

IM and Presence ノードもペアで展開されます。IM and Presence ペアの数も展開のサイズによって異なるため、後で説明します。IM and Presence ノードは、1:1 の冗長性を確保するためにペアで展開されます。

Unified CM のサイジング

Unified CM については、簡易サイジングのガイダンスで最大 10,000 ユーザおよび 10,000 デバイスの展開に対応できます。Unified CM は、異なる仮定条件やコール処理ペアの追加によってより多くのユーザおよびデバイスをサポートしますが、これはこの章で示す簡易サイジングのガイダンスの範囲外です。表 6-2 に、簡易サイジング展開を示します。これらの展開に対して行われた仮定については、この表の後で説明します。展開環境内のユーザまたはエンドポイントの数が表 6-2 に示す値の範囲外である場合や、個々の展開の要件が仮定条件の範囲外である場合は、これらの簡易サイジング展開を使用せずに、http://www.cisco.com/go/ucsrnd にある『*Cisco Collaboration SRND*』のサイジングに関する章および http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/tsd-products-support-series-home.html にある製品ドキュメントに記載されている通常のサイジング手順を実行してください。

表 6-2　　Unified CM の簡易サイジング展開

展開サイズ	展開する Unified CM ノード （各 Unified CM ノードで 7,500 ユーザの OVA テンプレートを使用）
5,000 までのユーザまたはデバイス	**5 ノード**： 1 つのパブリッシャ、2 つの TFTP、1 つのコール処理ペア（2 つのコール処理サブスクライバ）
5,000 ～ 10,000 のユーザまたはデバイス	**7 ノード**： 1 つのパブリッシャ、2 つの TFTP、2 つのコール処理ペア（4 つのコール処理サブスクライバ）

表 6-2 では、ユーザとデバイス（のどちらか大きい方）の最大数に基づいてサイジングしています。たとえば、5,000 人のユーザと 1 ユーザあたり平均 2 個のデバイス（ユーザごとにデスクの電話とソフトフォン モードの Jabber クライアントがある場合など）を含む展開では、合計で 10,000 個のデバイスがあるため、7 ノードの展開が必要です。

これらの簡易サイジング展開では、UCS サーバで消費されるリソース全体を最適化するため、7,500 ユーザの仮想マシン設定（OVA テンプレート）が使用されます。この OVA テンプレートには、UC のパフォーマンスを最大限に引き出す CPU プラットフォーム（Cisco Business Edition 7000 など）が必要です。このテンプレートは Business Edition 6000 などではサポートされません。これらの OVA 仮想マシン構成テンプレートおよびプラットフォーム要件の詳細については、www.cisco.com/go/uc-virtualized のドキュメントを参照してください。

7,500 ユーザの OVA テンプレートを使用して展開された Unified CM コール処理ペアは、一定の条件下で最大 7,500 人のユーザをサポートできます。しかし、この設計では Unified CM に追加の負荷がかかる仮定条件を使用します。たとえば、シングル ナンバー リーチ用のリモート接続先プロファイルを使って各ユーザを構成できること、各ユーザがエクステンション モビリティを使用できること、各エンドポイントを CTI で制御できること、いくつかの共有回線が構成されていること、モバイル アクセスやリモート アクセスが有効であることなどを仮定します。したがって、表 6-2 に示したように、Unified CM コール処理ペアあたりの容量は減少します。次に、簡易サイジング モデルで使用される仮定条件について詳しく説明します。

Unified CM の仮定条件

表 6-2 に示した 2 つの簡易サイジング展開には、次の仮定条件が適用されます。

- ユーザあたりの最繁時呼数（BHCA）が平均 4 個以下。BHCA とは、最繁時のコール試行の数です。
- デバイスあたりの DN が平均 2 個以下。
- コール処理サブスクライバ ペアあたりの共有回線が最大 500 回線で、各回線が平均 3 個以下のデバイスによって共有されます。
- Unified CM（ソフトフォン モード）に登録される Jabber クライアントの数をデバイスの制限に照らしてカウントする必要があります。
- パーティションが最大 3,000 個、コーリング サーチ スペース（CSS）が最大 6,000 個、クラスタあたりのトランスレーション パターンが最大 12,000 個。
- Unified CM クラスタごとに、ルート パターンが最大 1,000 個、ルート リストが最大 1,000 個、ルート グループが最大 2,100 個。Unified CM コール処理ペアごとに、ハント パイロットが最大 100 個、ハント リストが最大 100 個、サーキュラーおよびシーケンシャル回線グループが最大 50 個（回線グループあたりのメンバー数は平均 5）、ブロードキャスト回線グループが最大 50 個（回線グループあたりのメンバー数は平均 10）。

- Unified CM コール処理ペアごとに、CTI ポートが最大 500 個、CTI ルート ポイントが最大 100 個。
- 複数の Unified CM クラスタを展開するときは、GDPR/ILS が有効になっています。
- エクステンション モビリティ（EM）：すべてのユーザが EM を使用できますが、クラスタ間のエクステンション モビリティ（EMCC）ユーザは存在しません。
- Unified CM のメディア リソース：この設計では、Unified CM ソフトウェア会議ブリッジ（ソフトウェア CFB）と Unified CM メディア ターミネーション ポイント（MTP）は使用できません。代わりに、TelePresence Server と Cisco IOS ベースの MTP を使用します。
- モビリティ ユーザあたりのリモート接続先またはモビリティ ID が平均 1 個以下。たとえば、5,000 ユーザを含む展開では、最大 5,000 個のリモート接続先またはモビリティ ID が存在します。
- Active Directory と同期するユーザが最大 40,000 人（ただし、コールの発着信を行うアクティブ ユーザは、表 6-2 から選択する簡易サイジング展開に応じて最大 5,000 人または 10,000 人）。
- Unified CM コール処理ペアあたりの同時アクティブ コール（会議セッションと会議以外のセッション）が最大 1,500 個。たとえば、すべてのコールが会議コールで、1 つの会議の平均参加者数が 10 人の場合、この設計では Unified CM コール処理ペアあたり最大 150 個の会議コールがあると仮定します。
- Unified CM コール処理ペアあたりのコール数/秒（CPS）が最大 15 個。
- この設計では、Jabber の連絡先ソースは Unified CM ユーザ データ サービス（UDS）ではなく、基本ディレクトリ統合（BDI）または拡張ディレクトリ統合（EDI）に基づいています。Unified CM UDS が連絡先ソースとして構成された場合、Unified CM コール処理ペアあたりの最大ユーザ数は 3,750 人に減少します。
- Unified CM コール処理ペアあたりの同時モバイルおよびリモート アクセス エンドポイントが最大 2,500 個。

この他、シスコ コラボレーション ソリューションに適用可能な容量制限や、『*Cisco Collaboration SRND*』および製品ドキュメントに記載されている容量制限も適用されます。次に例を示します。

- コンピュータ テレフォニー インテグレーション（CTI）：すべてのデバイスを CTI で使用できます（デバイスあたり最大 5 回線、同じ CTI デバイスを監視する J/TAPI アプリケーションが最大 5 個）。
- アナンシエータ：Unified CM コール処理ペアあたり 48 個。保留音（MoH）：コール処理ペアあたりの同時 MoH セッションが 250 個。アナンシエータや同時 MoH セッションの数が多い場合は、スタンドアロンの Unified CM サブスクライバを MoH サーバとして展開します。
- ゲートウェイ：クラスタあたり最大 2,100 個。
- ロケーションと地域：クラスタあたり最大 2,000 個。
- エクステンション モビリティ（EM）：Unified CM コール処理ノードあたりの EM ユーザが最大 250 人、または 2 つのアクティブ コール処理ノードにまたがるクラスタあたり 375 人。

IM and Presence のサイジング

IM and Presence については、簡易サイジングのガイダンスで最大 15,000 ユーザの展開に対応できます。IM and Presence サービスは、IM and Presence ノード ペアの追加によってより多くのユーザをサポートしますが、これはこの章で示す簡易サイジングのガイダンスの範囲外です。表 6-3 に、簡易サイジング展開を示します。展開環境内のユーザ数が表 6-3 に示す値の範囲外である場合は、これらの簡易サイジング展開を使用せずに、『*Cisco Collaboration SRND*』のサイジングに関する章および製品ドキュメントに記載されている通常のサイジング手順を実行してください。

表 6-3　　IM and Presence の簡易サイジング展開

展開サイズ	展開する IM and Presence ノード
2,000 人未満のユーザ	2,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペア
2,000 ～ 5,000 人のユーザ	5,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペア
5,000 ～ 15,000 人のユーザ	15,000 ユーザの OVA テンプレートを使用する 1 つの IM and Presence ペア

これらの OVA 仮想マシン設定テンプレートには、UC のパフォーマンスを最大限に引き出す CPU プラットフォーム（Cisco Business Edition 7000 など）が必要です。これらの OVA 仮想マシン設定テンプレートおよびプラットフォーム要件の詳細については、www.cisco.com/go/uc-virtualized にあるドキュメントを参照してください。

2 つの IM and Presence ノードは、一方のノードに障害が発生した場合に冗長性を提供するため、ペアとして展開されます。

SRST のサイジング

Survivable Remote Site Telephony（SRST）モードの Cisco サービス統合型ルータ（ISR）でサポートされる電話機および DN の数は、プラットフォームによって異なります。表 6-4 では、3 つのプラットフォームに限定して容量の例を示します。その他の SRST プラットフォームに関する情報（必要な DRAM とフラッシュ メモリの量を含む）については、次の場所にある SRST のドキュメントを参照してください。

http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cusrst/requirements/guide/srs10spc.html

表 6-4　　SRST のサイジング例

プラットフォーム	電話機の最大数	DN の最大数
Cisco 2901 サービス統合型ルータ	35	200
Cisco 3925 サービス統合型ルータ	730	1,000
Cisco 4451-X サービス統合型ルータ	1,500	2,500

会議

会議展開のサイジングは、主に TelePresence Server で必要となる同時接続の数を決定する作業です。次のような検討事項があります。

- 地理的なロケーション：Unified CM のサービスを提供する地域ごとに、会議専用のリソースを確保する必要があります。たとえば、Unified CM、TelePresence Server、およびその他のサーバをインストールする中央のロケーションを米国向けに 1 か所、EMEA 向けに 1 か所、それぞれ設置できます。
- TelePresence Server プラットフォームの選択：仮想化か非仮想化か
- TelePresence Server プラットフォームの容量
- TelePresence Conductor プラットフォームの容量
- 会議のタイプ：音声またはビデオ（あるいはその両方）。スケジュールされた会議またはスケジュールされていない会議（あるいはその両方）
- 会議のビデオ解像度：高品質の会議ほど多くのリソースを消費します。
- 大規模な会議の要件：オールハンズ ミーティングなど

地域ネットワークの会議メディアをできるだけ多く維持するため、会議リソースは一般に 1 つの地域でのみ使用されます。したがって、サイジングは地域単位で検討することができます。

会議ポートの使用ガイドライン

音声およびビデオ会議のサイジングは、お客様、お客様のユーザ ベース、およびお客様の会議手順に関する個別の詳細に大きく依存します。この項のガイドラインを会議展開のサイジングの基本として使用できますが、ユーザとポートの比率は展開環境と組織の要件によって大きく異なります。

表 6-5 に、会議リソース要件を計画する最初の段階で推奨される比率を示します。これらの数は、展開されるエンドポイントの機能、代替の音声会議（Cisco WebEx など）の可用性、および会議の作成と参加におけるユーザの快適度によって大きく変化します。最初に、次の式を使ってポートの要件を計算します。

- 音声ポート = 50 + (<number of users> / 9)
- ビデオ ポート = 8 + (<number of users> / 15)

表 6-5　　推奨される会議ポートの数

ユーザ数	音声ポートの数	ビデオ ポートの数
1,000	161	75
1,750	244	125
3,000	383	208
5,000	605	342
10,000	1,161	675

表 6-5 に示した数は、スケジュールされた会議とスケジュールされていない会議のどちらにも使用できます。スケジュールされた会議については、お客様が既存の使用状況データを使って、同時会議の使用量についてより明確な結論を出すことが期待されます。

お客様が行う会議のタイプを理解することで、必要なポートの数をより正確に特定できます。ポートの総数は次の式で計算できます。

ポートの総数 = <Average number of participants in a meeting> X <Concurrent meetings>

たとえば、ユーザが 3,000 人の場合、表 6-5 では 208 ポートを推奨しています。これにより、たとえば、会議あたり平均 3 人の参加者と 69 個の同時会議、または会議あたり平均 6 人の参加者と 34 個の同時会議に対応できます。推奨されるポート数をこのように評価することで、ポートの総数が展開環境に対して十分なものかどうかを簡単に判定できます。

検討すべきもう 1 つの重要な点は、予想される最大の会議サイズです。ほとんどの場合、最大の会議はオールハンズ ミーティング タイプです。たとえば、お客様のユーザ数が 1,000 人でも、全員参加のテレプレゼンス会議で 96 個のシステムを結合する必要がある場合は、推奨値の 75 ポートでは間に合いません。

画面ライセンスとポート容量

ビデオの解像度によって、ユーザのビデオ エクスペリエンスの品質と Cisco TelePresence Server がサポートできるビデオ接続の数が決まります。最適なエクスペリエンスを実現するため、最小解像度 720p および 30 フレーム/秒（fps）の高精細度（HD）ビデオ コールを有効にすることをお勧めします。組織のエンドポイントとネットワークの予算および機能によっては、HD ビデオ コールを使用できない場合もあります。表 6-6 に、ビデオ ストリーミング レートを 30 fps とした場合のビデオ品質に基づく TelePresence Server のポート容量を示します。表には示していませんが、画面ライセンスあたりの音声ポート数は 52 個で、TelePresence Server ごとに最大 200 個の音声ポートがサポートされます。

表 6-6　　ビデオ品質に基づく TelePresence Server のポート容量

画面ライセンス[1]	1080p ポート[2]	720p ポート[3]	480p ポート[3]	360p ポート[3]
1	1	2	3	4
5	5	10	15	20
10	10	20	30	40
20	20	40	60	80
48	48	96	144	192

1. 1 つの TelePresence Server に展開できる画面ライセンスの数は、プラットフォームによって異なります。
2. 最大解像度 720p および 15 fps で別のコンテンツ チャネルを共有すると仮定します。
3. 最大解像度 720p および 5 fps で別のコンテンツ チャネルを共有すると仮定します。

（注）　Cisco TelePresence Conductor および TelePresence Server では、1 つの会議リソースで解像度の制限が異なる複数の同時会議をホストできます。TelePresence Server を 1 つの解像度専用にする必要はありません。

表 6-6 を見てわかるように、必要なビデオ品質は TelePresence Server で消費されるリソースの量に直接影響し、結果として展開に必要な TelePresence Server の数にも直接影響します。

TelePresence Server プラットフォームのサイジング

Cisco TelePresence Server は、会議のサポートや拡張性が異なる複数のモデルおよびプラットフォームで使用可能です。表 6-7 に、企業展開で推奨される TelePresence Server プラットフォームと、関連するポート容量の一部を示します。詳細や、その他の TelePresence Server プラットフォーム、またはその他のビデオおよびデータ チャネルの解像度については、次の場所にある『*Cisco TelePresence Data Sheet*』を参照してください。

http://www.cisco.com/c/en/us/products/conferencing/telepresence-server/datasheet-listing.html

表 6-7　　TelePresence Server プラットフォームと容量

TelePresence Server プラットフォーム[1]	クラスタ サポート	HD 1080p ポートの容量[2]	HD 720p ポートの容量[3]	SD 480p ポートの容量[3]	SD 360p ポートの容量[3]
Multiparty Media 400v	なし	14	28	42	56
Telepresence Server MSE 8710	あり、最大 4 台の 8710 をクラスタ化可能。	ブレードあたり 12。 クラスタあたり最大 48。	ブレードあたり 24。 クラスタあたり最大 97。	ブレードあたり 36。 クラスタあたり最大 146。	ブレードあたり 48。 クラスタあたり最大 195。

1. TelePresence Server は、任意の音声コーデックを使用するスタンドアロン展開またはクラスタの音声接続を最大 200 個サポートします。
2. 解像度 720p および 15 フレーム/秒（fps）でコンテンツを共有すると仮定します。
3. 解像度 720p および 5 フレーム/秒（fps）でコンテンツを共有すると仮定します。

他にも留意すべき事項があります。次に例を示します。

- TelePresence Server は、スタンドアロン サーバまたはクラスタのコールを最大 200 個サポートし、各会議で最大 104 個のコールをサポートします。
- 画面ライセンスは、単一ユニットで購入し、各デバイスにそのデバイスでサポートされる最大数まで適用することができます。

TelePresence Conductor のサイジング

スケジュールされていない会議用の TelePresence Server の総数は、TelePresence Conductor の容量によって制限されます。表 6-8 に、TelePresence Conductor の容量を示します。

表 6-8　　TelePresence Conductor の容量

OVA テンプレート	TelePresence Server の総数	すべての TelePresence Server の同時参加者の総数
小規模 OVA テンプレート	30	50
大規模 OVA テンプレートまたはアプライアンス	30	2,400

クラスタリングでは高可用性のみが提供されます。サポートできる会議ブリッジや同時コールの総数は増えません。

展開の規模が 1 つの TelePresence Conductor クラスタの容量を超える場合は、追加の独立した TelePresence Conductor クラスタを作成して、そこに TelePresence Server を追加し続けることができます。

独立した TelePresence Conductor クラスタは、地域の Unified CM クラスタごとに使用する必要があります。このマニュアルのトポロジ例（コール制御の章を参照）では、TelePresence Conductor クラスタが米国の Unified CM クラスタ用に 1 つ用意され、EMEA の Unified CM クラスタ用にもう 1 つ用意されます。

コラボレーション エッジ

この項では、コラボレーション エッジの 2 つの主要コンポーネントである Cisco Expressway と Cisco Unified Border Element のサイジングについて説明します。

Cisco Expressway のサイジング

Cisco Expressway の簡易サイジングおよびライセンスのガイダンスは、少数の設定（2、3、または 6 ノードのクラスタ）のみを対象としています。このマニュアルでは説明しませんが、他にも可能な設定があります。詳細については、Cisco Expressway の製品ドキュメントを参照してください。

表 6-9 に、1 つのノードによってある時点で処理できる最大容量を示します。

表 6-10 に、簡易サイジングおよびライセンス展開用に推奨されるクラスタ容量を示します。すべての展開モデルが冗長性に対応していることに注意してください。2 または 3 ノードのクラスタでは、1 つのノードに障害が発生してもクラスタ容量やライセンス容量に影響しません（N+1 冗長性）。6 ノードのクラスタでは、2 つのノードに障害が発生してもクラスタ容量やライセンス容量に影響しません（N+2 冗長性）。

モバイルおよびリモート アクセスにはライセンスは特に必要ありませんが、Business-to-Business（B2B）コミュニケーションにはリッチ メディアのライセンスが必要です。リッチ メディア セッション形式のライセンスは、Expressway クラスタ全体で共有されます。クラスタ内の各 Expressway ノードに割り当てられたリッチ メディア セッションは、クラスタ内のすべてのノードで共有されるクラスタ データベースに供与されます。このモデルでは、いずれか 1 つの Expressway ノードが表 6-9 に示した物理的な容量よりも多くのライセンスを保持できます。N+1 および N+2 冗長性モデルをサポートするには、クラスタ内のリッチ メディア セッションの総数がクラスタ内の残りの N ノードの物理的な容量を超えないようにする必要があります。

クラスタ容量、ライセンス容量、および冗長性レベルの関係をさらに理解するため、次の例では、中規模 OVA テンプレートを使用して通常動作中およびフェールオーバー後のビデオ容量を分析します。

> ノードあたりの最大ビデオ コール容量は 150 セッションです。回復力のない展開における 2 ノードのクラスタでは、クラスタのビデオ コール容量は 300 ですが、1 つのノードに障害が発生した場合はその半分に減少します。推奨される高可用性の 2 ノード クラスタでは、2 ノードのいずれかに障害が発生した場合に回復力を提供し、クラスタ容量を維持するため、ビデオ セッション容量が 150 に制限されます。通常動作中は、クラスタ全体でビデオ コールの負荷が分散されます。Business-to-Business（B2B）コミュニケーションでは、リッチ メディア セッションのライセンスがクラスタ全体で共有されます。1 つのノードに障害が発生すると、ライセンス共有によって 150 個のクラスタ ビデオ セッションのすべてを処理するためのライセンスが残りのノードに供与されます。ノードのビデオセッション容量も 150 であるため、残りのノードは 150 個のビデオ セッションをすべて処理でき、これによってクラスタ容量が維持されます。

表 6-9　Expressway ノードの容量

OVA テンプレート	ノードあたりのモバイルおよびリモート アクセスのプロキシ登録数[1]	ノードあたりのビデオ コール容量	ノードあたりの音声専用コール容量
中規模 OVA テンプレートによる仮想マシンまたはアプライアンス CE500	2,500	150	300
大規模 OVA テンプレートによる仮想マシンまたはアプライアンス CE1000	2,500	500	1,000

1. プロキシ登録に関する考慮事項は、モバイルおよびリモート アクセスにのみ適用され、Business-to-Business（B2B）コミュニケーションには適用されません。

表 6-10　Cisco Expressway の簡易サイジング展開と関連するクラスタ容量

展開モデル	Expressway クラスタの展開	冗長性モデル	クラスタあたりのモバイルおよびリモート アクセスのプロキシ登録数[1]	クラスタあたりのビデオ コール容量	クラスタあたりの音声専用コール容量
中規模 OVA テンプレートによる仮想マシンまたはアプライアンス CE500					
展開 1	2 ノード	N+1	2,500	150	300
展開 2	3 ノード	N+1	5,000	300	600
展開 3	6 ノード	N+2	10,000	600	1,200
大規模 OVA テンプレートによる仮想マシンまたはアプライアンス CE1000					
展開 4	2 ノード	N+1	2,500	500	1,000
展開 5	3 ノード	N+1	5,000	1,000	2,000
展開 6	6 ノード	N+2	10,000	2,000	4,000

1. プロキシ登録に関する考慮事項は、モバイルおよびリモート アクセスにのみ適用され、Business-to-Business（B2B）コミュニケーションには適用されません。

（注） 大規模 OVA テンプレートは、限られたハードウェアでのみサポートされます。詳細については、http://www.cisco.com/go/uc-virtualized のドキュメントを参照してください。

表 6-10 に示した Expressway の簡易サイジング展開には、次の仮定条件が適用されます。

- すべてのビデオ コールが暗号化されています。すべてのビデオ コールの平均コール レートは 768 kbps です。たとえば、ビデオ コールの半分が 384 kbps で、残りの半分が 1152 kbps です。
- すべての音声コールが暗号化され、すべての音声コールの平均帯域幅は 64 kbps です。
- 中規模 OVA テンプレートを使った仮想マシンまたは CE500 アプライアンスでは、コール レートはノードあたり最大 5 コール/秒（cps）です。
- 大規模 OVA テンプレートを使った仮想マシンまたは CE1000 アプライアンスでは、コール レートはノードあたり最大 10 コール/秒（cps）です。

Cisco Expressway をクラスタ化する場合は、次のガイドラインが適用されます。

- Expressway クラスタは最大 6 ノードをサポートします（クラスタ容量はノード容量の最大 4 倍）。
- Expressway-E ノードと Expressway-C ノードは別個にクラスタ化されます。Expressway-E クラスタは Expressway-E ノードのみで構成され、Expressway-C クラスタは Expressway-C ノードのみで構成されます。
- Expressway のピアは、Expressway-E クラスタと Expressway-C クラスタで同じ数だけ展開する必要があります。たとえば、3 ノードの Expressway-E クラスタは、3 ノードの Expressway-C クラスタとともに展開する必要があります。
- Expressway-E クラスタと Expressway-C クラスタの各ペア間およびペア内のすべてのノードの容量は、同じである必要があります。たとえば、Expressway-E クラスタ内または対応する Expressway-C クラスタ内のノードが中規模 OVA テンプレートを使用している場合は、大規模 OVA テンプレートを使用する Expressway-E ノードを展開してはいけません。
- Expressway-E クラスタと Expressway-C クラスタのペアは、ノード容量がすべてのノードで同じであるかぎり、アプライアンスで実行されるノードまたは仮想マシンとして実行されるノードを組み合わせて構成できます。
- 複数の Expressway-E および Expressway-C クラスタを展開して、容量を増やすことができます。

Expressway に詳細については、次の場所にある『*Cisco Expressway Administrator Guide*』を参照してください。

http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-maintenance-guides-list.html

Cisco Expressway のサイジング例

ある企業では、8,000 人のユーザがいて、平均 2,000 人のユーザが常に出張しています。モバイルユーザの 80% がモバイルおよびリモート アクセスを必要としています。このケースでは、1,600 人（2,000 人の 80%）が同時登録できるように Expressway をサイジングする必要があります。

さらに、モバイル ユーザの 10% が同時にコールを行います。これらのユーザの 5% が Expressway 経由でコールし、残りの 5% が携帯電話ネットワーク経由でコールするため、Expressway に対する同時コール数は 80（1,600 の 5%）です。

社内ネットワークでは、ユーザの 1% が同時に Business-to-Business（B2B）コールを行います。これによって、60 個（（8,000 - 2,000）の 1%）のコールが追加されます。

このケースでは、1,600 個の同時登録と 140 個の同時コール（80 + 60）をサポートするようにクラスタをサイジングする必要があります。

表 6-9 に示すように、中規模 OVA テンプレートは最大 150 個の同時コールと 2,500 個の同時登録をサポートします。したがって、中規模 OVA テンプレートを使用する 2 ノードで構成される Expressway-C クラスタと、やはり中規模 OVA テンプレートを使用する 2 ノードで構成される Expressway-E クラスタを展開することができます。表 6-10 の展開 1 で示したように、各 Expressway サーバ ノードは 1,600 個の登録と 140 個のコールをすべて同時に管理できます。クラスタ化が必要とされる理由は、2 つの Expressway ノードのいずれかが停止した場合に、もう一方のノードがすべてのトラフィックを処理できるためです。通常の状況では、Expressway-C クラスタと Expressway-E クラスタの 2 つのノード間でコールと登録の負荷が分散されます。

この例では、しばらくすると Business-to-Business（B2B）コールが 1% から 2% に増加します。そこで、140 個ではなく 200 個（80 + 120）の同時コールに対応する必要があります。中規模 OVA テンプレートの最大処理量は 150 コールなので、この場合は大規模なクラスタを展開する必要があります。表 6-10 に示すように、展開 2 によって、1 つのサーバに障害が発生しても 300 個の同時コールに対応できます。したがって、この例の管理者は、Expressway-C および Expressway-E クラスタにもう 1 つの中規模 OVA ノードを追加して、クラスタあたり合計 3 ノードを展開します。

Cisco Unified Border Element のサイジング

Cisco Unified Border Element は広範囲のシスコ ルーティング プラットフォームでサポートされます。これには、Cisco 2900、3900、および 4400 シリーズのサービス統合型ルータ（ISR）や Cisco 1000 シリーズのアグリゲーション サービス ルータ（ASR）が含まれます。Cisco Unified Border Element は、次のプラットフォームで冗長性も提供します。

- Cisco ISR プラットフォームでは、アクティブ コールのメディア保護を含むボックスツーボックス冗長性を提供できます。
- Cisco ASR プラットフォームでは、アクティブ コールのメディアとシグナリングの保護（ステートフル フェールオーバー）を含むインボックス冗長性またはボックスツーボックス冗長性を提供できます。

表 6-11 では、いくつかのプラットフォームについて容量の例を示します。その他のプラットフォームや、必要な DRAM とフラッシュ メモリの量などの詳細については、次の場所にある『*Cisco Unified Border Element Data Sheet*』および『*Cisco Unified Border Element and Gatekeeper Ordering Guide*』を参照してください。

http://www.cisco.com/c/en/us/products/unified-communications/unified-border-element/datasheet-listing.html

表 6-11　　Cisco Unified Border Element の容量の例

プラットフォーム	SIP トランク セッションの最大数
Cisco 2901 サービス統合型ルータ	100
Cisco 3925 サービス統合型ルータ	800
Cisco 4451-X サービス統合型ルータ	4,000
Cisco 1004 および 1006 アグリゲーション サービス ルータ	16,000

Cisco Unified Border Element のサイジング例

ある企業に 8,000 人のユーザがいます。最繁時にはユーザの 10% が同時にコールを行います。ユーザの 8% は外部の接続先にコールし、残りのユーザは内線コールに関与しています。電気通信業者とこの企業はすべてのコールに G.711 を使用できることで合意しているため、トランスコードは必要ありません。この展開では、640 個の SIP セッション（8,000 人の 8%）が必要です。表 6-11 に示すように、Cisco 3925 ISR で最大 800 個のセッションをサポートできます。したがって、この例では Cisco Unified Border Element ソフトウェアをインストールした 2 台の Cisco 3925 ISR を選択し、冗長性を提供するため 1 台をアクティブ、もう 1 台をスタンバイとして使用します。

コア アプリケーション

この項では、コア アプリケーションの章で説明したアプリケーション（つまり、Cisco Unity Connection および Cisco TelePresence Management Suite（TMS））のサイジングについて説明します。

Cisco Unity Connection

Cisco Unity Connection 導入プロセスの項で説明したように、この設計で推奨される Unity Connection の展開は、アクティブ/アクティブ モードのパブリッシャ 1 台とサブスクライバ 1 台で構成されます。

このガイドでは、Unity Connection のユーザ数に応じた 3 つの簡易サイジング展開について説明します。これらの展開を表 6-12 に示します。Unity Connection には他にも可能な展開がありますが、このガイドでは説明しません。その他の可能な展開については、『*Cisco Collaboration SRND*』および製品ドキュメントを参照してください。

表 6-12　　Cisco Unity Connection の簡易サイジング展開

展開サイズ	アクティブ/アクティブで展開する Unity Connection ノード
1,000 ユーザ	1,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア
1,000 ～ 5,000 ユーザ	5,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア
5,000 ～ 10,000 ユーザ	10,000 ユーザの OVA テンプレートを使用する 1 つの Unity Connection ペア

Cisco Unity Connection の仮定条件

OVA テンプレートの制限を超えないようにする必要があります。たとえば、5,000 ユーザの OVA テンプレートには、G.711 で 200 ポート、G.722 で 50 ポートの制限があります。OVA テンプレートの制限の詳細については、次を参照してください。

- 次の場所にある Cisco Unity Connection の仮想化に関する情報
  http://docwiki.cisco.com/wiki/Virtualization_for_Cisco_Unity_Connection
- 次の場所にある Cisco Unity Connection の製品ドキュメント
  http://www.cisco.com/c/en/us/support/unified-communications/unity-connection-version-10-x/model.html

ボイスメールの保存に必要なストレージ量を検討することも重要です。メッセージ ストレージは、仮想ディスクのサイズによって異なります。たとえば、G.711 コーデックを使用するメッセージのストレージは 5,000 ユーザの OVA テンプレートでおよそ 137,000 分であり、これは 200 GB の vDisk 1 台で定義されます。10,000 ユーザの OVA テンプレートを使用する場合は、異なるメッセージ ストレージ要件に対応するために別の vDisk サイズを使用できます。詳細については、『*Cisco Unity Connection Supported Platforms List*』を参照してください。

Cisco TelePresence Management Suite（TMS）

Cisco TMS については、表 6-13 に示す 2 つの簡易サイジング展開をお勧めします。TMS には他にも可能な展開がありますが、このガイドでは説明しません。たとえば、TMS、TMSPE、TMSXE、および Microsoft SQL のすべてのコンポーネントを同じ仮想マシンに配置する単一サーバ展開については、冗長性が提供されないため、ここでは説明しません。

表 6-13 に示した 2 つの展開では、高可用性が提供されます。冗長ノードは、拡張性ではなく回復力を確保するために展開されます。プライマリ ノードとバックアップ ノードに単一の仮想 IP アドレスを提供するロード バランサも必要です。

表 6-13　Cisco TMS の簡易展開と容量

展開モデル	展開	Cisco TMS	Cisco TMSXE	Cisco TMSPE
通常の展開 （2 vCPU の OVA テンプレート）	合計 2 ノード： 各ノードに TMS、TMSPE、および TMSXE を展開 Microsoft SQL 用のサーバを追加	制御対象システム（TMS に追加されるスケジューリング用のエンドポイント）が最大 200 個 同時参加者が最大 100 人 同時進行するスケジュール済み会議が最大 50 個	Microsoft Exchange で予約可能なエンドポイントが最大 50 個	Collaboration Meeting Room（CMR）が最大 1,000 個
大規模な展開 （4 vCPU の OVA テンプレート）	合計 4 ノード： 2 ノードに TMS と TMSPE を展開し、残りの 2 ノードに TMSXE のみを展開 Microsoft SQL 用のサーバを追加	制御対象システム（TMS に追加されるスケジューリング用のエンドポイント）が最大 5,000 個 同時参加者が最大 1,800 人 同時進行するスケジュール済み会議が最大 250 個	Microsoft Exchange で予約可能なエンドポイントが最大 1,800 個	Collaboration Meeting Room（CMR）が最大 48,000 個

Cisco TMS のパフォーマンスとスケーリングに影響を与えるその他の要因として、次が挙げられます。

- Cisco TMS Web インターフェイスにアクセスするユーザの数。
- スケジュールまたは監視されている会議の同時開催。
- 複数の拡張機能またはカスタム クライアントによる Cisco TMS Booking API（TMSBA）の同時使用。ブッキングのスループットは、Cisco TMS の [新しい会議（New Conference）] ページを含むすべてのスケジューリング インターフェイスで共有されます。

Cisco TMS のサイジングの詳細については、次の場所にある『*Cisco TelePresence Management Suite Installation and Upgrade Guide*』を参照してください。

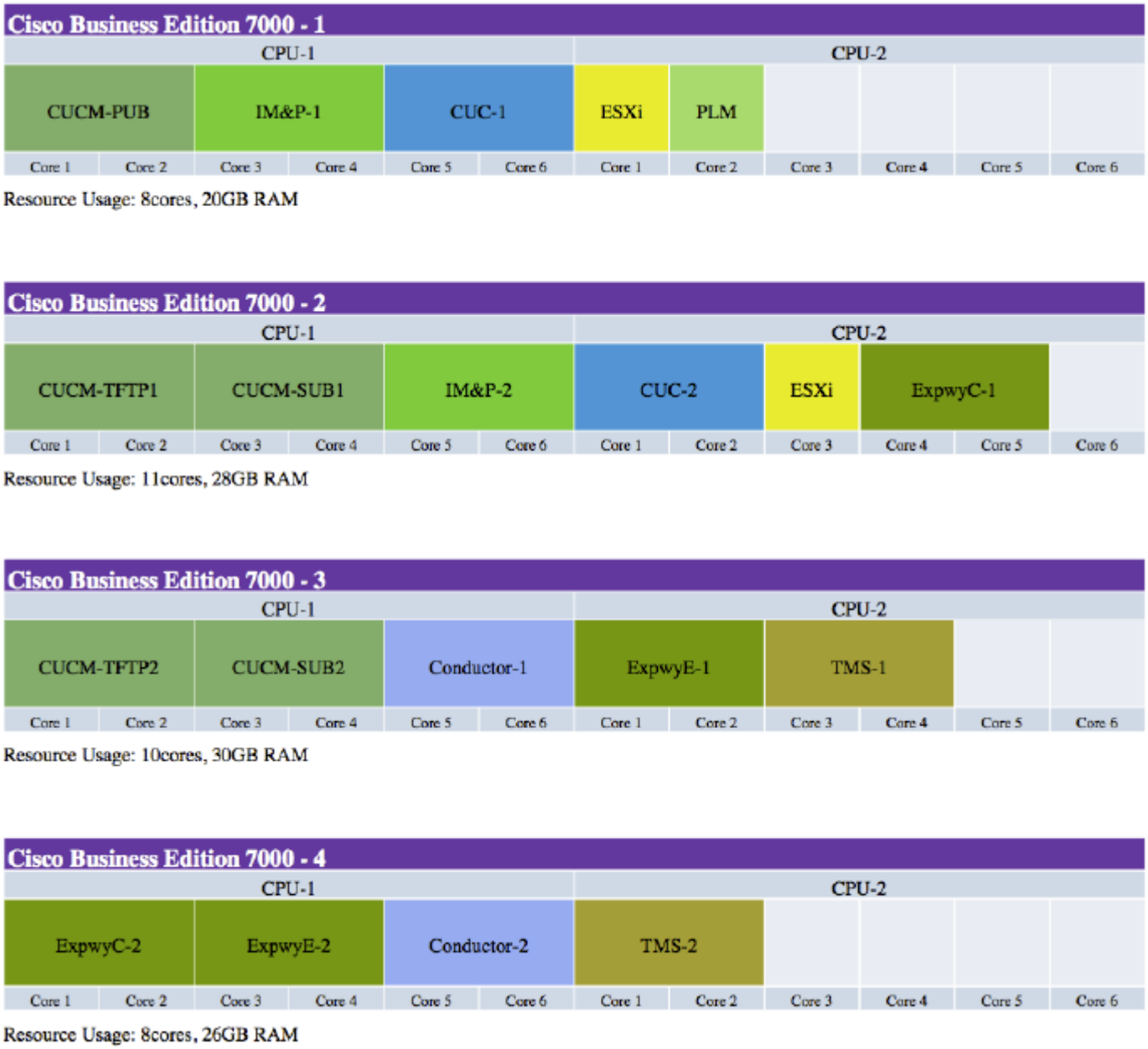
http://www.cisco.com/c/en/us/support/conferencing/telepresence-management-suite-tms/products-installation-guides-list.html

仮想マシンの配置とプラットフォーム

仮想化を使用して展開されるシスコ コラボレーション製品については、展開をサイジングした後の次のステップとして、Cisco Unified Computing System（UCS）サーバに仮想マシンをまとめて配置する方法を決定します。これにより、ソリューションに必要な UCS サーバの数が最終的に決定します。このプロセスは、Collaboration Virtual Machine Placement Tool（VMPT）を使用して実行します。このツールは、cisco.com へのログインが必要になりますが、http://www.cisco.com/go/vmpt から入手できます。

図 6-1 に、5,000 ユーザを含む展開に対する VMPT の使用例を示します。この例は、Cisco Business Edition 7000M が展開されていることを前提としています。TelePresence Server は、この例には含まれていませんが、Multiparty Media 400v や TelePresence Server MSE 8710 などのプラットフォームで展開できます。

図 6-1　　VMPT を使った仮想マシンの配置例



通常は、VMPT を使用するのに加えて、仮想マシンの配置を検証するため、展開環境が次のドキュメントに記載されている共存要件をすべて満たしているかどうか確認することをお勧めします。

http://docwiki.cisco.com/wiki/Unified_Communications_Virtualization_Sizing_Guidelines#Application_Co-residency_Support_Policy

主な配置と共存のルールは次のとおりです。

- オーバーサブスクリプションをしない:すべての仮想マシンの仮想ハードウェアと物理ハードウェアが 1 対 1 でマッピングされている必要があります。たとえば、CPU については、ハイパースレッディングが有効になっている場合でも、仮想ハードウェアと物理ハードウェアが 1 対 1 でマッピングされている必要があります。
- Cisco Unity Connection では、Unity Connection がインストールされている各 ESXi ホスト上の ESXi スケジューラ用に予備の物理コアを予約する必要があります。
- このガイドで説明しているほとんどのアプリケーションは、サードパーティ製アプリケーションとの共存をサポートしているため、同じ UCS サーバにインストールできます。ただし、サードパーティ製アプリケーションとの共存では、サードパーティ製アプリケーションがシスコ コラボレーション アプリケーションと同じルールに従う必要があります。たとえば、サードパーティ製アプリケーションをシスコ コラボレーション アプリケーションと同じホストにインストールした後は、そのサードパーティ製アプリケーションで CPU のオーバーサブスクリプションがサポートされない、Unity Connection の展開時に ESXi スケジューラ用に物理コアを予約する必要がある、などです。Cisco Business Edition プラットフォームでは、共存オプションの一部が ESXi ライセンスで指定されます。たとえば、Cisco UC Virtualization Hypervisor および Foundation では、共存できるサードパーティ製アプリケーションの数に制限があります。

冗長性の考慮

ハードウェア プラットフォームに高い冗長性がある場合でも、ハードウェアの冗長性を考慮することをお勧めします。たとえば、図 6-1 の例で示すように、プライマリ アプリケーションとバックアップ アプリケーションの仮想マシンを同じ UCS サーバに展開しないでください。代わりに、ホストの障害発生時に冗長性を提供するため、プライマリとバックアップの仮想マシンを異なるサーバに展開してください。

プラットフォーム

仮想化を使用して展開される製品には、Cisco Business Edition 7000 が最適なソリューションとして考えられます。このソリューションは、簡単に発注して展開することができ、Cisco UCS サーバ ハードウェアとハイパーバイザのライセンスを含んでいます。VMware vSphere Hypervisor (ESXi) が事前にインストールされています。Business Edition 7000 には、シスコ コラボレーション ソフトウェア セットも事前にロードされています。