Cisco Unified Communication ソリューション リファレンス ネットワーク デザイン（SRND）

Cisco Unified CallManager Release 5.0
2006 年 4 月

Text Part Number: OL-10030-02-J

CONTENTS

このマニュアルについて xxiii

改訂の履歴 xxiv

技術情報の入手方法 xxv

Cisco.com xxv

マニュアルの発注方法（英語版） xxv

シスコシステムズマニュアルセンター xxv

テクニカル サポート xxvi

Cisco Technical Support Web **サイト** xxvi

Japan TAC Web **サイト** xxvi

サービス リクエストの発行 xxvii

サービス リクエストのシビラティの定義 xxvii

補足資料および情報へのアクセス xxviii

CHAPTER 1 **概要** 1-1

Cisco Unified Communications **の概要** 1-3

Cisco IP **ネットワーク インフラストラクチャ** 1-4

QoS 1-4

コール処理エージェント 1-5

通信エンドポイント 1-5

会議、メッセージング、およびコラボレーション機能 1-6

アプリケーション 1-7

セキュリティ 1-8

CHAPTER 2 **IP テレフォニー配置モデル** 2-1

単一サイト 2-3

単一サイト モデルの利点 2-4

単一サイト モデルのベスト プラクティス 2-5

集中型コール処理を使用するマルチサイト WAN 2-6

集中型コール処理モデルのベスト プラクティス 2-8

リモート サイトのサバイバビリティ（呼処理の継続） 2-8

集中型コール処理のバリエーションとしての Voice Over the PSTN 2-11

AAR **を使用する** VoPSTN 2-13

ダイヤル プランを使用する VoPSTN 2-14
分散型コール処理を使用するマルチサイト WAN 2-15
分散型コール処理モデルの利点 2-17
分散型コール処理モデルのベスト プラクティス 2-17
分散型コール処理モデルのコール処理エージェント 2-18
IP WAN を介したクラスタ化 2-19
WAN の考慮事項 2-19
クラスタ内通信 2-20
サブスクライバ サーバ間のフェールオーバー 2-21
Cisco Unified CallManager パブリッシャ 2-21
コール詳細レコード（CDR） 2-22
遅延のテスト 2-22
エラー率 2-22
トラブルシューティング 2-23
ローカル フェールオーバー配置モデル 2-23
ローカル フェールオーバーに対する Cisco Unified CallManager のプロビジョニング 2-25
ローカル フェールオーバー用のゲートウェイ 2-26
ローカル フェールオーバー用のボイスメール 2-26
ローカル フェールオーバーに対する Music On Hold とメディア リソース 2-26
リモート フェールオーバー配置モデル 2-27
U. S. Section 508 準拠についての設計上の考慮事項 2-28

CHAPTER 3 ネットワーク インフラストラクチャ 3-1
LAN インフラストラクチャ 3-4
高可用性のための LAN 設計 3-4
キャンパス アクセス レイヤ 3-4
キャンパス ディストリビューション レイヤ 3-7
キャンパス コア レイヤ 3-10
ネットワーク サービス 3-11
Power over Ethernet（PoE） 3-21
カテゴリ 3 ケーブリング 3-21
IBM タイプ 1A および 2A ケーブリング 3-22
LAN の QoS 3-23
トラフィック分類 3-24
インターフェイス キューイング 3-26
帯域幅のプロビジョニング 3-26
QoS が使用されない場合の IP コミュニケーションの障害 3-27

WAN インフラストラクチャ 3-28
WAN の設計と設定 3-28
配置上の考慮事項 3-28
保証帯域幅 3-30
ベストエフォート型の帯域幅 3-30
WAN の QoS 3-31
トラフィックの優先順位 3-32
リンク効率手法 3-34
トラフィック シェーピング 3-36
リソース予約プロトコル（RSVP） 3-38
RSVP の原理 3-38
WAN ルータでの RSVP と QoS 3-41
RSVP のアプリケーション ID 3-45
RSVP 設計上のベスト プラクティス 3-47
帯域幅のプロビジョニング 3-48
ベアラ トラフィック用のプロビジョニング 3-49
RSVP を使用するベアラ トラフィックに関する追加の考慮事項 3-52
集中型コール処理を使用したコール制御トラフィック用のプロビジョニング 3-56
分散型コール処理を使用したコール制御トラフィック用のプロビジョニング 3-61
無線 LAN インフラストラクチャ 3-62
WLAN の設計と設定 3-62
無線インフラストラクチャに関する考慮事項 3-62
無線 AP の設定と設計 3-65
無線セキュリティ 3-67
WLAN の QoS 3-68
トラフィック分類 3-68
インターフェイス キューイング 3-69
帯域幅のプロビジョニング 3-70

CHAPTER 4 ゲートウェイ 4-1
Cisco ゲートウェイの概要 4-2
Cisco アクセス アナログ ゲートウェイ 4-2
Cisco アクセス デジタル トランク ゲートウェイ 4-2
ゲートウェイの選択 4-3
コア機能要件 4-3
ゲートウェイ プロトコル 4-3
ゲートウェイ プロトコルとコア機能要件 4-6

DTMF リレー 4-6
補足サービス 4-8
Cisco Unified CallManager の冗長性 4-11
サイト固有のゲートウェイ要件 4-13
QSIG サポート 4-21
FAX とモデムのサポート 4-22
FAX パススルーと Cisco FAX リレーに対するゲートウェイ サポート 4-22
モデム パススルーに対するゲートウェイ サポート 4-23
サポートされるプラットフォームと機能 4-24
プラットフォーム プロトコルのサポート 4-25
ゲートウェイの組み合せと機能の相互運用性 4-26
類似ゲートウェイ間の機能サポート 4-27
ゲートウェイ設定例 4-28
Cisco IOS ゲートウェイの設定 4-28
Cisco VG248 の設定 4-29
Cisco IOS ゲートウェイ用の Cisco Unified CallManager 設定 4-29
FAX とモデム パススルー用のクロック ソーシング 4-30
T.38 FAX リレー 4-30
Named Service Event（NSE）を使用して制御されるゲートウェイ 4-31
H.245 または SDP（Session Description Protocol）による機能交換を使用して制御されるゲートウェイ 4-31
H.323 Annex D を使用したコール エージェント制御の T.38 4-33
ビデオ テレフォニー用のゲートウェイ 4-34
公衆網からの着信コールのルーティング 4-36
公衆網への発信コールのルーティング 4-37
自動代替ルーティング（AAR） 4-38
最低料金選択機能 4-40
ISDN B チャネル バインディング、ロールオーバー、およびビジーアウト 4-41
着信コール 4-41
発信コール 4-42
Cisco Unified CallManager でのゲートウェイの設定 4-42
コール シグナリング ポート番号 4-43
コール シグナリング タイマー 4-43
音声ゲートウェイ ベアラ機能 4-44

CHAPTER 5 Cisco Unified CallManager トランク 5-1
H.323 トランク 5-3
クラスタ間トランク（非ゲートキーパー制御） 5-3

クラスタ間トランク（ゲートキーパー制御） 5-3
H.225 トランク（ゲートキーパー制御） 5-4
ゲートキーパー トランクの冗長性、復元性、およびロード バランシング 5-4
メディア ターミネーション ポイントを使用する H.323 トランク 5-9
Cisco Unified CallManager における H.323 の動作 5-10
SIP トランク 5-13

CHAPTER 6 メディア リソース 6-1
音声インターフェイス 6-2
中複雑度モードと高複雑度モード 6-2
フレックス モード 6-3
音声インターフェイスの DSP リソース 6-3
オーディオ会議 6-8
オーディオ会議のリソース 6-8
トランスコーディング 6-11
トランスコーディング リソース 6-12
メディア ターミネーション ポイント（MTP） 6-14
ストリームの再パケット化 6-14
H.323 補足サービス 6-14
H.323 発信時の Fast Start 6-14
Named Telephony Event（RFC 2833） 6-14
Named Telephony Event がメディア ターミネーション ポイントを必要とする条件 6-15
SIP および H.323 ゲートウェイでの DTMF の設定 6-17
CTI ルート ポイント 6-18
MTP リソース 6-18
Annunciator 6-20
Cisco RSVP Agent 6-22
Cisco IP Voice Media Streaming Application 6-22
ハードウェアおよびソフトウェアのキャパシティ 6-23
PVDM 6-23
Cisco 2800 および 3800 シリーズ プラットフォーム 6-24
ネットワーク モジュール 6-24
NM-HDV の DSP 要件の計算 6-25
一般的な設計ガイドライン 6-25
メディア リソース グループとメディア リソース グループ リスト 6-25
配置モデル 6-26
IP 公衆網アクセス 6-29

CHAPTER 7 **Music on Hold** 7-1

MoH の基本的な配置 7-2

ユニキャストおよびマルチキャスト MoH 7-2

共存 MoH サーバとスタンドアロン MoH サーバ 7-3

MoH の固定ソースとオーディオ ファイル ソース 7-3

Cisco Unified CallManager クラスタに含まれる MoH サーバ 7-5

基本的な MoH と MoH コール フロー 7-6

基本的な MoH 7-6

ユーザ保留とネットワーク保留 7-7

ユニキャストとマルチキャスト MoH コール フロー 7-9

MoH 設定上の考慮事項およびベスト プラクティス 7-10

コーデックの選択 7-10

マルチキャスト アドレッシング 7-10

MoH オーディオ ソース 7-11

複数の固定またはライブ オーディオ ソースの使用 7-11

同一 Cisco Unified CallManager クラスタ内のユニキャストとマルチキャスト 7-12

冗長性 7-13

QoS 7-13

MoH リソース用のハードウェアとキャパシティ プランニング 7-14

サーバ プラットフォームの最大同時セッション数 7-14

リソースのプロビジョニングとキャパシティ プランニング 7-15

MoH に対する IP テレフォニー配置モデルの影響 7-16

単一サイト キャンパス（すべての配置に関連） 7-16

集中型マルチサイト配置 7-16

コール アドミッション制御と MoH 7-17

支店ルータのフラッシュからのマルチキャスト MoH 7-18

分散型マルチサイト配置 7-21

WAN を介したクラスタ化 7-21

ユニキャストとマルチキャスト MoH コール フローの詳細 7-22

SCCP コール フロー 7-22

SIP コール フロー 7-25

CHAPTER 8 **コール処理** 8-1

Cisco Unified CallManager クラスタのガイドライン 8-2

ハードウェア プラットフォーム 8-2

Cisco Unified CallManager クラスタのサービス 8-4

クラスタ内通信 8-5

クラスタ内セキュリティ 8-6

パブリッシャ 8-7
コール処理サブスクライバ 8-7
TFTP サーバ 8-12
CTI Manager 8-13
IP Voice Media Streaming Application 8-13
音声アクティビティ検出 8-14
Cisco Unified CallManager のアプリケーション 8-14
Cisco Unified CallManager プラットフォームのキャパシティ プランニング 8-16
キャパシティの計算 8-17
Cisco CallManager キャパシティ ツール 8-18
ゲートキーパーの設計上の考慮事項 8-22
ハードウェア プラットフォームの選択 8-22
ゲートキーパーの冗長性 8-22
ホットスタンバイ ルータ プロトコル（HSRP） 8-23
ゲートキーパー クラスタリング（代替ゲートキーパー） 8-25
ディレクトリ ゲートキーパーの冗長性 8-29
Cisco Unified CallManager と CallManager Express の相互運用性 8-33
Cisco Unified CallManager および CME を SIP トランクで接続したマルチサイト IP テレフォニー配置 8-34
Cisco Unified CallManager と CME を H.323 トランクと IP-to-IP ゲートウェイで接続したマルチサイト IP テレフォニー配置 8-36

CHAPTER 9 コール アドミッション制御 9-1
ベスト プラクティスの概要 9-3
コール アドミッション制御の原理 9-4
トポロジ非対応コール アドミッション制御 9-4
トポロジ対応コール アドミッション制御 9-8
MPLS ネットワークの特別な考慮事項 9-12
コール アドミッション制御の要素 9-13
Cisco Unified CallManager の静的ロケーション 9-13
Cisco IOS ゲートキーパー ゾーン 9-16
Cisco Unified CallManager の RSVP 対応ロケーション 9-18
Cisco RSVP Agent のプロビジョニング 9-20
Cisco RSVP Agent の登録 9-22
RSVP ポリシー 9-25
静的ロケーションから RSVP コール アドミッション制御への移行 9-26
RSVP アプリケーション ID 9-29

RSVP 機能のある Cisco IOS Gatekeeper および IP-to-IP ゲートウェイ 9-30
中継ゾーン（Via-Zone）ゲートキーパー 9-31
設計上のベスト プラクティス 9-32
冗長性 9-33
設定のガイドライン 9-34
コール アドミッション制御の設計 9-38
単純なハブアンドスポーク トポロジ 9-38
集中型の Cisco Unified CallManager 配置 9-39
分散型の Cisco Unified CallManager 配置 9-40
2 層ハブアンドスポーク トポロジ 9-42
集中型の Cisco Unified CallManager 配置 9-43
分散型の Cisco Unified CallManager 配置 9-45
単純な MPLS トポロジ 9-46
集中型の Cisco Unified CallManager 配置 9-48
分散型の Cisco Unified CallManager 配置 9-50
汎用トポロジ 9-52
集中型の Cisco Unified CallManager 配置 9-53
分散型の Cisco Unified CallManager 配置 9-56

CHAPTER 10 ダイヤル プラン 10-1
プランニングの考慮事項 10-3
ダイヤル パターン認識 10-3
オンネットとオフネットのダイヤリング 10-4
省略ダイヤリング 10-4
内線ダイヤリングの重複の防止 10-5
ダイヤリング ストリングの長さ 10-5
定型オンネット ダイヤル プラン 10-5
可変長のオンネット ダイヤル プラン 10-7
オンネットとオフネットのアクセス コード 10-8
事前の計画 10-8
ダイヤル プランの要素 10-9
SCCP 電話機でのユーザ入力 10-9
タイプ A の SIP 電話機でのユーザ入力 10-10
タイプ B の SIP 電話機でのユーザ入力 10-12
SIP ダイヤル規則 10-14
Cisco Unified CallManager におけるコール ルーティング 10-16
ルート パターン 10-18
ルート リスト 10-21

ルート グループ 10-21
ルート グループ デバイス 10-22
Cisco Unified CallManager におけるコール特権 10-22
パーティション 10-23
コーリング サーチ スペース 10-24
Cisco Unified CallManager における番号操作 10-27
Automated Alternate Routing 10-28
宛先公衆網番号の確立 10-29
必要なアクセス コードの付加 10-29
適切なダイヤル プランおよびルートの選択 10-30
同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項 10-30
エクステンション モビリティ 10-31
ハント リストと回線グループ 10-33
ハント パイロット 10-36
ハント リスト 10-37
回線グループ 10-37
回線グループ デバイス 10-38
時間帯ルーティング 10-38
H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング 10-39
ゲートキーパーを使用する Cisco IOS でのコール ルーティング 10-42
集中型ゲートキーパー設定 10-47
分散型ゲートキーパー設定 10-49
ディレクトリ ゲートキーパーを使用した分散型ゲートキーパー設定 10-50
H.323 ダイヤル ピアを使用する Cisco IOS のコール特権 10-52
H.323 ダイヤル ピアを使用する Cisco IOS での番号操作 10-55
設計上の考慮事項 10-57
マルチサイト配置用の設計ガイドライン 10-57
ダイヤル プラン アプローチの選択 10-60
定型オンネット ダイヤル プランの配置 10-62
クラスタ内でのサイト間コール 10-63
発信公衆網コールと IP WAN コール 10-63
緊急コール 10-63
着信コール 10-63
ボイスメール コール 10-64
分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置 10-64
クラスタ内でのサイト間コール 10-67

発信公衆網コールと IP WAN コール 10-67
着信コール 10-69
ボイスメール コール 10-69
フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置 10-70
クラスタ内でのサイト間コール 10-72
発信公衆網コールと IP WAN コール 10-73
着信コール 10-76
ボイスメール コール 10-76
サイト コードを使用しない配置に関する特別な考慮事項 10-76
Cisco Unified CallManager 5.0 を使用する電話機でのダイヤル パターン認識の配置 10-78
従来のアプローチによる Cisco Unified CallManager のサービス クラスの構築 10-80
回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築 10-84
回線 / デバイス アプローチのガイドライン 10-88
回線 / デバイス アプローチにおけるエクステンション モビリティの考慮事項 10-89
H.323 を使用している Cisco IOS でのサービス クラスの構築 10-92
コール カバレッジの配置 10-96
マルチサイト集中型コール処理モデルへのコール カバレッジの配置 10-96
マルチサイト分散型コール処理モデルへのコール カバレッジの配置 10-98
ハント パイロットのスケーラビリティ 10-99

CHAPTER 11 緊急サービス 11-1
911 機能の計画 11-2
Public Safety Answering Point（PSAP） 11-2
911 ネットワーク サービス プロバイダー 11-2
適切な 911 ネットワークへのインターフェイス ポイント 11-3
インターフェイス タイプ 11-4
動的 ANI（トランク接続） 11-4
静的 ANI（回線接続） 11-6
緊急応答ロケーションのマッピング 11-6
緊急ロケーション識別番号のマッピング 11-7
非固定電話機の考慮事項 11-8
Cisco Emergency Responder 11-9
緊急コール ストリング 11-10
ゲートウェイの考慮事項 11-11

ゲートウェイの配置 11-11
ゲートウェイのブロック 11-11
応答監視 11-12
Cisco Emergency Responder の考慮事項 11-13
Cisco Unified CallManager と Emergency Responder とのバージョンの互換性 11-13
コール アドミッション制御ロケーションを超えたデバイス モビリティ 11-13
デフォルトの緊急応答ロケーション 11-13
ソフト クライアント 11-13
テスト コール 11-14
共用ディレクトリ番号への PSAP コールバック 11-14
マルチクラスタの考慮事項 11-14
単一の Cisco ER グループ 11-15
複数の Cisco ER グループ 11-16
Cisco ER クラスタ内の緊急コール ルーティング 11-19
Cisco ER クラスタリングのスケーラビリティの考慮事項 11-19
ALI フォーマット 11-20

CHAPTER 12 サードパーティ製のボイスメール設計 12-1
SMDI 12-2
Cisco Messaging Interface 12-2
Cisco VG248 12-3
FXS ポートを使用する場合の考慮事項 12-3
Digital Set Emulation 12-4
二重 PBX 統合 12-5
集中型ボイスメール 12-7
確実な接続解除監視 12-12
サードパーティ製ボイスメール統合の要約 12-12

CHAPTER 13 Cisco Unity 13-1
メッセージング配置モデル 13-3
単一サイト メッセージング 13-3
集中型メッセージング 13-3
分散型メッセージング 13-4
メッセージング フェールオーバー 13-4
メッセージング システム インフラストラクチャ コンポーネント 13-6
ポート グループ（分離統合） 13-7
帯域幅の管理 13-8

Cisco Unity および Unity Connection のネイティブ トランスコーディング動作 13-10
ボイスメール統合のための Cisco Unified CallManager SIP トランクの設定 13-11
Cisco Unified CallManager クラスタとの音声ポート統合 13-12
専用 Cisco Unified CallManager バックアップ サーバを使用する音声ポート統合 13-14
集中型メッセージングと集中型コール処理 13-15
分散型メッセージングと集中型コール処理 13-17
結合されたメッセージング配置モデル 13-19
集中型メッセージングと WAN を介したクラスタ化 13-21
分散型メッセージングと WAN を介したクラスタ化 13-23
Cisco Unity メッセージング フェールオーバー 13-25
Cisco Unity フェールオーバーと WAN を介したクラスタ化 13-26
集中型メッセージングと複数の Cisco Unified CallManager サーバ 13-27

CHAPTER 14 Cisco Unified MeetingPlace の統合 14-1
MeetingPlace サーバの推奨事項 14-2
配置モデル 14-3
MeetingPlace のコンポーネント 14-6
MeetingPlace Audio Server 14-6
MeetingPlace H.323/SIP IP Gateway 14-6
MeetingPlace 配置のサイズの選定 14-8
音声会議の使用率のサイズ選定 14-8
Web 会議の使用率のサイズ選定 14-9
Video Integration と MCU のサイズ選定 14-9
MeetingPlace のネットワーク インフラストラクチャ 14-11
MeetingPlace と IP テレフォニー コンポーネント間の接続 14-12
Quality of Service（QoS） 14-12
トラフィック分類 14-12
コール アドミッション制御と帯域幅プロビジョニング 14-13
音声とビデオのレートとコーデックの選択 14-13
MeetingPlace Web セッションのネットワーク使用率 14-14
ジッタ 14-15
ドメイン ネーム システム（DNS） 14-15
ネットワーク タイム プロトコル（NTP） 14-15
非武装地帯（DMZ）の要件 14-16
相互運用性プロトコル 14-18
IP ネットワーク 14-18
MeetingPlace Audio Server がサポートするプロトコル 14-18

その他の MeetingPlace コンポーネントがサポートするプロトコル 14-19
公衆電話交換網（PSTN） 14-22
デジタル トランク 14-22
会議 14-25
オーディオ会議 14-25
コール フロー 14-25
会議のタイプ 14-26
ポート管理 14-27
スケジューリング 14-27
オーディオ会議のカスケード化 14-27
ビデオ エンドポイントを使用したオーディオ専用会議へのダイヤルイン 14-28
Web 会議 14-28
MeetingPlace Web サーバ 14-28
SQL データベース 14-29
会議のタイプ 14-30
Web 会議のカスケード化 14-30
セグメント化会議 14-30
ビデオ会議 14-30
音声リンク 14-31
MeetingPlace Video 14-31
MCU の設定 14-32
Enhanced Media Processor（EMP）の要件 14-33
ポート管理 14-33
スケジューリング 14-33
ビデオ会議への参加 14-34
会議のタイプ 14-34
ビデオ会議のコール フロー 14-35
ビデオ会議のカスケード化 14-38
ゲートキーパーとダイヤル プラン 14-39
Cisco Unified CallManager での動的 H.323 アドレッシング 14-39
Cisco Unified CallManager 冗長性グループと H.323 クライアント 14-39
MCU の登録 14-40
MeetingPlace 14-40
Reservationless Single Number Access（RSNA） 14-40
冗長性とロード バランシング 14-41
MeetingPlace Audio Server 14-41
MeetingPlace H.323/SIP IP Gateway 14-42

MeetingPlace Web 14-43
Cisco Unified CallManager 14-43
MeetingPlace Video 14-44
MCU 14-44

CHAPTER 15 IP ビデオ テレフォニー 15-1
IP ビデオ テレフォニー ソリューションのコンポーネント 15-1
Cisco Unified CallManager 5.0 のビデオ機能拡張 15-2
プロトコル 15-2
ビデオ コールの MTP およびトランスコーダ サポート 15-3
トポロジ対応ロケーション 15-3
Administration に関する考慮事項 15-5
リージョン 15-5
ロケーション 15-8
Retry Video Call as Audio 15-9
Wait for Far-End to Send TCS 15-12
マルチポイント会議 15-15
SCCP MCU リソース 15-17
メディア リソース グループとメディア リソース グループ リスト 15-18
H.323 および SIP MCU リソース 15-19
MCU のサイズの選定 15-21
ダイヤルイン会議の IVR 15-22
ゲートキーパー 15-24
サポートされるゲートキーパー プラットフォーム 15-27
エンドポイント ゲートキーパー 15-27
H.323 クライアントのプロビジョニング 15-28
H.323 MCU のプロビジョニング 15-33
H.320 ゲートウェイのプロビジョニング 15-35
ゲートキーパー ゾーンの設定 15-36
エンドポイント ゲートキーパーの要約 15-44
Cisco Unified CallManager 4.0 からの移行 15-47
アプリケーション 15-48
CTI アプリケーション 15-48
Cisco Emergency Responder 15-48
Cisco Unified CallManager Assistant 15-49
Cisco IP 音声自動応答装置と Cisco IP Contact Center 15-49
Cisco Attendant Console 15-49
Cisco Personal Assistant 15-50

Cisco IP SoftPhone および Cisco IP Communicator 15-50
コラボレーション ソリューション 15-50
T.120 アプリケーション共有 15-50
Cisco Unified MeetingPlace 15-50
無線ネットワーキング ソリューション 15-51
Cisco Aironet 802.11b ネットワーキング ソリューション 15-51
Cisco Unified Wireless IP Phone 7920 15-51
XML サービス 15-51

CHAPTER 16 LDAP ディレクトリ統合 16-1
ディレクトリ統合とは 16-2
IP テレフォニー エンドポイントのディレクトリ アクセス 16-4
Cisco Unified CallManager 5.0 でのディレクトリ統合 16-6
Cisco Unified CallManager 4.x の方法との比較 16-6
Cisco Unified CallManager 5.0 のディレクトリ アーキテクチャ 16-8
LDAP 同期 16-11
同期のメカニズム 16-14
セキュリティの考慮事項 16-16
LDAP 同期のベスト プラクティス 16-16
Microsoft Active Directory に関する追加の考慮事項 16-17
LDAP 認証 16-19
Microsoft Active Directory に関する追加の考慮事項 16-22

CHAPTER 17 IP テレフォニー移行オプション 17-1
段階的な移行 17-2
パラレル カットオーバー 17-3
マルチサイト企業における QSIG の必要性 17-4
要約 17-5

CHAPTER 18 音声セキュリティ 18-1
セキュリティの概要 18-2
セキュリティ ポリシー 18-2
レイヤ化したセキュリティ 18-3
インフラストラクチャの保護 18-4
物理的なセキュリティ 18-4
IP アドレッシング 18-5
電話機のセキュリティ 18-6
電話機の PC ポート 18-6
Gratuitous ARP 18-7

PC Voice VLAN へのアクセス 18-8
Web アクセス 18-9
ビデオ機能 18-10
アクセス設定 18-10
電話機の認証および暗号化 18-11
アクセス セキュリティ 18-13
Voice VLAN と Video VLAN 18-13
スイッチ ポート 18-14
ポートセキュリティ：MAC CAM フラッディング 18-14
ポート セキュリティ：ポート アクセスの防止 18-15
ポート セキュリティ：不良ネットワーク拡張の防止 18-16
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止 18-17
DHCP スヌーピング：DHCP スターベーション攻撃の防止 18-19
DHCP スヌーピング：バインディング情報 18-20
Dynamic ARP Inspection の要件 18-21
Quality of Service 18-25
アクセス コントロール リスト 18-26
VLAN アクセス コントロール リスト 18-26
ルータのアクセス コントロール リスト 18-28
ゲートウェイおよびメディア リソース 18-30
ゲートウェイの周囲へのファイアウォールの配置 18-31
ファイアウォール 18-33
ルーテッド ASA および PIX 18-36
トランスペアレント ASA および PIX 18-36
ASA および PIX の設定例 18-38
FWSM ルーテッド モード 18-39
FWSM トランスペアレント モード 18-39
FWSM の設定例 18-40
データ センター 18-42
アプリケーション サーバ 18-42
Cisco Unified CallManager およびアプリケーション サーバ上の Cisco Security Agent 18-42
マネージドではない Cisco Security Agent 18-42
マネージド Cisco Security Agent 18-43
アンチウイルス 18-43
サーバに関する一般的なガイドライン 18-44
配置例 18-46
ロビーに設置された電話機の例 18-46
ファイアウォールの配置例（集中型配置） 18-48

まとめ 18-50

CHAPTER 19 IP テレフォニー エンドポイント 19-1
アナログ ゲートウェイ 19-2
アナログ インターフェイス モジュール 19-2
低密度アナログ インターフェイス モジュール 19-2
高密度アナログ インターフェイス モジュール 19-3
アナログ インターフェイス モジュールでサポートされているプラットフォームおよび Cisco IOS 要件 19-3
Cisco コミュニケーション メディア モジュール（CMM） 19-5
WS-X6624-FXS アナログ インターフェイス モジュール 19-5
Cisco VG224 ゲートウェイ 19-5
Cisco VG248 ゲートウェイ 19-6
Cisco ATA 186 および 188 19-6
Cisco Unified IP Phone 19-7
Cisco ベーシック IP Phone 19-7
Cisco Unified IP Phone 7902G 19-7
Cisco Unified IP Phone 7905G 19-7
Cisco Unified IP Phone 7911G 19-7
Cisco Unified IP Phone 7912G 19-7
Cisco ビジネス IP Phone 19-8
Cisco Unified IP Phone 7940G 19-8
Cisco Unified IP Phone 7941G 19-8
Cisco Unified IP Phone 7941G-GE 19-8
Cisco マネージャ IP Phone 19-8
Cisco Unified IP Phone 7960G 19-9
Cisco Unified IP Phone 7961G 19-9
Cisco Unified IP Phone 7961G-GE 19-9
Cisco エグゼクティブ IP Phone 19-9
Cisco Unified IP Phone 7970G 19-10
Cisco 7971G-GE 19-10
Cisco Unified IP Phone 拡張モジュール 7914 19-10
ソフトウェアベースのエンドポイント 19-11
Cisco IP Communicator 19-11
IP Communicator の最大設定の制限 19-11
コーデックの選択 19-11
コール アドミッション制御 19-12
Cisco IP SoftPhone 19-12
Cisco IP SoftPhone の最大設定の制限 19-13

コーデックの選択 19-14
コール アドミッション制御 19-15
無線エンドポイント 19-16
サイト調査 19-16
認証 19-16
キャパシティ 19-17
電話機設定 19-18
ローミング 19-18
AP コール アドミッション制御 19-19
デバイス モビリティおよび Cisco Unified CallManager 19-20
Cisco IP Conference Station 19-21
ビデオ エンドポイント 19-22
SCCP ビデオ エンドポイント 19-22
Cisco Unified Video Advantage 19-22
Cisco IP Video Phone 7985G 19-24
Cisco Unified Video Advantage および Cisco IP Video Phone 7985G でサポートされているコーデック 19-25
サードパーティ製 SCCP ビデオ エンドポイント 19-25
サードパーティ製 SIP IP Phone 19-27
QoS の推奨事項 19-28
Cisco VG224 および VG248 19-28
Cisco ATA 186 および IP Conference Station 19-29
Cisco ATA 188 および IP Phone 19-29
ソフトウェアベースのエンドポイント 19-33
Cisco Unified Wireless IP Phone 7920 19-37
ビデオ テレフォニー エンドポイント 19-40
Cisco Unified Video Advantage と Cisco Unified IP Phone 19-40
Cisco IP Video Phone 7985G 19-41
Sony 社製と Tandberg 社製の SCCP エンドポイント 19-41
H.323 と SIP のビデオ エンドポイント 19-41
エンドポイント機能の要約 19-43

CHAPTER 20 Cisco Unified CallManager アプリケーション 20-1
IP Phone Service 20-2
IP Phone Service をサポートする電話機 20-2
Cisco Unified CallManager サービスと IP Phone Service のエンタープライズ サービス パラメータ 20-2
IP Phone Service の Cisco Unified CallManager サービス 20-2
IP Phone Service の エンタープライズ サービス パラメータ 20-3

IP Phone Service のアーキテクチャ 20-3
IP Phone Service の冗長性 20-6
IP Phone Service のスケーラビリティ 20-7
IP Phone Service のガイドラインと制限 20-7
エクステンション モビリティ（EM） 20-8
EM Phone のサポート 20-8
Cisco Unified CallManager および EM のサービス パラメータ 20-8
EM 用の Cisco Unified CallManager サービス 20-8
EM のサービス パラメータ 20-9
EM のアーキテクチャ 20-10
EM の冗長性 20-11
EM のガイドラインと制限 20-12
EM のパフォーマンスとキャパシティ 20-13
EM 相互作用：Unified CM Assistant、AC、および WebDialer 20-13
Cisco Unified CallManager Assistant（Unified CM Assistant） 20-14
Unified CM Assistant Phone のサポート 20-14
Cisco Unified CallManager および Unified CM Assistant のサービス パラメータ 20-14
Unified CM Assistant 用の Cisco Unified CallManager サービス 20-14
Unified CM Assistant のサービス パラメータ 20-15
Unified CM Assistant の機能とアーキテクチャ 20-16
Unified CM Assistant のプロキシ回線モード 20-16
Unified CM Assistant のシェアドライン モード 20-17
Unified CM Assistant のアーキテクチャ 20-18
Unified CM Assistant のダイヤル プランの考慮事項 20-20
Unified CM Assistant Console 20-23
Unified CM Assistant Console のインストール 20-23
Unified CM Assistant Console の QoS 20-23
Unified CM Assistant Console のディレクトリ ウィンドウ 20-23
Unified CM Assistant の冗長性 20-24
サービスとコンポーネントの冗長性 20-25
デバイスと到達可能性の冗長性 20-26
Unified CM Assistant のガイドラインと制限 20-27
Unified CM Assistant のパフォーマンスとキャパシティ 20-27
Unified CM Assistant と EM の相互作用 20-28
Attendant Console 20-29
AC Phone のサポート 20-29
Cisco Unified CallManager および AC のサービス パラメータ 20-29
AC 用の Cisco Unified CallManager サービス 20-29

AC のサービス パラメータ 20-29
AC のアプリケーション ユーザ 20-30
AC の機能とアーキテクチャ 20-30
AC のアーキテクチャ 20-32
Attendant Console デスクトップ アプリケーション 20-33
Attendant Console のインストール 20-33
Attendant Console の QoS 20-33
Attendant Console のディレクトリ ウィンドウ 20-34
AC の冗長性 20-36
サービスとコンポーネントの冗長性 20-36
デバイスと到達可能性の冗長性 20-36
AC のガイドラインと制限 20-37
AC のパフォーマンスとキャパシティ 20-38
AC と EM の相互作用 20-38
WebDialer 20-40
WebDialer Phone のサポート 20-40
Cisco Unified CallManager および WebDialer のサービス パラメータ 20-40
WebDialer 用の Cisco Unified CallManager サービス 20-40
WebDialer サービス パラメータ 20-41
WebDialer の機能とアーキテクチャ 20-41
WebDialer サーブレット 20-42
Redirector サーブレット 20-43
WebDialer のアーキテクチャ 20-44
WebDialer の URL 20-46
WebDialer の冗長性 20-47
サービスとコンポーネントの冗長性 20-47
デバイスと到達可能性の冗長性 20-47
WebDialer のガイドラインと制限 20-48
WebDialer と EM の相互作用 20-48

APPENDIX A 推奨されるハードウェアとソフトウェアの組み合せ A-1

GLOSSARY 用語集

INDEX 索引

このマニュアルについて

このマニュアルでは、Cisco Unified CallManager 5.0. に基づいて Cisco Unified Communications システムを展開するための、設計上の考慮事項とガイドラインについて説明しています。

このマニュアルでは、次に示す Cisco Unified Communications システムのコンポーネントを中心に説明します。

- Cisco Unified CallManager
- Cisco Unified Video Advantage
- Cisco Unified MeetingPlace

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

- Cisco Unified Communications システムの詳細：
  http://www.cisco.com/go/unified-techinfo
  http://www.cisco.com
- Cisco Unified CallManager 5.0 の詳細：
  http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/5_0/index.htm
  http://www.cisco.com
- ソリューション リファレンス ネットワーク デザイン（SRND）に関するその他のマニュアル：
  http://www.cisco.com/go/srnd

（注） 特に指定のない限り、このマニュアルの情報は、Cisco Unified CallManager Release 5.0 に適用されます。

改訂の履歴

このマニュアルは、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/srnd

この Cisco.com の Web サイトを定期的に参照し、お手元のマニュアルの（表紙ページにある）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、更新されているかどうかを確認してください。

次の表では、このマニュアルに対する改訂の履歴をリストしています。

改訂日	備考
2006 年 4 月	新しい製品名を記述するように本文が更新され、いくつかの誤植も修正されました。
2006 年 3 月	Cisco Unified CallManager Release 5.0 を対象にしたこのマニュアルの初版です。

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカルサポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

WWW 上の次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com 登録ユーザ（Cisco Direct Customers）の場合、Ordering ツールからシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） Web または電話でサービス リクエストを発行する前に、Cisco Product Identification（CPI）ツールを使用して製品のシリアル番号を確認してください。CPI ツールには、Cisco Technical Support Web サイトから、Documentation & Tools の下の **Tools & Resources** リンクをクリックするとアクセスできます。アルファベット順の索引ドロップダウン リストから **Cisco Product Identification Tool** を選択するか、Alerts & RMAs の下の **Cisco Product Identification Tool** リンクをクリックします。CPI ツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

補足資料および情報へのアクセス

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

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

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

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

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

概要

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

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

- IP テレフォニー

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

- カスタマー コンタクト センター

  Cisco IP Contact Center 製品は、グローバルに使用可能なネットワークを介したカスタマー コミュニケーションを効率的かつ効果的にする方法とアーキテクチャを組み合せたものです。企業でこのソリューションを使用すると、より広範なリソースから必要なものを引き出して、お客様にサービスを提供することができます。具体的には、大規模なエージェント プールへのアクセス、複数のコミュニケーション手段、およびカスタマー セルフヘルプ ツールなどがあります。

- ビデオ テレフォニー

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

- リッチメディア会議

  Cisco Conference Connection および Cisco Unified MeetingPlace は、音声、ビデオ、および Web 会議に対応した IP ベースの統合ツール セットを使用して、仮想的な会議環境を拡張します。

- サードパーティ製アプリケーション

  シスコでは最先端の企業と協力して、メッセージング、カスタマー ケア、およびワークフォース オプティマイゼーションなど、重要なビジネス ニーズに焦点を当てた革新的なサードパーティ製 IP 通信アプリケーションおよび製品を種類豊富に提供しています。

このマニュアルでは、次に示す Cisco Unified Communications System のコンポーネントについて、設計上のポイントを中心に説明します。

- Cisco Unified CallManager
- Cisco Unified Video Advantage
- Cisco Unified MeetingPlace

Cisco IP Contact Center など、その他の要素については、次の Web サイトで入手可能なマニュアルを参照してください。

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

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

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

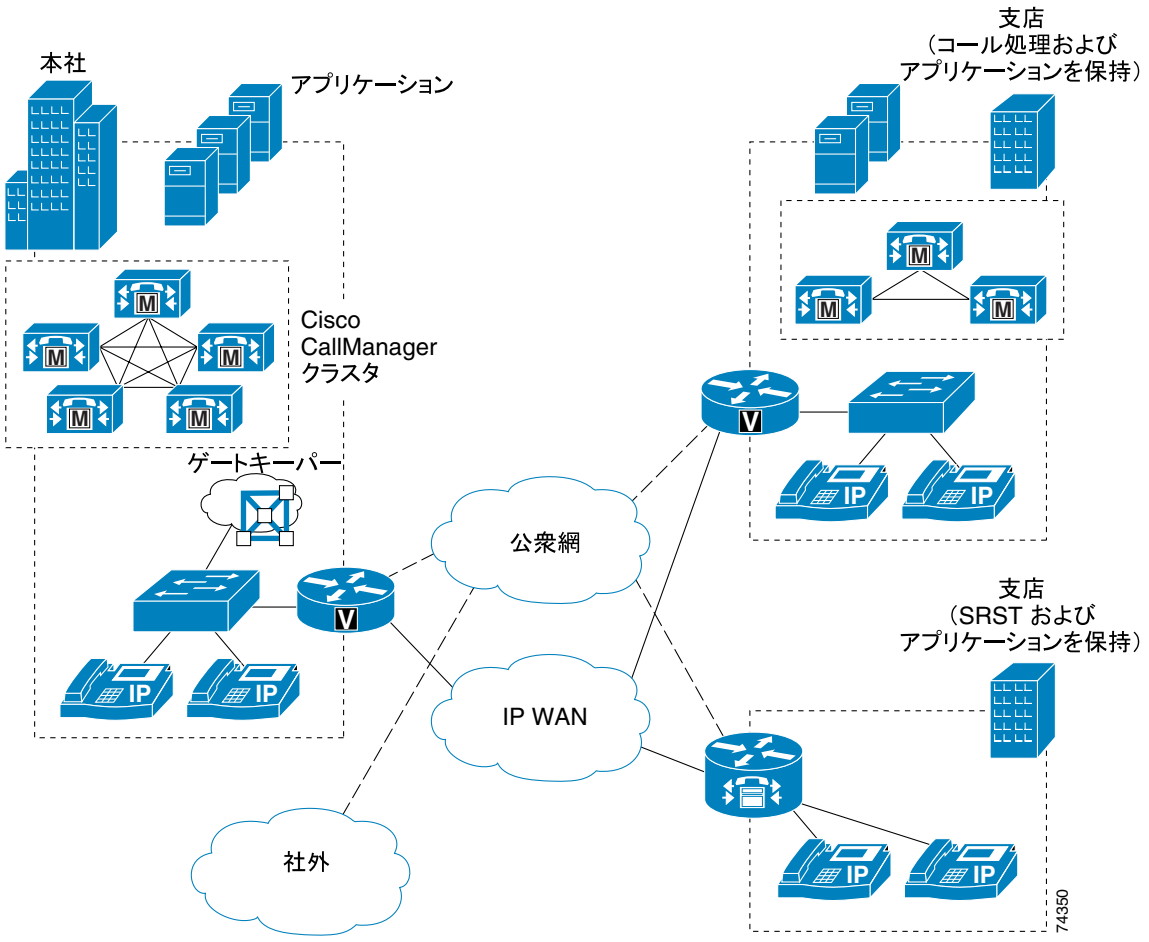
http://www.cisco.com

Cisco Unified Communications の概要

Cisco IP テレフォニーは、生産性を向上させ、音声とデータが別々になっているネットワークの管理と保守に関連したコストを削減しようとする組織に適したソリューションです。このソリューションは業界を先導するレベルのものです。Cisco IP ネットワーク インフラストラクチャの柔軟性と高度な機能性が提供するフレームワークにより新しいアプリケーションを迅速に導入することができます。それらは、デスクトップ IP テレフォニー、ユニファイド メッセージング、ビデオ テレフォニー、デスクトップ コラボレーション、エンタープライズ アプリケーションと IP Phone ディスプレイとの統合、コラボレーティブ IP コンタクト センターなどです。これらのアプリケーションにより、生産性が向上し、企業の収益が増大します。

図 1-1 は、Cisco Unified CallManager をコール処理エージェントとして使用した、Cisco IP ネットワーク インフラストラクチャを利用する一般的な IP テレフォニーの配置を示しています。

図 1-1　一般的な IP テレフォニーの配置



Cisco IP テレフォニーの基本アーキテクチャには、次の主要コンポーネントが含まれています（図 1-1 を参照）。

- Cisco IP ネットワーク インフラストラクチャ（P.1-4）
- QoS（P.1-4）
- コール処理エージェント（P.1-5）
- 通信エンドポイント（P.1-5）
- 会議、メッセージング、およびコラボレーション機能（P.1-6）
- アプリケーション（P.1-7）
- セキュリティ（P.1-8）

Cisco IP ネットワーク インフラストラクチャ

ネットワーク インフラストラクチャには、Public Switched Telephone Network（PSTN; 公衆電話交換網）ゲートウェイ、アナログ電話サポート、および Digital Signal Processor（DSP; デジタル シグナル プロセッサ）ファームが含まれています。このインフラストラクチャは、ハードフォン、ソフトフォン、およびビデオ装置などの複数のクライアント タイプをサポートできます。また、インフラストラクチャには、従来型の PBX システム、ボイスメール システム、およびディレクトリ システムの統合に必要なインターフェイスと機能も組み込まれています。このインフラストラクチャの構築に使用される一般的な製品には、Cisco 音声ゲートウェイ（非ルーティング、ルーティング、および統合）、Cisco IOS と Catalyst スイッチ、および Cisco ルータなどがあります。

IP ネットワーク インフラストラクチャの詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章を参照してください。

QoS

音声は、IP ネットワーク トラフィックの 1 つのクラスであり、パケット損失、遅延、遅延変動（ジッタとも呼ばれます）に関する厳密な要件があります。音声トラフィックに対するこれらの要件を満たすために、Cisco Unified Communications には、トラフィック分類、キューイング、トラフィック シェーピング、RTP ヘッダー圧縮（cRTP）、および Transmission Control Protocol（TCP）ヘッダー圧縮などの QoS 機能が組み込まれています。

Cisco Unified Communications の QoS コンポーネントは、Cisco IP ネットワーク インフラストラクチャの IP トラフィック管理、キューイング、およびシェーピングの豊富な機能により提供されます。このインフラストラクチャで IP テレフォニー用の QoS は、主に次の要素により実現可能となります。

- トラフィック マーキング
- 拡張キューイング サービス
- Link fragmentation and interleaving（LFI）
- Compressed RTP（cRTP）
- Low-Latency Queuing（LLQ; 低遅延キューイング）
- リンク効率
- トラフィック シェーピング
- コール アドミッション制御（帯域幅の割り当て）

QoS の詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章にある QoS に関する各項を参照してください。

コール処理エージェント

Cisco Unified CallManager は、Cisco IP テレフォニーの中核となるコール処理ソフトウェアです。このソフトウェアは、Cisco IP ネットワーク インフラストラクチャ上にコール処理機能を構築します。Cisco Unified CallManager ソフトウェアは、企業の電話機能を拡張して、IP Phone、メディア処理装置、音声ゲートウェイ、およびマルチメディア アプリケーションなどのパケット テレフォニー ネットワーク デバイスとして利用できるようにします。

企業の規模、地域分布、および必要機能に応じて、次のモデルのいずれかに従って Cisco Unified CallManager のコール処理機能を配置できます。

- 単一サイト コール処理モデル

  単一サイト モデルでは、各サイトまたはキャンパスに、コール処理機能を実行するための自身の Cisco Unified CallManager または Cisco Unified CallManager クラスタがあります。音声トラフィックは IP WAN を通過しません。その代わりに、外部コール、またはリモート サイトへのコールには、公衆電話交換網（PSTN）を使用します。
- 集中型コール処理を使用するマルチサイト WAN モデル

  集中型コール処理を使用するマルチサイト WAN モデルでは、Cisco Unified CallManager クラスタはメイン（または中央）キャンパスに置かれ、遠隔地の支店との通信は、通常、IP WAN を介して行われます。中央サイトまたは IP WAN のどちらかがダウンしても、リモート サイトは、SRST（Survivable Remote Site Telephony）と呼ばれる機能を使用して、処理を続行できます。また、IP WAN が一時的にオーバーサブスクリプションになっても、リモート サイトでは、公衆網を介してコールを発信することができます。さらに、クラスタ間トランクを使用して、複数の中央サイトを相互接続することができます。
- 分散型コール処理を使用するマルチサイト WAN モデル

  分散型コール処理を使用するマルチサイト WAN モデルでは、各サイトには、コール処理用の独自の Cisco Unified CallManager クラスタがあります。サイト間の通信は、通常、IP WAN を介して行われ、公衆網がバックアップ音声パスの役目をします。このモデルを使用する場合、IP WAN を経由して相互接続できるサイトの数には制限はありません。
- IP WAN を介したクラスタ化

  QoS 機能に対応している IP WAN によって相互接続される複数サイト間で、単一の Cisco Unified CallManager クラスタを配置できます。コール処理の冗長性を実現するには、バックアップ サーバを各サイトにローカルに配置するか、または WAN を介したリモート サイトに配置します。WAN を介したクラスタ化は、ビジネスが継続して行われるサイトの障害回復プランとして、または中小規模サイト用の単一ソリューションとして適しています。

Cisco IP テレフォニー ネットワークの設計にこれらの配置モデルを適用する方法については、P.2-1 の「IP テレフォニー配置モデル」を参照してください。

通信エンドポイント

通信エンドポイントとは、卓上電話機や、PC 上で実行されるソフトフォン アプリケーションなどの、ユーザ機器です。IP 環境では、各電話機はイーサネット接続を備えています。IP Phone は、従来の電話機に要求されるすべての機能に加えて、Web サイトへのアクセス機能などのより高度な機能も備えています。

IP テレフォニー エンドポイントには、デスクトップ Cisco Unified IP Phone のさまざまなモデルのほかに、次のデバイスがあります。

- ソフトウェアベースのエンドポイント

  Cisco IP Communicator および Cisco Unified Personal Communicator は、ご使用のコンピュータをフル機能の IP Phone に変えるデスクトップ アプリケーションです。これらのアプリケーションには、コール トラッキング、デスクトップ コラボレーション、およびオンライン電話帳からのワンクリック ダイヤルといった機能が追加されています。Cisco IP Communicator は、拡張されたテレフォニー機能を PC から提供するソフトウェアベースのアプリケーションです。旅行

時の補助的な電話機、在宅勤務用のデバイス、メインのデスクトップ電話機などとして機能することで、さまざまなお客様のニーズに適合するよう設計されています。Cisco Unified Personal Communicator では、幅広い通信アプリケーションとサービスが 1 つのデスクトップ コンピュータ アプリケーションとして統合され、音声、ビデオ、Web 会議、コール管理、電話帳、在席情報に対する強力なコミュニケーション ツールに迅速かつ簡単にアクセスできます。

- ビデオ テレフォニー エンドポイント

  ビデオ テレフォニー機能は、現在、Cisco Unified CallManager と完全に統合されています。また、Cisco Unified Video Advantage では、Cisco Unified IP Phones および Cisco IP Communicator Softphone アプリケーションへのビデオ テレフォニー機能が提供されます。このビデオ テレフォニー ソリューションは、Windows ベースのアプリケーションと USB カメラで構成されています。ユーザは、使い慣れた電話機インターフェイスを使用して Cisco Unified IP Phone から通話を行い、余分なボタンを押したりマウスをクリックしたりすることなく、通話が PC 上にビデオ付きで表示されます。

- 無線エンドポイント

  Cisco Wireless IP Phone 7920 は、シスコの IP Phone ファミリを 10/100 イーサネットから 802.11 Wireless LAN（WLAN; 無線 LAN）へと広げます。Cisco Wireless IP Phone 7920 には、他の Cisco Unified IP Phone と同様の機能を持つ複数のライン アピアランスが用意されています。また、Cisco Wireless IP Phone 7920 には、802.11b ネットワークの動作に対応した拡張 WLAN セキュリティと QoS も用意され、XML ベースのデータアクセスとサービスが提供されます。

各種のエンドポイントの詳細については、P.19-1 の「IP テレフォニー エンドポイント」を参照してください。

会議、メッセージング、およびコラボレーション機能

Cisco Unified Communications は、会議、音声メッセージング、マルチメディア コラボレーションの各機能を提供する、次の追加機能とアプリケーションをサポートしています。

- 会議

  Cisco Unified CallManager は、多数の他の Cisco ソフトウェアおよびハードウェア デバイスと連携し、Annunciator および Music On Hold など会議の全機能を提供することができます。Cisco Unified CallManager での会議機能の設計およびプロビジョニングの詳細については、P.6-1 の「メディア リソース」を参照してください。

- 音声メッセージング

  Cisco Unified CallManager には、サードパーティ製のボイスメール システムとの統合、および Cisco Unity および Unity Connection との統合によって、あらゆるボイスメールおよび音声メッセージング機能を提供する機能があります。サードパーティ製ボイスメール システムと Cisco Unified CallManager との統合の詳細については、P.12-1 の「サードパーティ製のボイスメール設計」を参照してください。Cisco Unity および Unity Connection と Cisco Unified CallManager との統合の詳細については、P.13-1 の「Cisco Unity」を参照してください。

- ビデオ テレフォニー

  ビデオ テレフォニー機能が Cisco Unified CallManager に完全に統合され、シスコおよびシスコの戦略的パートナーから新しいビデオ エンドポイントも入手できるようになりました。ビデオ コールおよび会議は、IP phone で音声コールを発信するのと同じくらい簡単になりました。Cisco Unified CallManager でのビデオ機能の詳細については、P.15-1 の「IP ビデオ テレフォニー」を参照してください。

- マルチメディア コラボレーション

  Cisco Unified MeetingPlace は、音声、ビデオ、および Web 会議機能を統合した、完全なリッチメディア会議アプリケーションです。これを使用すると、リモート会議が、対面式の会議と同じくらい自然で効果的なものになります。Cisco Unified CallManager と MeetingPlace との統合の詳細については、P.14-1 の「Cisco Unified MeetingPlace の統合」を参照してください。

アプリケーション

アプリケーションは、次のような高度なテレフォニー機能や統合されたネットワーク機能を追加することで、コール処理インフラストラクチャに基づいて Cisco IP テレフォニーのエンドツーエンド機能を拡張します。

- IP Phone サービス

  Cisco Unified IP Phone Service は、Web クライアントやサーバ、および Cisco Unified IP Phone の XML 機能を利用するアプリケーションです。Cisco Unified IP Phone のファームウェアには、限定的な Web ブラウジング機能を可能にするマイクロブラウザが含まれています。これらの電話サービス アプリケーションは、ユーザのデスクトップ電話機上で直接実行することで、付加価値サービスと生産性向上を提供します。

- エクステンション モビリティ

  Cisco Unified CallManager の Extension Mobility（EM; エクステンション モビリティ）機能では、ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone を独自に設定することが可能です。ユーザがログインすると、IP Phone は、回線番号、短縮ダイヤル、サービス リンク、およびその他のユーザ固有の電話機のプロパティなど、ユーザの個別のデバイス プロファイル情報を受け入れます。EM 機能では、認証されたユーザのデバイス プロファイルに従って電話機が動的に設定されます。このアプリケーションの利点は、電話機が EM をサポートしている限り、ユーザが物理的な場所に関係なく、Cisco Unified CallManager クラスタ内の任意の電話機から自分の内線番号に接続できることです。

- Cisco Unified CallManager Assistant

  Cisco Unified CallManager Assistant は、Cisco Unified CallManager に統合されたアプリケーションです。これを使用すると、1 人以上のマネージャに代わってアシスタントが着信コールを処理できます。Unified CallManager Assistant Console デスクトップ アプリケーションを使用すると、アシスタントが手早くマネージャの状態を確認し、コールをどうするかを決定できます。アシスタントは、自分の電話機のソフトキーを使用するか、キーボード ショートカット、ドロップダウン メニュー、またはマネージャのプロキシ回線へのコールのドラッグ アンド ドロップするなどのいずれかの PC インターフェイスを使用して、コールを操作できます。

- Attendant Console

  Cisco Unified CallManager Attendant Console（AC）アプリケーションを使用すると、受け付け係が企業内でコールに応答して転送したり、コールを送信したりできます。係員は Windows 2000 または Windows XP を実行している PC に、クライアント / サーバ Java アプリケーションの Attendant Console をインストールできます。Attendant Console は Cisco CallManager Attendant Console Server に接続し、ログイン サービス、回線状態、およびディレクトリ サービスを提供します。1 つの AC サーバに複数の Attendant Console を接続できます。

- WebDialer

  Cisco WebDialer は Cisco Unified CallManager のクリックダイヤル アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できるようになります。管理者が CTI リンクを管理したり、JTAPI または TAPI アプリケーションを作成したりするために必要なものはありません。Cisco WebDialer には、独自のユーザ インターフェイスと認証メカニズムを提供するための、簡単な Web アプリケーションと HTTP または Simple Objects Access Protocol（SOAP）が用意されているからです。どちらの方法でも、このソリューションは Cisco Unified CallManager クラスタ全体を、完全な冗長性を持ってサポートできます。

これらのアプリケーションの詳細については、P.20-1 の「Cisco Unified CallManager アプリケーション」を参照してください。

セキュリティ

Cisco Unified Communications 配置のセキュリティに関しては、特に次の点を考慮する必要があります。

- 重要なアプリケーション サーバやネットワーク コンポーネントへの物理的なアクセスを制限するための物理的なセキュリティ
- 不正なログインや攻撃を防止するためのネットワーク アクセス セキュリティ
- Cisco Unified CallManager、エンドポイント デバイス、およびさまざまなディレクトリやデータベース用のセキュリティ対策
- さまざまなユーザ クラスの発信権限を定義するためのメカニズム
- セキュリティを向上させるための慎重なネットワーク設計と管理

IP テレフォニー ネットワークのセキュリティの詳細については、P.18-1 の「音声セキュリティ」を参照してください。

CHAPTER 2

IP テレフォニー配置モデル

この章では、Cisco Unified CallManager 5.0 の IP テレフォニー配置モデルについて説明します。以前のリリースの Cisco Unified CallManager での設計ガイドについては、次の Web サイトで入手可能な IP Telephony Solution Reference Network Design（SRND）のマニュアルを参照してください。

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

各 Cisco Unified Communications は、次に説明する主要配置モデルに基づいて実現されています。

- 単一サイト（P.2-3）

  単一サイトで IP テレフォニーを実現する場合のモデルは、その単一サイトに配置されるコール処理エージェント、およびそのサイト全体に音声トラフィックを伝送するための LAN または MAN（メトロポリタンエリア ネットワーク）から構成されています。コールが LAN または MAN を超えて発信される場合は、PSTN（公衆電話交換網）が使用されます。IP WAN が単一サイト モデルに組み込まれている場合、IP WAN はデータ トラフィック専用です。テレフォニー サービスは WAN を介して行われることはありません。

  このモデルは、キャンパスが 1 個所の場合、または回線数が 30,000 未満のサイトの場合に適用されます。

- 集中型コール処理を使用するマルチサイト WAN（P.2-6）

  集中型コール処理を使用するマルチサイト WAN モデルは、単一のコール処理エージェントから構成されています。このコール処理エージェントは、多数のサイトにサービスを行い、IP WAN を使用してサイト間で音声トラフィックを転送します。また、IP WAN は、中央サイトとリモート サイト間のコール制御信号も伝送します。

  このモデルは、次のようなメイン サイトに適用されます。QoS 対応 WAN 経由で接続されている、小規模のリモート サイトが多数あり、WAN の故障中はそれらのリモート サイトにフル機能が要求されない場合です。

- 分散型コール処理を使用するマルチサイト WAN（P.2-15）

  分散型コール処理を使用するマルチサイト WAN モデルでは、複数の独立したサイトから構成されています。各サイトには独自のコール処理エージェントがあり、そのエージェントは、分散サイト間の音声トラフィックを伝送する IP WAN に接続されます。このモデルの IP WAN は、各サイトに独自のコール処理エージェントがあるので、サイト間のコール制御信号を伝送しません。

  このモデルは、回線数が 30,000 を超える大規模の中央サイトの場合、または、6 個所以上に分散している大規模サイトの合計回線数が 30,000 を超えていて、そのサイト間が QoS 対応 WAN で相互接続されている場合に適用されます。

- IP WAN を介したクラスタ化（P.2-19）

  このモデルでは、単一の Cisco Unified CallManager クラスタが配置されていて、複数のサイト間は QoS 機能に対応している IP WAN によって接続されています。

このモデルは、最大で 6 個所に分散している大規模サイトの合計回線数が 30,000 以内で、そのサイト間が QoS 対応 WAN で相互接続されている場合に適用されます。

(注)　このマニュアルは、読者が前述の配置モデルの内容を理解していることを前提としています。したがって、配置モデルについて十分に理解した上で、読み進むことをお勧めします。

また、P.2-28 の「U. S. Section 508 準拠についての設計上の考慮事項」の項では、IP テレフォニー ネットワークを設計するときに、身体に障害のあるユーザに対して U.S. Section 508 に従ってアクセシビリティ機能を組み込む場合のガイドラインを示します。

(注)　推奨されるハードウェア　プラットフォームとソフトウェア　リリースに関する最新情報については、次の Web サイトにあるドキュメントを参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

単一サイト

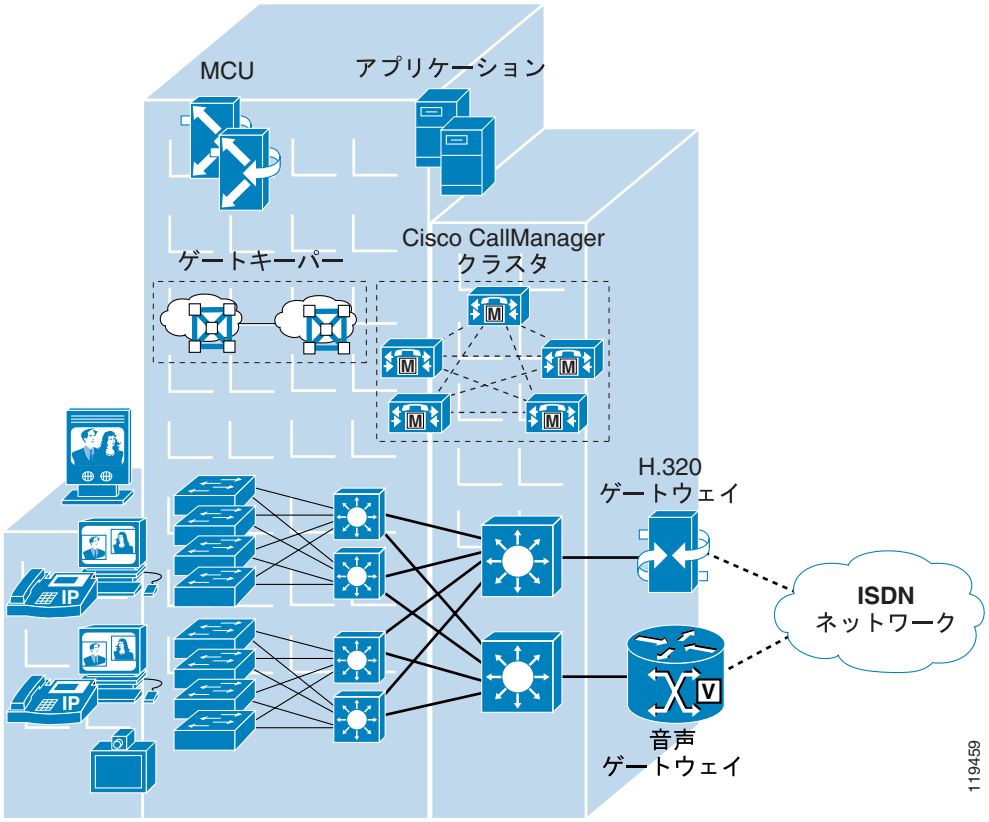
単一サイトで IP テレフォニーを実現する場合のモデルは、その単一サイト（キャンパス）に配置される 1 つのコール処理エージェントから構成されています。テレフォニー サービスは、IP WAN を使用して行われることは*ありません*。企業は、一般的に、LAN または MAN に対しては単一サイト モデルを配置して、サイト内の音声トラフィックを伝送しています。このモデルでは、コールが LAN または MAN を越えて発信される場合は、PSTN（公衆電話交換網）が使用されます。

単一サイト モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CallManager または Cisco Unified CallManager クラスタ。
- クラスタあたり最大 30,000 の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Cisco Unified CallManager クラスタあたり最大 500 の H.323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメールまたはユニファイド メッセージング コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする　H.323　クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS リリース 12.3(8)T 以降）に登録することが必要。Cisco Unified CallManager は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。
- 公衆 ISDN 網の H.320 ビデオ会議デバイスとの通信に H.323/H.320 ビデオ ゲートウェイが必要。
- サイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）。
- サイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）。7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec もサポートされます。

図 2-1 は、単一キャンパスまたは単一サイト内の IP テレフォニー ネットワークのモデルを示しています。

図 2-1　単一サイト配置モデル



単一サイト モデルの利点

統合されたネットワーク ソリューションの単一インフラストラクチャには、コスト上の大きな利点があります。また、このソリューションの IP テレフォニーでは、企業の多くの IP ベース アプリケーションを利用できるようになります。単一サイトの配置では、各サイトを完全に独立させることも可能です。IP WAN の障害の場合、または帯域幅不足の場合、各サイト間のサービスの依存関係はなくなります。また、コール処理サービスまたは機能が失われることもありません。

要約すると、単一サイト モデルの主な利点は次のとおりです。

- 配置しやすい
- 集中ソリューション用の共通インフラストラクチャである
- ダイヤル プランが単純
- G.711 コーデックのみを使用するので、トランスコーディング リソースの必要がない

単一サイト モデルのベスト プラクティス

単一サイト モデルを実装する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

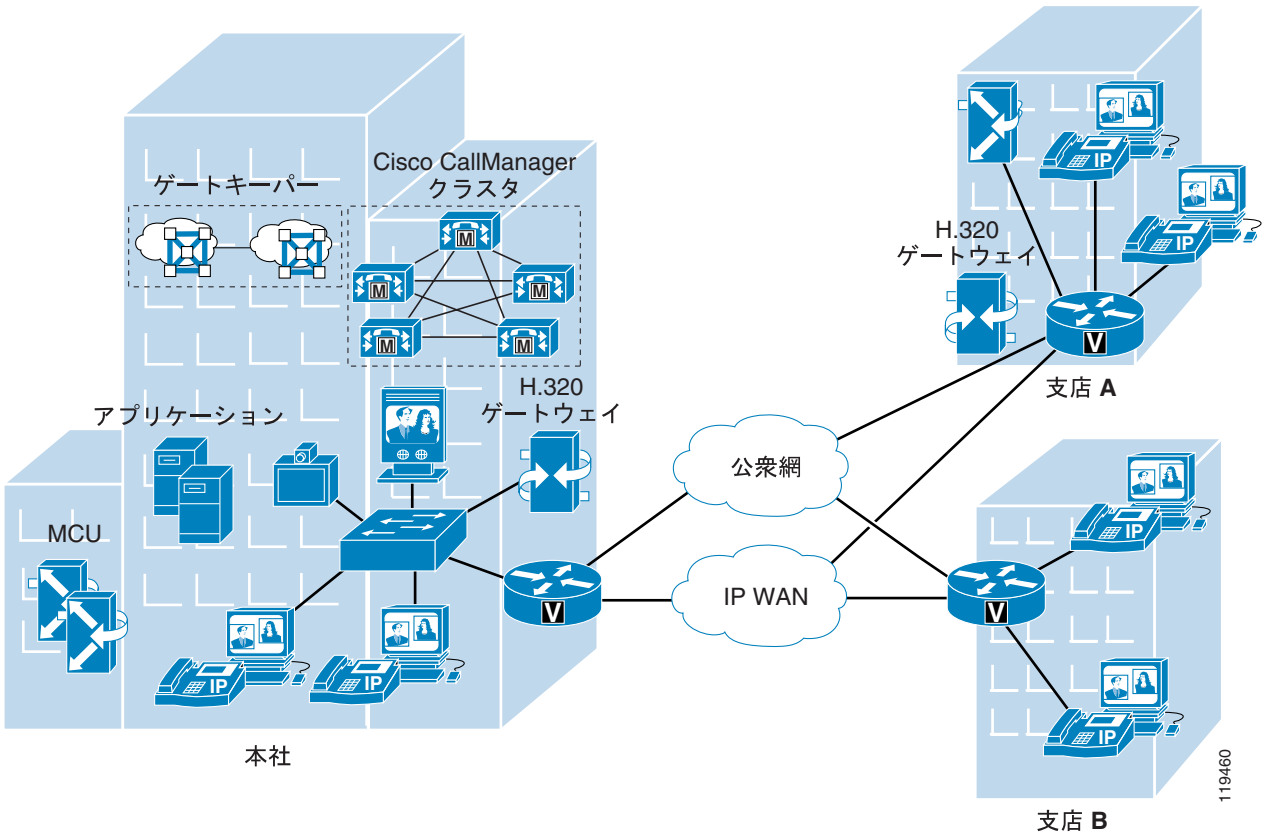
- 一般的なインフラストラクチャ 構想に基づいて可用性および耐障害性を高めます。IP テレフォニーへの迅速な移行、アプリケーションにビデオ ストリーミングやビデオ会議などを容易に統合、および IP テレフォニー配置を拡張し、WAN または複数の Cisco Unified CallManager クラスタへのアクセスを可能にするには、インフラストラクチャを適切に構築する必要があります。
- 自社内のコール パターンを知っておく必要があります。単一サイト モデルは、大部分のコールが社内の同一サイトから発信されている場合、または社外の公衆網ユーザ宛てに発信されている場合に適用します。
- すべてのエンドポイントに G.711 コーデックを使用します。この方式を実施すると、トランスコーディングに対してデジタル シグナル プロセッサ（DSP）リソースを消費する必要がなくなり、その分のリソースは、会議やメディア ターミネーション ポイント（MTP）などの他の機能に割り当てることができます。
- H.323 機能を必要とし*ない*場合は、公衆網に Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）ゲートウェイを使用します。この方式を実施すると、ダイヤル プランの設定が容易になります。H.323 は、特定の機能（たとえば、Signaling System 7（SS7）や Non-Facility Associated Signaling（NFAS））をサポートするために必要な場合があります。
- 高可用性、電話機用の接続オプション（インライン パワー）、Quality of Service（QoS）メカニズム、およびセキュリティ用の推奨ネットワーク インフラストラクチャを実装しています（P.3-1 の「ネットワーク インフラストラクチャ」を参照）。
- P.8-1 の「コール処理」の章にリストされているプロビジョニングの推奨事項を実行します。

集中型コール処理を使用するマルチサイト WAN

集中型コール処理を使用するマルチサイト WAN モデルは、単一のコール処理エージェントから構成されています。このコール処理エージェントは、多数のサイトにサービスを行い、IP WAN を使用してサイト間の IP テレフォニー トラフィックを転送します。また、この IP WAN は、中央サイトとリモート サイト間のコール制御シグナリングも伝送します。図 2-2 は、一般的な集中型コール処理配置を示しています。この配置では、中央サイトのコール処理エージェントとして Cisco Unified CallManager クラスタを使用し、すべてのサイトを接続するために、QoS 対応の IP WAN を使用します。リモート サイトでは、コール処理に集中型 Cisco Unified CallManager クラスタを使用します。ボイスメール システムや IVR システムなどのアプリケーションも、管理と保守にかかる全体的なコストを削減するために、一般に中央に配置されます。

（注） このマニュアルで説明する集中型コール処理モデルを適用した各ソリューションでは、さまざまなサイトは、QoS 対応の IP WAN に接続されています。

図 2-2　集中型コール処理を使用するマルチサイト配置モデル



集中型コール処理を使用するマルチサイト モデルの設計上の特長は、次のとおりです。

- 単一の Cisco Unified CallManager または Cisco Unified CallManager クラスタ。
- クラスタあたり最大 30,000 の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Cisco Unified CallManager クラスタあたり最大 500 の H.323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）。
- すべての外部コールに対して公衆網で対応。

- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメールまたはユニファイド メッセージング コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする　H.323　クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS リリース 12.3(8)T 以降）に登録することが必要。Cisco Unified CallManager は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。
- マルチポイント ビデオ会議には MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースが中央サイトに存在していても、ローカル会議リソースが必要な場合はリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網の H.320 ビデオ会議デバイスとの通信に H.323/H.320 ビデオ ゲートウェイが必要。これらのゲートウェイは中央サイトにあっても、ローカル ISDN アクセスが必要な場合はリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、および異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、および異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。
- Cisco Unified CallManager のロケーションでコール アドミッション制御を提供し、ビデオ コールでは自動代替ルーティング（AAR）もサポート。
- Cisco Unified CallManager クラスタあたり最大 500 のロケーション。
- ビデオ用の Survivable Remote Site Telephony（SRST）のサポート*なし*。WAN 接続に失敗すると、リモート サイトにある SCCP ビデオ エンドポイントは音声専用デバイスとなり、H.323 ビデオ デバイスが失敗します。リモート サイトの 2 つのデバイス間のアクティブな SCCP ビデオ コールは、ビデオと音声の両方のチャネルで継続されますが、コール転送などの追加機能をアクティブにできなくなります。アクティブな H.323 ビデオ コールは失敗します。SRST モードでは、新しいコールが常に音声のみになります。WAN 接続がダウンすると、WAN 上のすべてのコールがドロップされます。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）
- ATM とフレーム リレーのサービス インターワーキング（SIW）
- Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）
- 音声およびビデオ対応 IP Security Protocol VPN（IPSec VPN（V3PN））

WAN エッジに置かれているルータには、プライオリティ キューイングやトラフィック シェーピングなどの QoS メカニズムが装備されていて、WAN の帯域幅が恒常的に不足している場合に、データ トラフィックから音声トラフィックを保護しています。さらに、コール アドミッション制御方式も導入されていて、音声トラフィックによる WAN リンクのオーバーサブスクリプションを防いだり、確立済みのコール品質が低下するのを防いだりしています。集中型コール処理配置の場合、Cisco Unified CallManager 内にコール アドミッション制御を行う*ロケーション*が構築されます（ロケーションの詳細については、P.9-13 の「Cisco Unified CallManager の静的ロケーション」の項を参照してください）。

リモート サイトでは、さまざまな Cisco ゲートウェイにより、公衆網を介したアクセスが可能です。IP WAN に障害が起きた場合、または IP WAN 上で使用可能な帯域幅がすべて消費されてしまった場合でも、リモート サイトのユーザは、公衆網アクセス コードをダイヤルして、公衆網を利用してコールを発信できます。SCCP および SIP 電話機は、Cisco IOS ゲートウェイの Survivable Remote Site Telephony（SRST）機能を利用すると、WAN に障害が発生している支店でのコール処理が可能になります。

集中型コール処理モデルのベスト プラクティス

集中型コール処理を使用したマルチサイト WAN モデルを実装する場合は、次のガイドライン、およびベスト プラクティスを参考にしてください。

- 音声のカットスルー遅延（クリッピングとも呼ばれます）を減らすために、Cisco Unified CallManager とリモート ロケーション間の遅延を最小限に抑えます。
- リモート支店とのコール アドミッションを制御するには、Cisco Unified CallManager 内のロケーション メカニズムを使用します。このメカニズムをさまざまな WAN トポロジに適用する方法については、P.9-1 の「コール アドミッション制御」の章を参照してください。
- ロケーション メカニズムは、Cisco Unified CallManager 3.1 およびそれ以降のリリースで実行される複数サーバに対して作動します。この設定では、Cisco Unified CallManager がサポートされているサーバ上で実行されている場合、最大 30,000 台の IP Phone（または 20,000 台のデバイス ユニット）をサポートできます。
- 各リモート サイトでの Survivable Remote Site Telephony（SRST）モードでサポートされている IP Phone およびライン アピアランスの数は、その支店内にあるルータのプラットフォーム、取り付け済みメモリ容量、および Cisco IOS リリースにより異なります（SRST プラットフォームおよびコード仕様に関する詳細は、Cisco.com から入手できる SRST 文書を参照してください）。一般的には、特定サイトに対して集中型コール処理か、分散コール処理かを決定するには、次に示す種々の要素によります。
  - IP WAN 帯域幅、または遅延制限
  - 音声ネットワークに関する臨界状況
  - 機能セットの必要性
  - スケーラビリティ
  - 管理の容易性
  - コスト

  カスタマーのビジネス ニーズに分散型コール処理モデルがふさわしいと判断する場合は、2 つの選択肢があります。ローカルに Cisco Unified CallManager サーバをインストールする方法と、支店ルータ上で Cisco Unified CallManager Express を稼働する方法です。

リモート サイトのサバイバビリティ（呼処理の継続）

集中型コール処理モデルで WAN を介した IP テレフォニーを配置する場合、リモート サイトのデータ サービスと音声サービスの高可用性を確保するために、追加の処置が必要です。表 2-1 では、リモート サイトでの高可用性を提供するためのさまざまな方法をまとめています。これらの方法のどれを選択するかは、ビジネスまたはアプリケーションの特殊な要件、可用性が高いデータ サービスと音声サービスに関連した優先順位、コストの考慮事項などの複数の要素によって異なります。

表 2-1　リモート サイトの高可用性を提供する方法

方法	データ サービスの高可用性	音声サービスの高可用性
支店ルータにおける冗長 IP WAN リンク	あり	あり
支店ルータの冗長プラットフォーム + 冗長 IP WAN リンク	あり	あり
SRST（Survivable Remote Site Telephony）のみ	なし	あり
データのみの ISDN バックアップ + SRST	あり	あり
データと音声の ISDN バックアップ	あり	あり（下記の規則を参照）

表 2-1 にリストされている最初の 2 つのソリューションは、IP WAN アクセス ポイントに冗長性を追加して、リモート IP Phone と中央の Cisco Unified CallManager との間の IP 接続を常に保持することによって、ネットワーク インフラストラクチャ層に高い可用性を提供します。これらのソリューションは、データ サービスと音声サービスの両方に適用され、コール処理層からはまったく見えません。このオプションは、支店ルータでの冗長 IP WAN リンクの追加から、冗長 IP WAN リンクを備えた 2 つ目の支店ルータ プラットフォームの追加までにわたります。

表 2-1 にリストされている 3 番目のソリューションでは、WAN 障害が検出された場合、SRST（Survivable Remote Site Telephony）が、リモート オフィスのルータ内でコール処理機能のサブセットを提供し、IP Phone を拡張して、ローカル ルータ内のコール処理機能に「re-home」機能を提供することによって、音声サービスのみの高い可能性を提供します。図 2-3 では、SRST を使用した典型的なコールのシナリオを示しています。

図 2-3　Survivable Remote Site Telephony（SRST）アプリケーションのシナリオ

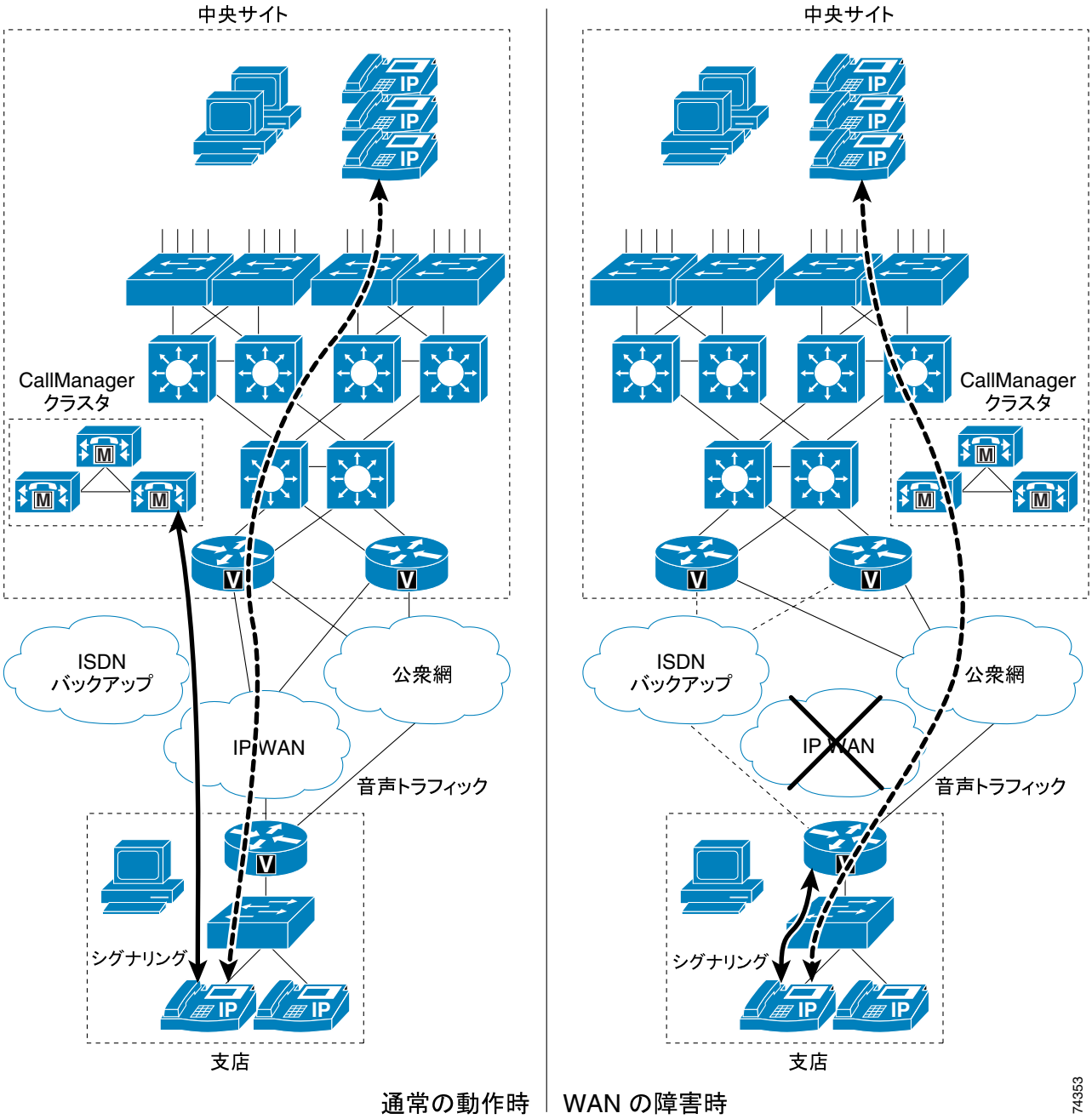


図 2-3 の左側に表示されている通常の動作では、支店は、データ トラフィック、音声トラフィック、およびコール シグナリングを伝送する IP WAN を経由して、中央サイトに接続されます。支店の IP Phone は、中央サイトの Cisco Unified CallManager クラスタとコール信号情報を交換し、IP WAN を介してコールを発信します。支店のルータまたはゲートウェイは、両方のタイプのトラフィック（コール信号と音声）を透過的に転送し、IP Phone を認識しません。

支店との WAN リンクに障害が起きた場合、またはその他のなんらかのイベントにより、Cisco Unified CallManager クラスタとの接続が失われた場合、支店の IP Phone は支店のルータに再登録されます。支店のルータは、設定について IP Phone に照会し、この情報を使用して独自の設定を自動的に作成します。支店の IP Phone は、内部で、または公衆網を介してコールの発信と受信を行うことができます。電話機は「Unified CM fallback mode」というメッセージを表示し、Cisco Unified CallManager の一部の拡張機能が利用不能になり、電話機のディスプレイでグレー表示されます。

中央サイトとの WAN 接続が再度確立されると、支店の IP Phone は、Cisco Unified CallManager クラスタに自動的に再登録され、正常な動作に戻ります。支店のルータは、IP Phone についての情報を削除し、標準のルーティングまたはゲートウェイ設定に戻ります。

表 2-1 の最後の 2 つのソリューションでは、ISDN バックアップ リンクを使用して、WAN 障害時の存続可能性を提供します。ISDN バックアップ用には、次の 2 つの配置オプションがあります。

- データのみの ISDN バックアップ

  このオプションでは、ISDN はデータのみの存続可能性の確保に使用され、一方 SRST は音声の存続可能性の確保に使用されます。IP Phone からの信号が中央サイトの Cisco Unified CallManager に到達しないようにするために、SCCP（Skinny Client Control Protocol）トラフィックが ISDN インターフェイスに入るのを防ぐように、支店ルータでアクセス コントロール リストを設定する必要があることに注意してください。
- データと音声の ISDN バックアップ

  このオプションでは、ISDN はデータと音声の両方の存続性を確保するのに使用されます。この場合、IP Phone は常に Cisco Unified CallManager クラスタとの IP 接続を保持するので、SRST は使用されません。しかし、データと音声のトラフィックの転送に ISDN を使用するのは、次の条件がすべて満たされる場合だけにすることをシスコはお勧めします。
  - ISDN リンク上で音声トラフィックに割り当てられた帯域幅が、IP WAN リンク上で音声トラフィックに割り当てられた帯域幅と同じである。
  - ISDN リンクの帯域幅が固定されている。
  - 必要なすべての QoS 機能が、ルータの ISDN インターフェイスに配置されている。QoS の詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章を参照してください。

集中型コール処理のバリエーションとしての Voice Over the PSTN

集中型コール処理配置モデルは、サイト間音声メディアが WAN の代わりに公衆網を介して送信されるように調整できます。このように設定された場合、すべてのテレフォニー エンドポイントのシグナリング（コール制御）は、引き続き中央の Cisco Unified CallManager クラスタによって制御されます。したがって、この Voice over the PSTN（VoPSTN）モデル バリエーションでも、シグナリング トラフィック用に設定された適切な帯域幅を持つ、QoS 対応の WAN が必要になります。

VoPSTN は、次のいずれかの方法で実装できます。

- Automated Alternate Routing（AAR; 自動代替ルーティング）機能を使用する（AAR の詳細については、P.10-28 の「Automated Alternate Routing」の項を参照してください）。
- Cisco Unified CallManager と公衆網ゲートウェイの両方のダイヤル プラン構成要素を組み合せて使用する。

VoPSTN が魅力的なオプションとなる可能性があるのは、IP WAN 帯域幅が不足しているか、または公衆網料金と比較して高価である配置や、IP テレフォニー システムがすでに配置されている状況で IP WAN 帯域幅のアップグレードを計画している配置です。

（注） VoPSTN 配置モデル バリエーションでは、まさにその性質のために、Cisco Unified CallManager 機能セットの一部を削減した基本的な音声機能が提供されます。

システム設計者は、実装時の選択内容に関係なく、特に次の問題に対処する必要があります。

- 集中型ボイスメールには、次の要件があります。
  - 配置に含まれているすべてのロケーションに対して Redirected Dialed Number Identification Service（RDNIS）エンドツーエンドをサポートする、テレフォニー ネットワーク プロバイダー。RDNIS は、ボイスメールにリダイレクトされるコールがリダイレクト元の DN を搬送するために必要となります。その結果、ボイスメール ボックスが正しく選択されることが保証されます。
  - ボイスメール システムが MGCP ゲートウェイを介してアクセスされる場合、ボイスメールのパイロット番号は完全修飾 E.164 番号である必要があります。
- エクステンション モビリティ機能は、単一の支店サイトにある IP Phone に制限されます。
- オンネット（クラスタ内）コールはすべて、オフネット（公衆網）コールと同じコール処理によって宛先の電話機に送信されます。この対象には、Missed Calls や Received Calls などのコール ディレクトリに送信される桁数も含まれます。
- 支店間コールはそれぞれ、2 つの独立した Call Detail Record（CDR; コール詳細レコード）を生成します。1 つは、発信側の電話機から公衆網へのコール レッグに対応するもので、もう 1 つは、公衆網から着信側の電話機へのコール レッグに対応するものです。
- オンネット コールとオフネット コールの呼出音タイプを区別する手段はありません。
- 宛先の電話機すべてにおいて、直接発信できる完全修飾 Direct Inward Dial（DID; ダイヤルイン方式）の公衆網番号が必要になります。DID 以外の DN に別の支店サイトから直接到達することはできません。
- VoPSTN を使用する際、Music On Hold（MoH）は、保留側が MoH リソースと同じ場所にある場合に限り使用されます。MoH サーバが中央サイトに配置されている場合は、中央サイトのデバイスによって保留にされたコールのみが保留音を受信します。
- 支店サイトの外部の宛先に着信転送すると、支店のゲートウェイを介したヘアピンコールが発生します。支店のゲートウェイのトラフィック エンジニアリングを、必要に応じて調整する必要があります。
- 支店のゲートウェイに着信するコールを支店サイトの外部の宛先にコール転送すると、ゲートウェイを介したヘアピンコールが発生し、2 つのトランク ポートが使用されます。この動作は、次の場合に発生します。
  - 支店の外部にあるボイスメール システムにコールが転送される場合
  - 別の支店にあるオンネットの内線番号にコールが転送される場合

  支店と公衆網を接続するトランクのサイズを選定するときは、このコール転送フローによるゲートウェイ ポートの使用率を考慮する必要があります。
- 会議リソースは、会議を開始する電話機と同じ場所にある必要があります。
- VoPSTN は、中央サイトに IP オーディオのストリーミングを要求する（つまり、ゲートウェイを通過しない）アプリケーションをサポートしません。このアプリケーションには、次のようなものがあります。
  - 集中型 Music On Hold（MoH）サーバ
  - IVR
  - CTI ベースのアプリケーション
- 中央サイトの外部で Attendant Console を使用する場合、リモート サイトがキャッシングしないで大規模なユーザ アカウント ディレクトリにアクセスする必要があるときは、かなり大きな帯域幅が必要になることがあります。
- 支店間メディア（着信転送を含む）はすべて公衆網を介して送信されるため、支店間トラフィック、着信転送、および集中型ボイスメール アクセスのすべてを収容できるように、ゲートウェイ トランク グループの回線数を調整する必要があります。
- シェアドラインを支店間に配置して、回線を共有するデバイスを別々の支店に配置することは避けるようお勧めします。

このような一般的な考慮事項のほか、以降の項では、次の実装方法のそれぞれに固有の推奨事項や問題について説明します。

- AAR を使用する VoPSTN（P.2-13）
- ダイヤル プランを使用する VoPSTN（P.2-14）

AAR を使用する VoPSTN

この方法では、Cisco Unified CallManager ダイヤル プランを従来の集中型コール処理配置として設定し、さらに自動代替ルーティング（AAR）機能を正しく設定します。コール アドミッション制御のロケーション メカニズムによって、新たなコールを受け入れるのに十分な WAN 帯域幅がないと判別された場合、AAR は、サイト間コールを公衆網を介して透過的に再ルーティングします。

公衆網をプライマリ（および唯一の）音声パスとして使用するには、各ロケーション（支店サイト）のコール アドミッション制御の帯域幅を 1 Kbps に設定します。この設定により、すべてのコールが WAN を通過することが防止されます。このように設定されている場合、サイト間コールはすべて AAR 機能をトリガーし、AAR 機能は公衆網を介してコールを再ルーティングします。

VoPSTN の AAR 実装方法には、次の利点があります。

- 完全な IP テレフォニー配置に簡単に移行できます。WAN を介した音声メディアをサポートする帯域幅が使用可能になった場合、ダイヤル プランはそのまま保持できるため、変更作業としては、サイトごとにロケーション帯域幅の値をアップデートするだけで済みます。
- 通話中のコールバックなど、一部の補足機能がサポートされます。

AAR 実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

- AAR 機能を正しく設定する必要があります。
- 一般に、サポートされているデバイスには、IP Phone、ゲートウェイ、およびアナログ電話機を収容するゲートウェイがあります。
- 支店間コールが AAR を使用できるのは、宛先デバイスが IP Phone または Cisco Unity ポートの場合のみです。
- 他のエンドポイントに対する支店間コールは、完全修飾 E.164 番号を使用する必要があります。
- すべてのオンネット支店間コールでは、「Network congestion, rerouting」というメッセージが表示されます。
- 宛先の電話機が登録から外れている場合（たとえば、WAN 接続の通信断が原因で）、AAR 機能は起動されないため、省略ダイヤリングは使用できなくなります。宛先の電話機が SRST ルータに登録されている場合は、その公衆網 DID 番号を直接ダイヤルすることで、宛先に到達できます。
- 発信側の電話機が登録から外れている場合（たとえば、WAN 接続の通信断が原因で）、その電話機は SRST モードに移行します。このような状況で省略ダイヤリング機能を保持するには、SRST ルータに適切なトランスレーション ルールを設定します。
- 同じ支店内のシェアドラインは、その支店のコーリング サーチ スペースのみに含まれているパーティション内に設定される必要があります。シェアドラインへのサイト間アクセスには、次のどちらかの操作が必要です。
  - 発信側サイトでシェアドラインの DID 番号をダイヤルします。
  - シェアドラインへのサイト間省略ダイヤリングが必要な場合は、ユーザがダイヤルした省略ストリングをシェアドラインの DID 番号へと変換するトランスレーション パターンを使用します。

（注） この場合、シェアドラインの DN を別の支店から直接ダイヤルすると、AAR ベースの公衆網コールが複数トリガーされます。

ダイヤル プランを使用する VoPSTN

この方法は、Cisco Unified CallManager 内の特定のダイヤル プラン設定と公衆網ゲートウェイを利用して、すべてのサイト間コールを公衆網を介してルーティングします。ダイヤル プランでは、各サイトの IP Phone の DN を別のパーティションに配置する必要があります。また、その DN のコーリング サーチ スペースは、サイトの内部パーティションと、ローカル公衆網ゲートウェイが関連付けられているルート パターンのみにアクセスする必要があります。

サイト間省略ダイヤリングは、各支店サイトの変換セット（支店サイトごとに 1 セット）からも使用可能です。この変換は、Cisco IOS 内の H.323 ゲートウェイと変換規則を使用して行うのが最適です。

VoPSTN のダイヤル プラン実装方法には、次の利点があります。

- AAR が必要ないため設定が容易になります。
- 発信側または宛先側のどちらかで WAN 障害が発生した状態でも、省略ダイヤリングは自動的に動作します。これは、H.323 ゲートウェイ内の Cisco IOS 変換規則が SRST モードで有効になるためです。

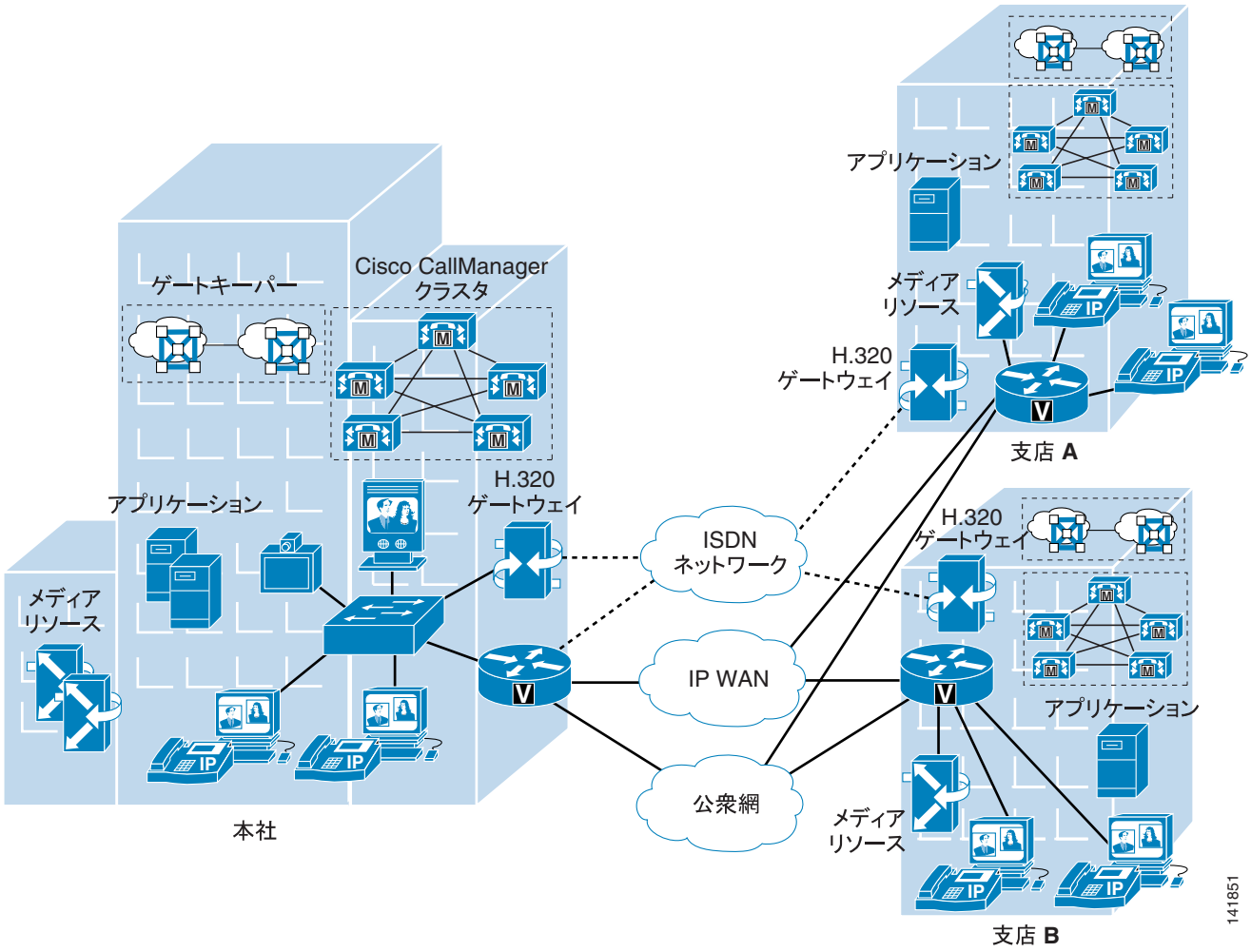
ダイヤル プラン実装方法には、VoPSTN について示した一般的な考慮事項のほかに、次の設計ガイドラインが適用されます。

- 通話中のコールバックなど、補足機能はサポートされません。
- CTI ベースのアプリケーションの中には、重複している内線番号（つまり、別々のパーティションにあるが、同じ DN が設定されている複数の電話機）をサポートしないものがあります。
- 完全な IP テレフォニー配置に簡単に移行することはできません。これは、ダイヤル プランの再設計が必要になるためです。

分散型コール処理を使用するマルチサイト WAN

分散型コール処理を使用するマルチサイト WAN モデルでは、複数の独立したサイトから構成されています。各サイトには独自のコール処理エージェントがあり、そのエージェントは、分散サイト間の音声トラフィックを伝送する IP WAN に接続されます。図 2-4 は、一般的な分散型コール処理配置を示しています。

図 2-4　分散型コール処理を使用するマルチサイト配置モデル



分散型コール処理モデルの各サイトは、次のいずれかになります。

- 独自のコール処理エージェントを使用する単一サイト。コール処理エージェントは、次のいずれかになります。
  - Cisco Unified CallManager
  - Cisco Unified CallManager Express
  - その他の IP PBX
- 集中型コール処理サイトと、それに関連したすべてのリモート サイト。
- Voice over IP（VoIP）ゲートウェイを備えたレガシー PBX。

分散型コール処理を使用するマルチサイト モデルの設計上の特長は、次のとおりです。

- クラスタあたり最大 30,000 の Skinny Client Control Protocol（SCCP）または Session Initiation Protocol（SIP）IP Phone または SCCP ビデオ エンドポイント。
- Cisco Unified CallManager クラスタあたり最大 500 の H.323 デバイス（ゲートウェイ、MCU、トランク、およびクライアント）。
- すべての外部コールに対して公衆網で対応。
- 会議、トランスコーディング、および Media Termination Point（MTP; メディア ターミネーション ポイント）に対してデジタル シグナル プロセッサ（DSP）リソースで対応。
- ボイスメールまたはユニファイド メッセージング コンポーネント。
- レガシー Private Branch Exchange（PBX; 構内交換機）システムおよびボイスメール システムとの統合機能。
- コールを発信するためにゲートキーパーを必要とする H.323 クライアント、MCU、および H.323/H.320 ゲートウェイを、Cisco IOS ゲートキーパー（Cisco IOS リリース 12.3(8)T 以降）に登録することが必要。Cisco Unified CallManager は H.323 トランクを使用してゲートキーパーと統合し、そこに登録された H.323 デバイスのコール ルーティングと帯域幅管理サービスを提供します。複数の Cisco IOS ゲートキーパーを使用して、冗長性を提供することもできます。Cisco IOS ゲートキーパーを使用して、分散した Cisco Unified CallManager クラスタ間でコール ルーティングおよび帯域幅管理を提供することもできます。多くの場合、Cisco Unified CallManager クラスタごとに専用のエンドポイント ゲートキーパーを持ち、それとは別のゲートキーパーを使用してクラスタ間コールを管理することを推奨します。状況によっては、ネットワークのサイズやダイヤル プランの複雑さに応じて、同じゲートキーパーを両方の機能に使用することもできます（詳細については、P.15-24 の「ゲートキーパー」を参照してください）。
- マルチポイント ビデオ会議のクラスタごとに MCU リソースが必要。会議の要件に応じて、SCCP または H.323、あるいはその両方がリソースとして必要です。すべてのリソースがリージョン サイトに存在していても、ローカル会議リソースが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 公衆 ISDN 網の H.320 ビデオ会議デバイスとの通信に H.323/H.320 ビデオ ゲートウェイが必要。これらのゲートウェイはリージョン サイトにあっても、ローカル ISDN アクセスが必要な場合は各クラスタのリモート サイトに分散していてもかまいません。
- 同じサイト内のデバイス間の広帯域オーディオ（G.711、G.722、Cisco Wideband Audio など）、異なるサイトのデバイス間の狭帯域オーディオ（G.729、G.728 など）。
- 同じサイト内のデバイス間の広帯域ビデオ（384 kbps 以上など）、異なるサイトのデバイス間の狭帯域ビデオ（128 kbps など）。同じサイト内のデバイス間のコールに限っては、7 Mbps で動作する Cisco Unified Video Advantage Wideband Codec を推奨します。ただし、Cisco VT Camera Wideband Video Codec はクラスタ間トランクでサポートされていません。
- 最大 768 kbps 以上の WAN リンク速度。速度が 768 kbps 未満の WAN 接続ではビデオを*推奨しません*。
- コール アドミッション制御は、同じ Cisco Unified CallManager クラスタで制御されるサイト間のコールに対しては Cisco Unified CallManager のロケーションから提供され、Cisco Unified CallManager クラスタ間のコールに対しては Cisco IOS ゲートキーパーから提供されます（クラスタ間トランク）。クラスタ内とクラスタ間の両方のビデオ コールに対して、自動代替ルーティング（AAR）もサポートされます。

IP WAN は、分散型コール処理のサイトをすべて相互接続します。一般に、公衆網は、IP WAN 接続に障害が起きたか、使用可能な帯域幅がすべて消費されてしまった場合に、サイト間のバックアップ接続の役目を果たします。公衆網のみで接続されているサイトは、独立サイトであり、分散型コール処理モデルには含まれません（P.2-3 の「単一サイト」を参照）。

IP WAN の接続オプションは、次のとおりです。

- 専用回線
- フレーム リレー
- 非同期転送モード（ATM）

- ATM とフレーム リレーのサービス インターワーキング（SIW）
- Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）
- 音声およびビデオ対応 IP Security Protocol VPN（IPSec VPN（V3PN））

分散型コール処理モデルの利点

分散型コール処理を使用するマルチサイト WAN モデルには、次の利点があります。

- サイト間のコールに IP WAN を使用する場合の公衆網コール コストの節約。
- IP WAN を使用し、公衆網着信番号に近いリモート サイトのゲートウェイを通じてのコールの転送による通話料金の回避。この方法は Tail-End Hop-Off（TEHO）と呼ばれます。
- 音声トラフィックが他のタイプのトラフィックと IP WAN を共有できるようにすることによる、使用可能な帯域幅の最大限の利用。
- 各サイトのコール処理エージェントの存在による、IP WAN の障害時の機能の保全。
- 数百のサイトへのスケーラビリティ。

分散型コール処理モデルのベスト プラクティス

分散型コール処理を使用するマルチサイト WAN 配置には、単一サイト、または集中型コール処理を使用するマルチサイト WAN 配置と同じ要件が少なからずあります。分散型コール処理モデルについては、ここでリストされているベスト プラクティスに加えて、他のモデルのベスト プラクティスにも従ってください（P.2-3 の「単一サイト」および P.2-6 の「集中型コール処理を使用するマルチサイト WAN」を参照）。

ゲートキーパーまたは Session Initiation Protocol（SIP）プロキシ サーバは、分散型コール処理を使用するマルチサイト WAN モデルの重要な要素です。どちらもダイヤル プランの解決を行います。さらに、ゲートキーパーは、コール アドミッション制御も行います。ゲートキーパーは、コール アドミッション制御と E.164 ダイヤル プラン解決を実行する H.323 デバイスです。

ゲートキーパーの使用には、次のベスト プラクティスが適用できます。

- Cisco IOS ゲートキーパーを使用して、各サイトとのコール アドミッションを制御します。
- ゲートキーパーの有効性を高めるには、HSRP（ホットスタンバイ ルータ プロトコル）ゲートキーパー ペア、ゲートキーパーのクラスタ化、および代替ゲートキーパー サポートを使用します。さらに、ネットワーク内の冗長性を確実にするために複数のゲートキーパーを使用します（P.8-22 の「ゲートキーパーの設計上の考慮事項」を参照）。
- プラットフォームの規模を適切に調整して、パフォーマンスとキャパシティの要件が満たされることを確認します。
- WAN 上のコーデックは 1 つのタイプに限定して使用します。これは、H.323 仕様では、レイヤ 2、IP、UDP（User Data Protocol）、または RTP（Real-time Transport Protocol）ヘッダーのオーバーヘッドが、帯域幅要求で許可されないからです（ヘッダーのオーバーヘッドは、パケットのペイロードまたは符号化された音声部分のみで許可されます）。WAN 上で使用するコーデックを 1 つのタイプに限定すると、最悪のシナリオに備えて IP WAN を過剰にプロビジョニングする必要がなくなるので、キャパシティ プランニングが簡単になります。
- ゲートキーパー ネットワークは、数百単位のサイトにスケーラブルです。また、設計上の制限は WAN トポロジからしか受けません。

ゲートキーパーが実行する各種機能の詳細については、次の項を参照してください。

- ゲートキーパーのコール アドミッション制御については、P.9-1 の「コール アドミッション制御」を参照してください。
- ゲートキーパーのスケーラビリティと冗長性については、P.8-1 の「コール処理」を参照してください。

- ゲートキーパーのダイヤル プラン解決については、P.10-1 の「ダイヤル プラン」を参照してください。

SIP デバイスは、E.164 番号と SIP ユニフォーム リソース識別子（URI）を解決して、エンドポイント間で相互にコールを発信できるようにします。Cisco Unified CallManager は、E.164 番号の使用のみをサポートします。

SIP プロキシの使用には、次のベスト プラクティスが適用できます。

- SIP プロキシの適切な冗長性を確保します。
- SIP プロキシのキャパシティが、ネットワークに必要なコール レートおよびコール数に対応していることを保証します。
- コール アドミッション制御のプランニングは、このドキュメントの対象外です。

分散型コール処理モデルのコール処理エージェント

コール処理エージェントの選択は、多くの要素によって異なります。設計での主な要素は、サイトの規模および機能要件です。

分散型コール処理配置の場合、各サイトには独自のコール処理エージェントがあります。各サイトの設計は、コール処理エージェント、必要な機能、および必要な耐障害性によって変わります。たとえば、500 台の電話機を備えたサイトでは、2 つのサーバを含む Cisco Unified CallManager クラスタは、1 対 1 の冗長性を提供することができ、バックアップ サーバは、パブリッシャおよび TFTP（トリビアル ファイル転送プロトコル）サーバとして使用されます。

IP ベース アプリケーションの要件も、コール処理エージェントの選択に大きな影響を与えます。これは、多くの Cisco IP アプリケーションをサポートするのは、Cisco Unified CallManager だけであるからです。

表 2-2 は、推奨されるコール処理エージェントを示しています。

表 2-2　推奨されるコール処理エージェント

コール処理エージェント	推奨規模	備考
Cisco Unified CallManager Express（CME）	最大 240 台の電話機	• 小規模なリモート サイト用 • キャパシティは Cisco IOS プラットフォームに依存する
Cisco Unified CallManager	50 ～ 30,000 台の電話機	• Cisco Unified CallManager クラスタの規模に応じて、小規模から大規模までのサイト • 集中型または分散型コール処理をサポートする
VoIP ゲートウェイを備えた従来の PBX	PBX に依存する	• IP WAN コール数と機能は、PBX と VoIP ゲートウェイを接続するプロトコルおよびゲートウェイ プラットフォームによって異なる

IP WAN を介したクラスタ化

QoS 機能に対応している IP WAN によって相互接続される複数サイト間で、単一の Cisco Unified CallManager クラスタを配置できます。ここでは、WAN を介したクラスタ化の概要を簡潔に説明します。詳細については、P.8-1 の「コール処理」の章を参照してください。

WAN を介したクラスタ化では、次の 2 種類の配置方法がサポートされます。

- ローカル フェールオーバー配置モデル（P.2-23）

  ローカル フェールオーバーでは、Cisco Unified CallManager サブスクライバ サーバとバックアップ サーバを同じサイトに配置し、これらのサーバ間に WAN を置かないことが必要です。この配置モデルは、Cisco Unified CallManager を備えた 2 ～ 4 つのサイトに理想的です。

- リモート フェールオーバー配置モデル（P.2-27）

  リモート フェールオーバーでは、WAN を介してバックアップ サーバを配置できます。この配置モデルを使用すると、Cisco Unified CallManager サブスクライバ サーバを備えた最大 8 つのサイトを、別のサイトにある Cisco Unified CallManager サブスクライバでバックアップすることが可能です。

また、2 つの配置モデルを組み合せて、特定のサイト要件を満たすことも可能です。たとえば、2 つのメイン サイトにプライマリ サブスクライバとバックアップ サブスクライバを配置し、別の 2 つのサイトにはそれぞれプライマリ サーバのみを配置し、2 つのメイン サイトにある共用バックアップまたは専用バックアップのどちらかを使用することができます。

WAN を介したクラスタ化の主な利点は、次のとおりです。

- クラスタ内の全サイトに対してユーザを 1 箇所で管理
- 機能の透過性
- シェアドライン アピアランス
- クラスタ内のエクステンション モビリティ
- 統一ダイヤル プラン

これらの機能により、このソリューションは、ビジネスが継続して行われるサイトの障害回復プランとして、または最大 8 つの中小規模サイト用の単一ソリューションとして理想的なものになります。

WAN の考慮事項

WAN を介したクラスタ化が成功するには、WAN 自体のさまざまな特性を慎重に計画し、設計し、実装する必要があります。Cisco Unified CallManager サーバ間の Intra-Cluster Communication Signaling（ICCS）は、複数のトラフィック タイプから構成されます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。さまざまなタイプの ICCS トラフィックについては、P.2-20 の「クラスタ内通信」で説明されています。この項では、プロビジョニングについてのさらに詳しいガイドラインも記述されています。WAN の特性には、次の設計上のガイドラインが適用されます。

- 遅延

  すべての優先 ICCS トラフィックに対する、任意の Cisco Unified CallManager サーバ間の片方向の最大遅延は 20 ms、つまり 40 ms Round-Trip Time（RTT; ラウンドトリップ時間）以下でなければなりません。その他の ICCS トラフィックの遅延は、タイムリーにデータベースとディレクトリにアクセスするために、妥当なものでなければなりません。遅延の測定については、P.2-22 の「遅延のテスト」を参照してください。2 つのサイト間の伝搬遅延は、他のネットワーク遅延を考慮しない場合、1 キロメートル当たり 6 マイクロ秒になります。これは、20 ms 遅延

に対して理論的な最大距離約 3000 km、つまり約 1860 マイルに相当します。この距離は、相対的なガイドラインとしてのみ記載されています。実際には、ネットワーク内の他の遅延により、これより短くなります。

- ジッタ

  ジッタは、処理、キュー、バッファ、輻輳、またはパス変動遅延により、パケットがネットワークを介して受ける変動遅延です。IP Precedence 3 ICCS トラフィックのジッタは、QoS 機能を使用して最小限に抑える必要があります。

- パケット損失とエラー

  ネットワークは、すべての ICCS トラフィック、特に優先 ICCS トラフィックに対して、十分な優先順位付き帯域幅を提供するように設計される必要があります。標準的な QoS メカニズムを実装して、輻輳とパケット損失を回避する必要があります。回線エラーや他の「現実的な」状況によってパケットが損失した場合、ICCS パケットは再送信されます。これは、高信頼性伝送のために TCP プロトコルが使用されているからです。再送信が行われると、セットアップ、接続解除（終了）、または他の補足サービスの実行中に、コールが遅延する場合があります。パケット損失の状況によっては、コールが失われる可能性があります。ただし、このシナリオ以上に、T1 または E1 上でエラーが発生することが考えられます。このエラーは、トランクを介した公衆網 /ISDN へのコールに影響を及ぼします。

- 帯域幅

  予想されるコール ボリューム、デバイスのタイプ、およびデバイス数に対して、各サーバ間で適切な帯域幅を提供してください。この帯域幅は、サイト間の音声や映像のトラフィックを含めて、ネットワークを共有する他のアプリケーション用のその他の帯域幅とは別に必要です。提供される帯域幅では、さまざまなクラスのトラフィックに優先順位付けとスケジューリングを行うために、QoS が使用可能になっていなければなりません。帯域幅は、一般的に多めに設定し、少なめにサブスクライブします。

- QoS

  ネットワーク インフラストラクチャは、QoS 技術を使用して、一貫した予測可能なエンドツーエンド レベルのサービスをトラフィックに提供します。QoS も帯域幅も、それだけでは解決法になりません。QoS が使用可能になった帯域幅を、ネットワーク インフラストラクチャに設計する必要があります。

クラスタ内通信

一般に、クラスタ内通信とは、サーバ間のすべてのトラフィックを意味します。Intra-Cluster Communication Signaling（ICCS）と呼ばれるリアルタイム プロトコルもあります。このプロトコルは、クラスタ内の各サーバまたはノードにおけるコール処理の中心である、Cisco CallManager Service プロセスとの通信を提供します。

サーバ間のクラスタ内トラフィックは、次のものから構成されます。

- 主な設定情報を提供する IBM Informix Dynamic Server（IDS）データベースからのデータベース トラフィック。IDS データベースは、ベストエフォートを使用して、パブリッシャ サーバから、クラスタ内の他のすべてのサーバに複製されます。IDS トラフィックは、Cisco QoS の推奨事項に沿って再優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。この一例は、IDS データベース設定を使用する、エクステンション モビリティの拡張使用です。
- サブスクライバをパブリッシャに認証し、パブリッシャのデータベースにアクセスするために使用されるファイアウォール管理トラフィック。管理トラフィックは、クラスタ内のすべてのサーバ間を通過します。管理トラフィックは、Cisco QoS の推奨事項に沿って優先順位付けが行われ、より高い優先順位のデータ サービスになります（たとえば、特定のビジネス ニーズによって必要な場合は IP Precedence 1）。
- ICCS リアルタイム トラフィック。このトラフィックは、シグナリング、コール アドミッション制御、および開始と終了時のコールについてのその他の情報から構成されます。ICCS は、Cisco CallManager Service が使用可能になっているすべてのサーバ間で、伝送制御プロトコル（TCP）接続を使用します。この接続は、これらのサーバ間でフルメッシュです。クラスタに

は、Cisco CallManager Service が使用可能になっているサーバが 8 つしかないので、各サーバには最大 7 つの接続が可能です。このトラフィックは、優先 ICCS トラフィックであり、Cisco CallManager リリースおよびサービス パラメータ設定に応じてマークされます。

- CTI Manager リアルタイム トラフィック。このトラフィックは、コールに関係する CTI デバイスに使用されるか、Cisco Unified CallManager サーバ上のその他のサードパーティ製デバイスの制御または監視に使用されます。このトラフィックは、優先 ICCS トラフィックとしてマークされ、CTI Manager を備えた Cisco Unified CallManager サーバと、CTI デバイスを備えた Cisco Unified CallManager サーバとの間に存在します。

サブスクライバ サーバ間のフェールオーバー

Cisco Unified CallManager 5.0 を使用すると、初期化時またはブートアップ時にデバイス設定レコードがキャッシュされます。その結果、Cisco Unified CallManager の初期化に時間がかかることはありますが、パブリッシャ データベースへのアクセス時の遅延によって、すべてのデバイスのフェールオーバーまたはフェールバックが影響を受けることはありません。

Cisco Unified CallManager パブリッシャ

パブリッシャは、マスター データベースの読み取り専用コピーをクラスタ内の他のすべてのサーバに複製します。クラスタ内の別のサーバが通信不能である期間に、パブリッシャのマスター データベースに変更が加えられた場合、パブリッシャは、通信が再確立されたときに、更新されたデータベースを複製します。パブリッシャが通信不能であるか、オフラインになっている期間、コンフィギュレーション データベースに変更を加えることはできません。サブスクライバ データベースはすべて、読み取り専用であり、変更できません。クラスタの通常の操作の大部分は、以下を含めて、この期間には影響を受けません。

- コール処理
- フェールオーバー
- 設定済みデバイスのインストレーション登録

一部の機能には、パブリッシャ上のマスター データベースへのアクセス権が必要です。これは、これらの機能がレコードに変更を加えるために書き込みアクセス権が必要であるからです。パブリッシャは、コンフィギュレーション データベースへの読み取りと書き込みアクセス権がある、Cisco Unified CallManager クラスタ内の唯一のサーバです。パブリッシャへの書き込みアクセス権が必要な主な機能には、次のものがあります。

- 設定の追加、変更、および削除
- エクステンション モビリティ
- ユーザ短縮ダイヤル
- データベースを必要とする Cisco Unified CallManager User ページのオプション
- Cisco Unified CallManager ソフトウェアのアップグレード
- 全転送の変更
- メッセージ待機インジケータ（MWI）の状態

これ以外のサービスやアプリケーションも影響を受ける場合があります。したがって、パブリッシャなしで機能するかどうかを配置時に確認する必要があります。

コール詳細レコード（CDR）

コール詳細レコードが使用可能である場合、各サブスクライバによって収集され、定期的にパブリッシャにアップロードされます。パブリッシャが通信不能である間、CDR は、サブスクライバのローカル ハードディスクに保存されます。パブリッシャとの接続が再確立されると、未処理の CDR はすべて、パブリッシャにアップロードされます。

遅延のテスト

任意の 2 つのサーバ間の最大ラウンドトリップ時間（RTT）は、常に 40 ms 以下でなければなりません。この制限には、この 2 つのサーバ間の伝送パスの遅延がすべて含まれる必要があります。Cisco Unified CallManager サーバで **ping** ユーティリティを使用してラウンドトリップの遅延を確認しても、正確な結果は得られません。ping は、ベストエフォート型のパケットとして送信されます。ICCS トラフィックと同じ QoS 対応パスを使用して転送されません。したがって、遅延を確認するには、Cisco Unified CallManager サーバに最も近いネットワーク デバイスを使用することをお勧めします。理想的には、サーバが接続されているアクセス スイッチです。Cisco IOS は、ICCS トラフィックが通過するのと同じ QoS 対応パス上で ping パケットが送信されるように、レイヤ 3 タイプ オブ サービス（ToS）ビットを設定できる拡張 ping を備えています。拡張 ping によって記録される時間は、ラウンドトリップ時間（RTT）、つまり通信パスを通過して戻るのに要する時間です。任意の 2 つの Cisco Unified CallManager サーバ間の最大 RTT は 40 ms です。したがって、片方向の最大遅延は 20 ms になります。この遅延は、Cisco Unified CallManager クラスタのコール処理機能のパフォーマンスに非常に重要であり、厳密に実行する必要があります。

次の例は、ToS ビット（IP Precedence）が 3 に設定された、Cisco IOS 拡張 ping です。

```
Access_SW#ping
Protocol [ip]:
Target IP address: 10.10.10.10
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 3
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte Intelligent Contact ManagementP Echos to 10.10.10.10, timeout
is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

エラー率

予想されるエラー率はゼロでなければなりません。エラー、パケットのドロップ、または IP ネットワークに対するその他の障害は、クラスタのコール処理パフォーマンスに影響を与える可能性があります。これは、ダイヤル トーンの遅延、IP Phone 上のキーやディスプレイの反応の遅れ、またはオフフックしてから音声パスの接続までの遅れによって気付く場合があります。Cisco Unified CallManager はランダム エラーに対する許容性がありますが、クラスタのパフォーマンス低下を避けるために、エラーを回避する必要があります。

トラブルシューティング

クラスタ内の Cisco Unified CallManager サブスクライバが、予想より高い遅延、エラー、またはパケットのドロップにより、ICCS 通信の障害を検出する場合、次の症状のいくつかが発生する場合があります。

- クラスタ内のリモート Cisco Unified CallManager サーバ上にある IP Phone、ゲートウェイ、またはその他のデバイスが、一時的に通信不能になることがあります。
- コールの接続が切断されたり、コールのセットアップ中に失敗する場合があります。
- ユーザにダイヤル トーンが聞こえるまでに、予想以上に長い遅延が起こる場合があります。
- Busy Hour Call Completions（BHCC）が低い場合があります。
- ICCS（SDL セッション）がリセットされたり、接続が切断されることがあります。次に、Cisco Unified CallManager SDL トレースの例を示します。このトレースでは、リモート サーバ VO30-7835-8 がサービス休止になり、そのサーバが通信可能であったデバイスが、「利用可能な」宛先として除去されます。

```
RemoteCMOutOfService: Ip address: VO30-7835-8 remoteClusterId
VO30-7835-1-Cluster|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2>
|Delete entries from SsManagerTable, now this table has 75
entries|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2><CT::0,0,0,0.0><IP::><DEV:
:>
|Delete entries from FeatActTable, now this table has 70
entries|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2><CT::0,0,0,0.0><IP::><DEV:
:>
|Digit analysis: Remove remote pattern /5000020 , PID:
7:34:1|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2><CT::0,0,0,0.0><IP::><DEV::
>
|Digit analysis: Remove remote pattern /5000066 , PID:
7:34:2|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2><CT::0,0,0,0.0><IP::><DEV::
>
.
.
.
|Digit analysis: Remove remote pattern /5001002 , PID:
7:34:106|<CLID::VO30-7835-1-Cluster><NID::VO30-7835-2><CT::0,0,0,0.0><IP::><DEV
::>
```

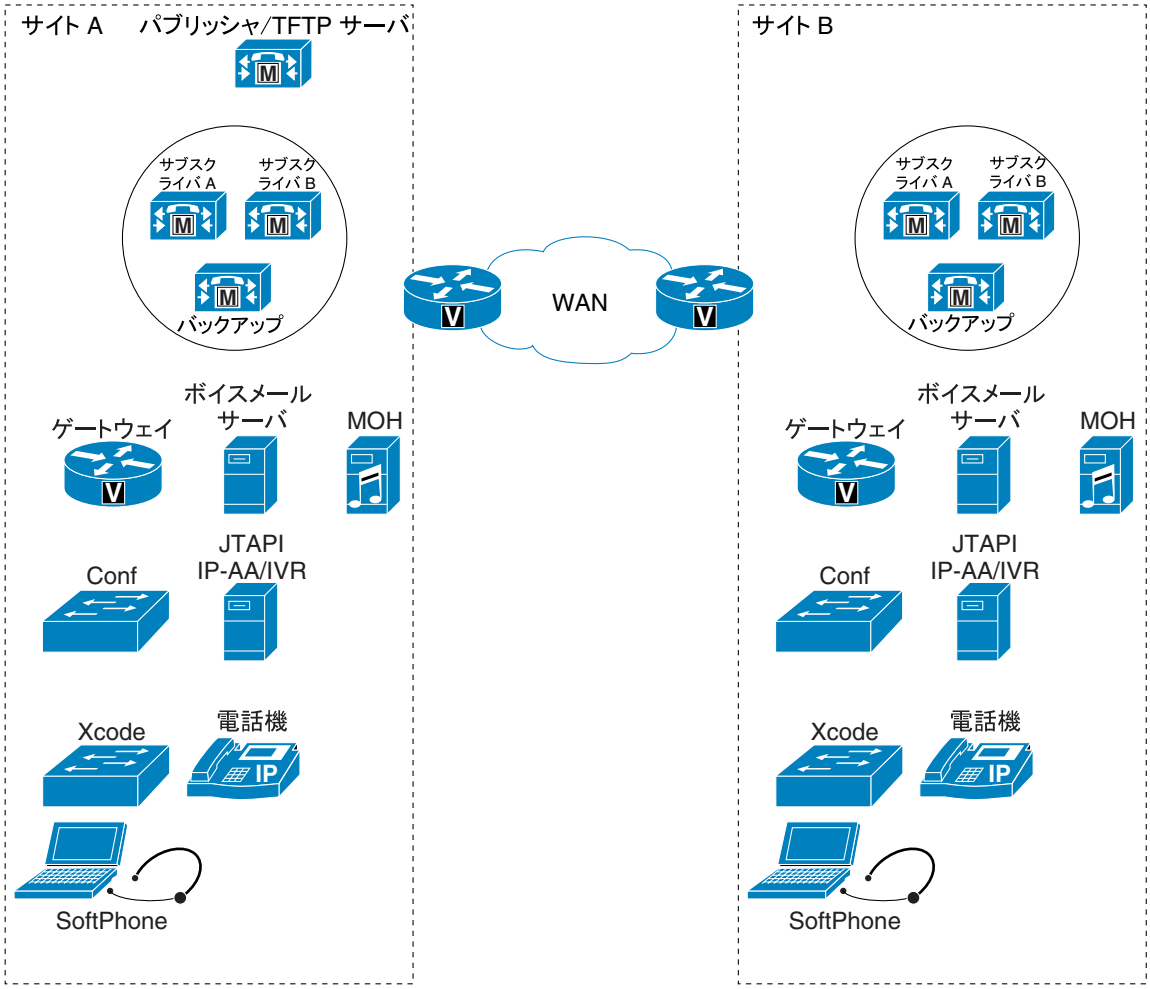
要約すると、ICCS 通信の問題のトラブルシューティングを行うには、次のタスクを実行します。

- サーバ間の遅延を検証する
- エラーやパケットのドロップがないかどうか、すべてのリンクを調べる
- QoS が正常に設定されていることを確認する
- すべてのトラフィックをサポートするために、キューに対して、WAN を介した十分な帯域幅が提供されることを確認する

ローカル フェールオーバー配置モデル

ローカル フェールオーバー配置モデルは、WAN を介したクラスタ化に対する最大の復元性があります。このモデルの各サイトには、少なくとも 1 つのプライマリ Cisco Unified CallManager サブスクライバと 1 つのバックアップ サブスクライバがあります。この設定では、最大 4 つのサイトをサポートできます。電話機および他のデバイスの最大数は、配置されているサーバの数とタイプによって異なります。全サイトの IP Phone の最大総数は 30,000 です（図 2-5 を参照）。

図 2-5　ローカル フェールオーバー モデルの例



リモート フェールオーバー モデルを実装する場合は、次のガイドラインに従ってください。

- 少なくとも 1 つのプライマリ Cisco Unified CallManager サブスクライバと 1 つのバックアップ サブスクライバを含むように、各サイトを設定します。
- Cisco Unified CallManager の *グループ*と *デバイス プール*を設定して、サイト内のデバイスが、あらゆる状況でそのサイトのサーバだけに登録されるようにします。
- 各サイトで主要なサービス（TFTP、DNS、DHCP、LDAP、および IP Phone サービス）、すべてのメディア リソース（コンファレンス ブリッジと Music On Hold）、およびゲートウェイを複製します。複製を確実に行い、最大レベルの復元性を得るよう、シスコは強くお勧めします。また、この方法を拡張して、各サイトにボイスメール システムを組み込むこともできます。
- WAN 障害が発生した場合、パブリッシャ データベースへのアクセスがないサイトでは、次に示すように、いくつかの機能を使用できないことがあります。
  - ローカル サイトのシステム管理者は、設定を一切追加、変更、または削除することができません。
  - エクステンション モビリティ ユーザは、IP Phone のログインまたはログアウトを行うことができません。
  - 全コール転送を変更することはできません。
- WAN 障害が発生した状態では、コールを発信するサブスクライバと現在通信していない電話番号にコールを発信すると、ファースト ビジー音が聞こえるか、またはコール転送されます（転送先の電話番号のロケーションによっては、ボイスメールに転送される可能性があります）。このような場合、ユーザは公衆網を介してその番号を手動でダイヤルする必要があります。

- WAN を介してクラスタ化されているサイト間で 10,000 BHCA（Busy Hour Call Attempt）が発生するたびに、Intra-Cluster Communication Signaling（ICCS）に 900 Kbps の帯域幅が必要です。これは、帯域幅の最小必要量であり、帯域幅は、900 kbps の倍数で割り当てられます。ICCS のトラフィック タイプは、優先またはベストエフォートのどちらかとして分類されます。優先 ICCS トラフィックには、IP Precedence 3（DSCP 24 または PHB CS3）が付けられます。ベストエフォート型 ICCS トラフィックには、IP Precedence 0（DSCP 0 または PHB BE）が付けられます。
- WAN を介してクラスタ化されているサイト間の推奨される最小帯域幅は、1.544 Mbps です。この量にすると、ICCS 用に最小 900 Kbps が確保され、データベースおよび他のサーバ間トラフィック用に最小 644 Kbps が確保されます。
- Cisco Unified CallManager クラスタ内の任意の 2 つのサーバ間では、最大ラウンドトリップ時間（RTT）として 40 ms まで許容されます。この時間は、単方向で最大 20 ms の遅延、または理想的な条件下での約 1860 マイル（3000 km）の伝送距離に相当します。
- 集中型コール処理を使用するリモート支店を、WAN を介したクラスタ化を使用してメイン サイトに接続する場合は、WAN を介したクラスタ化に使用されるリンクがオーバーサブスクリプションにならないよう、慎重にコール アドミッション制御を設定します。
  - WAN を介したクラスタ化に使用されるリンク上で帯域幅が制限されていない場合（つまり、リンクへのインターフェイスが OC-3s または STM-1s で、コール アドミッション制御に関する要件がない場合）は、リモート サイトがメイン サイトのいずれかに接続される場合があります。これは、すべてのメイン サイトでロケーションを Hub_None として設定する必要があるためです。この設定が行われても、コール アドミッション制御に使用するハブアンドスポーク トポロジは保持されます。
  - Multiprotocol Label Switching（MPLS）バーチャル プライベート ネットワーク（VPN）機能を使用している場合は、Cisco Unified CallManager ロケーションとリモート サイトにあるすべてのサイトが、メイン サイトのいずれかに登録される場合があります。
  - メイン サイト間の帯域幅が制限されている場合は、サイト間でコール アドミッション制御を使用し、ロケーションが Hub_None として設定されているメイン サイトにすべてのリモート サイトを登録する必要があります。このメイン サイトはハブ サイトと見なされ、それ以外のリモート サイトと、WAN を介してクラスタ化されたサイトはすべて、スポーク サイトとなります。
- ソフトウェア アップグレード時は、ソフトウェア リリース ノートで説明されている標準のアップグレード手順を使用して、クラスタ内のすべてのサーバを同じ保守期間内にアップグレードする必要があります。

ローカル フェールオーバーに対する Cisco Unified CallManager のプロビジョニング

ローカル フェールオーバー モデルに対する Cisco Unified CallManager クラスタのプロビジョニングは、P.8-1 の「コール処理」の章で説明されているキャパシティについての設計上のガイドラインに従う必要があります。WAN を介してサイト間の音声コールまたはビデオ コールが可能である場合、サイト間のコール アドミッション制御を提供するために、他のサイトのデフォルト ロケーションに加えて、Cisco Unified CallManager の *ロケーション*も設定する必要があります。デバイス数に対して帯域幅が余分にプロビジョニングされる場合でも、ロケーションに基づくコール アドミッション制御を設定するのが最良の方法です。ロケーションベースのコール アドミッション制御によってコールが拒否された場合は、自動代替ルーティング（AAR）機能によって公衆網への自動フェールオーバーを行うことができます。

冗長性とアップグレード時間を改善するために、2 つの Cisco Unified CallManager サーバで Cisco TFTP サービスを使用可能にすることをお勧めします。また、低速 WAN リンクを介して、パブリッシャーからリモートとなるロケーションにある複数のサーバで、Cisco TFTP サービスを使用可能にしないでください。クラスタ内に複数の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。

サイトやサーバの利用可能なキャパシティに応じて、パブリッシャ サーバまたはサブスクライバ サーバのどちらかで、TFTP サービスを実行できます。TFTP サーバ オプションは、サイトごとに DHCP サーバ上で正しく設定する必要があります。DHCP を使用していないか、TFTP サーバが手

動で設定される場合、ユーザが、サイトの正しいアドレスを設定する必要があります。パブリッシャから離れた TFTP サーバでは、クラスタのアップグレード時や Cisco TFTP サービスの再起動時に、すべての設定ファイルをアップグレードおよび再構築するためにより多くの時間がかかります。この時間は、TFTP サーバとパブリッシャ間の遅延や、データベースに設定されているデバイスの数によって異なります。

WAN の障害時に Cisco Unified CallManager の正常な動作に影響を与える可能性がある他のサービスも、連続したサービスを確保するために、すべてのサイトで複製されなければなりません。これらのサービスには、DHCP サーバ、DNS サーバ、社内電話帳、および IP Phone サービスがあります。各 DHCP サーバで、ロケーションごとに DNS サーバ アドレスを正しく設定してください。

IP Phone は、サイト間のシェアドライン アピアランスを備えている場合があります。サイト間に提供される ICCS 帯域幅により、追加の ICCS トラフィックをシェアドライン アピアランスを生成することができます。WAN の障害時に、各ライン アピアランスのコール制御は分割されますが、WAN が回復された後、コール制御は 1 つの Cisco Unified CallManager サーバに戻ります。WAN の回復中に、2 つのサイト間には追加のトラフィックがあります。コール量が多い時期にこの状態が起きると、その期間中、共有ラインが予想通りに動作しない場合があります。この状態が数分以上続くことはありませんが、これが問題になる場合は、影響を最小限に抑えるために、追加の優先順位付き帯域幅を設定することができます。

ローカル フェールオーバー用のゲートウェイ

ゲートウェイは、通常、どのサイトにも配置されていて、公衆網へのアクセスに対応しています。ゲートウェイを同一サイトの Cisco Unified CallManager サーバに登録するために、デバイス プールを設定する必要があります。サイトのローカル ゲートウェイを公衆網アクセス用の第一選択肢として選択し、他のサイトのゲートウェイをオーバーフロー用の第二選択肢として選択するために、パーティションとコーリング サーチ スペースも設定する必要があります。各サイトで緊急用サービスへのアクセスを確保するように特に注意してください。

WAN 障害時にアクセスが必要のない場合、および WAN を介したコール数に対して十分な追加帯域幅が設定される場合、公衆網ゲートウェイへのアクセスを集中させることができます。E911 要件に対応するために、各サイトで追加のゲートウェイが必要な場合があります。

ローカル フェールオーバー用のボイスメール

Cisco Unity や他のボイスメール システムは、すべてのサイトに配置が可能で、Cisco Unified CallManager クラスタに組み込むことができます。この設定では、WAN 障害時に公衆網を使用しなくても、ボイスメールにアクセスできます。ボイスメール プロファイルを使用すると、同じロケーションにある IP Phone に、サイトに適したボイスメール システムを割り当てることができます。SMDI プロトコルを使用するボイスメール システム、サブスクライバ上の COM ポートに直接接続されたボイスメール システム、および Cisco Messaging Interface（CMI）を使用するボイスメール システムを、クラスタごとに最大 4 つ設定できます。

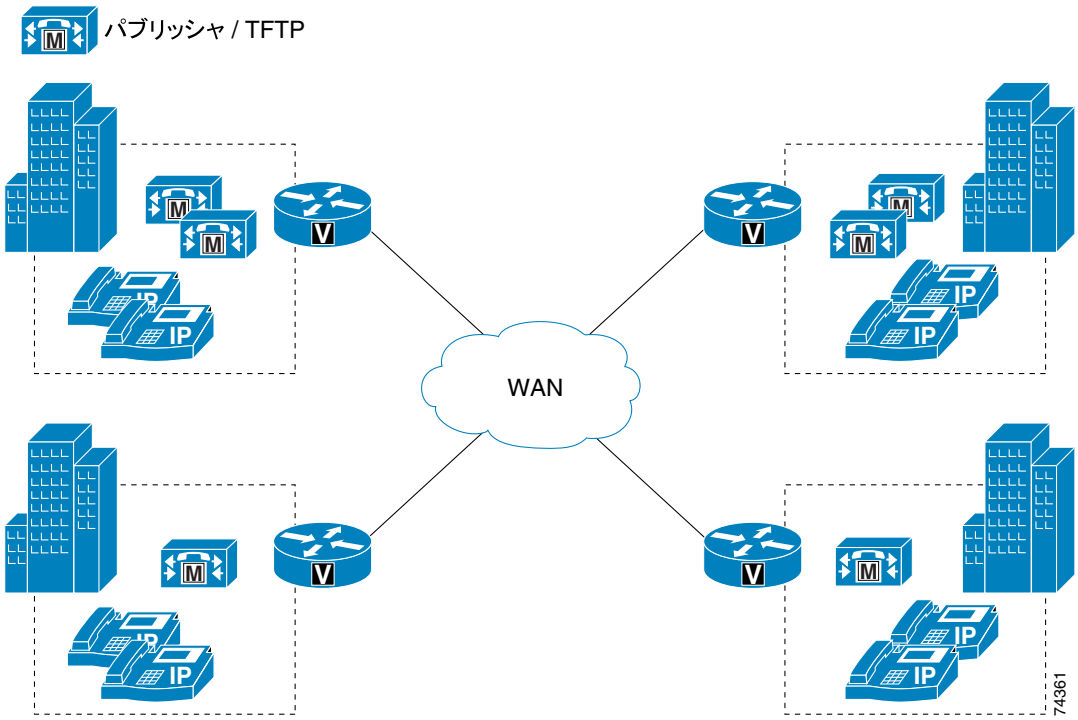
ローカル フェールオーバーに対する Music On Hold とメディア リソース

各サイトでは、Music On hold（MoH）サーバや、他のコンファレンス ブリッジなどのメディア リソースに、ユーザのタイプおよび数に十分なキャパシティをプロビジョニングする必要があります。Media Resource Group（MRG; メディア リソース グループ）と Media Resource Group List（MRGL; メディア リソース グループ リスト）の使用により、メディア リソースは、オンサイト リソースによって提供され、WAN 障害時に使用できます。

リモート フェールオーバー配置モデル

リモート フェールオーバー配置モデルでは、バックアップ サーバを柔軟に配置できます。各サイトには、少なくとも 1 つのプライマリ Cisco Unified CallManager サブスクライバを含め、バックアップ サブスクライバを必要に応じて配置します。このモデルでは、最大 8 つのサイトを配置できます。また、P.8-1 の「コール処理」の章で説明されている 1:1 冗長性と 50/50 ロードバランシング オプションを使用すると、IP Phone やその他のデバイスは、通常、ローカル サブスクライバに登録されます。バックアップ サブスクライバは、他の 1 つ以上のサイトで、WAN を介して配置されます（図 2-6 を参照）。

図 2-6　4 サイト構成のリモート フェールオーバー モデル



リモート フェールオーバー モデルを実装する場合は、ローカル フェールオーバー モデルのガイドライン（P.2-23 の「ローカル フェールオーバー配置モデル」を参照）と、次の変更点に従ってください。

- 少なくとも 1 つのプライマリ Cisco Unified CallManager サブスクライバと、必要に応じてオプションのバックアップ サブスクライバを含むように、各サイトを設定します。
- Cisco Unified CallManager の *グループ*と *デバイス プール*を設定して、WAN を介してサーバにデバイスを登録できるようにします。
- デバイスが、WAN を介して同じクラスタ内のリモート Cisco Unified CallManager サーバに登録される場合、シグナリング トラフィックまたはコール制御トラフィックのために帯域幅を追加する必要があります。この帯域幅は、ICCS トラフィックより大きくなる場合があります。また、シグナリングに関する帯域幅のプロビジョニング計算を使用して計算する必要があります（P.3-48 の「帯域幅のプロビジョニング」を参照）。

U. S. Section 508 準拠についての設計上の考慮事項

どの配置モデルを選択するかにかかわらず、IP テレフォニー ネットワークを設計する場合は、障害者の方が利用しやすいテレフォニー機能になるように、Telecommunications Act Section 255 電気通信法および U.S. Section 508 に定める基準に準拠する必要があります。

IP テレフォニー ネットワークを構成する際は、次に説明する基本設計ガイドラインに従い、Section 508 を遵守してください。

- ネットワーク上の Quality of Service（QoS）を使用可能にします。
- ターミナル テレタイプ（TTY）デバイスまたは Telephone Device for the Deaf（TDD）に接続する電話には、G.711 コーデックのみを設定します。G.729 のような低ビット レートのコーデックを音声通信に適用している場合でも、Total Character Error Rate（TCER）が 1% を超えている場合は、TTY/TDD デバイスが適切に作動しないことがあります。
- 必要に応じて、TTY/TDD デバイスに G.711 を設定し、WAN に対応します。
- Echo Cancellation を使用可能（ON）にし、パフォーマンスを最適化します。
- Voice Activity Detection（VAD; 音声アクティビティ検出）は、TTY/TDD 接続に影響を与えるため、使用されることはありません。したがって、設定は使用可能、使用不可のどちらであっても関係ありません。
- Cisco Unified CallManager 内の *リージョン*および*デバイス プール*を適切に設定して、TTY/TDD デバイスが常時 G.711 コードを使用するようにします。
- TTY/TDD の IP テレフォニー ネットワークへの接続は、次のいずれかの方法で行います。
  - 直接接続（推奨方式）

    RJ-11 アナログ回線用 TTY/TDD を直接 Cisco FXS ポートに接続します。FXS ポートはすべて動作します。たとえば、Cisco VG248、Catalyst 6000、Cisco ATA 188 モジュール、または FXS ポートを備えている他の Cisco 音声ゲートウェイ上で動作します。シスコは、この接続方式をお勧めします。
  - アコースティック カップル

    IP Phone のハンドセットを TTY/TDD に接続しているカップリング機器に置きます。アコースティック カップルは、RJ-11 接続に比較すると信頼性が劣ります。カップリング方式は部屋の周囲の雑音やその他の要素で、一般的に通信エラーを起こしやすい方式です。
- stutter ダイヤルトーンをサポートする必要がある場合は、アナログ電話を Cisco VG248 または ATA 188 上に備えている FXS ポートに接続します。

CHAPTER 3

ネットワーク インフラストラクチャ

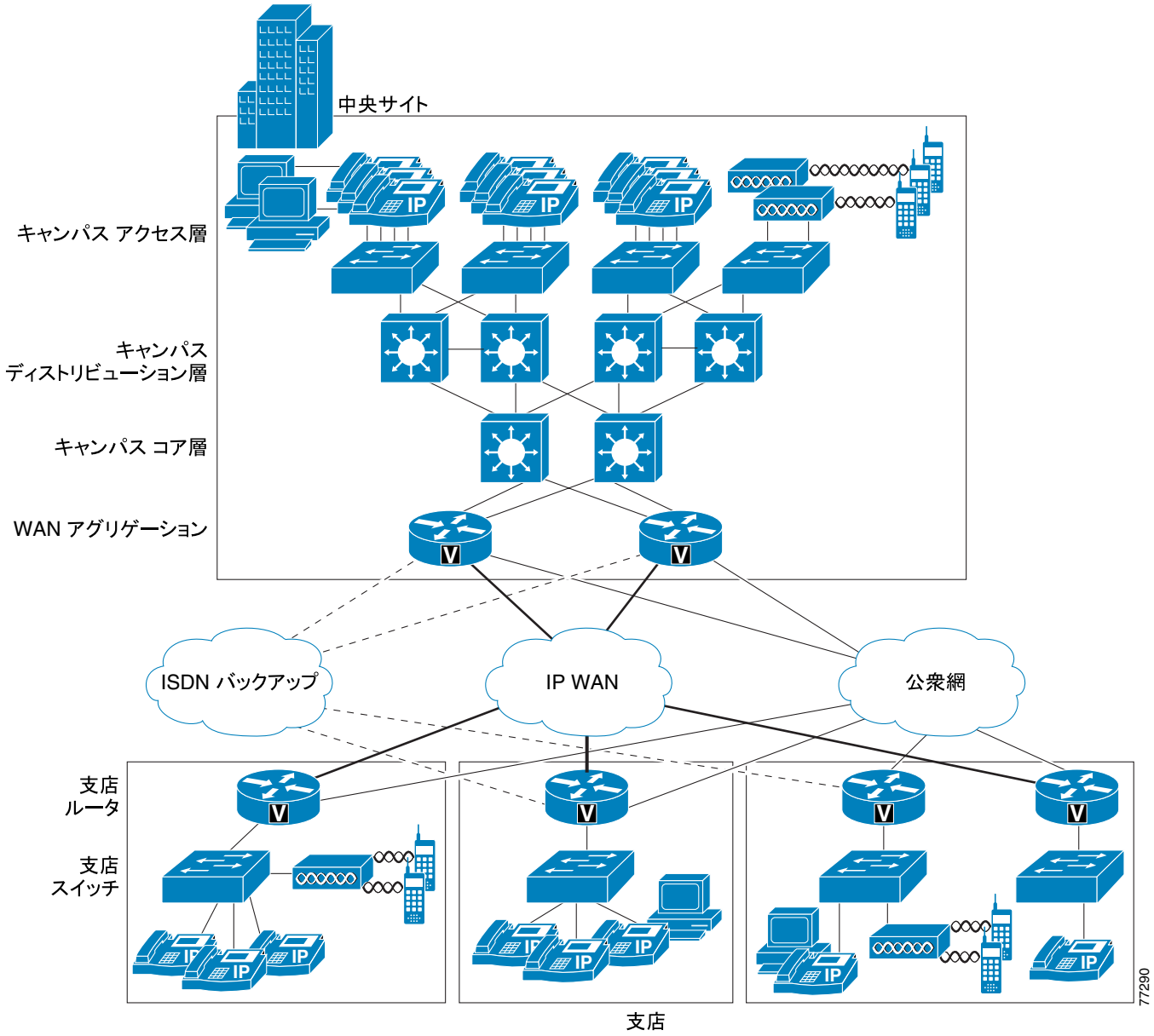
この章では、企業の環境で IP テレフォニー システムを構築するために必要な、ネットワーク インフラストラクチャの要件について説明します。図 3-1 は、ネットワーク インフラストラクチャを形成する各種デバイスの役割を示し、表 3-1 では、それらの役割のサポートに必要な機能を示しています。

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

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

- LAN インフラストラクチャ（P.3-4）
- WAN インフラストラクチャ（P.3-28）
- 無線 LAN インフラストラクチャ（P.3-62）

図 3-1　一般的なキャンパス ネットワーク インフラストラクチャ



支店

表 3-1　ネットワーク インフラストラクチャ内の役割に必要な機能

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

LAN インフラストラクチャ

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

- 高可用性のための LAN 設計（P.3-4）
- LAN の QoS（P.3-23）

高可用性のための LAN 設計

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

- キャンパス アクセス レイヤ（P.3-4）
- キャンパス ディストリビューション レイヤ（P.3-7）
- キャンパス コア レイヤ（P.3-10）
- ネットワーク サービス（P.3-11）

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

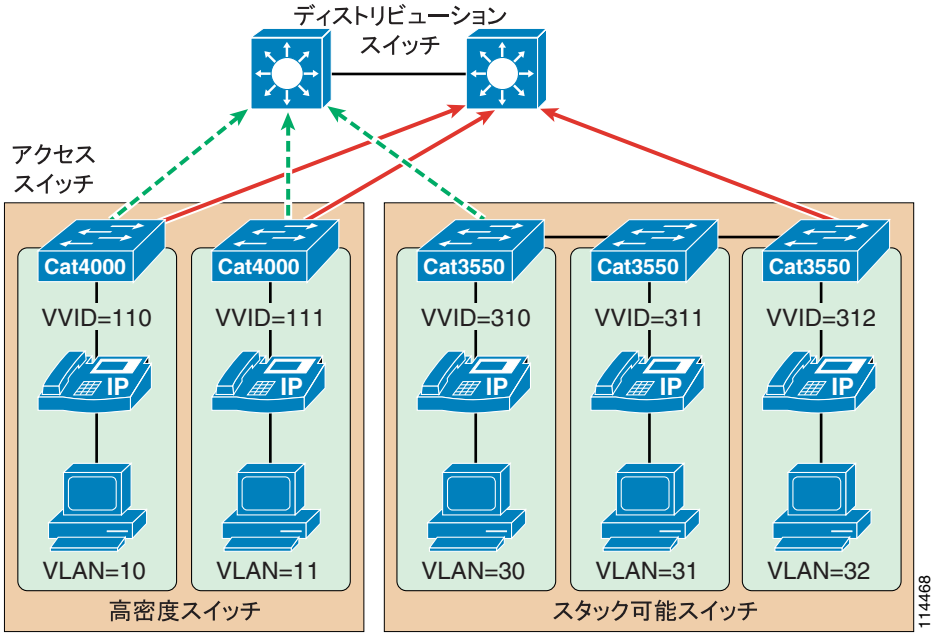
http://www.cisco.com/warp/public/cc/so/neso/lnso/cpso/gcnd_wp.pdf

キャンパス アクセス レイヤ

キャンパス LAN のアクセス レイヤに含まれるネットワーク部分は、デスクトップ ポート（複数可）からワイヤリング クローゼット スイッチまでです。

アクセス レイヤを適切に設計するには、最初に、Virtual LAN（VLAN）ごとに単一の IP サブネットを割り当てます。一般に、VLAN は、複数のワイヤリング クローゼット スイッチにまたがってはいけません。つまり、VLAN が存在するアクセス レイヤ スイッチは 1 つのみである必要があります（図 3-2 を参照）。この方法にすると、レイヤ 2 からトポロジ上のループが排除されるため、スパニング ツリーのコンバージェンスによってフローが一時的に中断することがなくなります。ただし、標準ベースの IEEE 802.1w Rapid Spanning Tree Protocol（RSTP）と 802.1s Multiple Instance Spanning Tree Protocol（MISTP）を導入すると、スパニング ツリーが収束する速度が大幅に高くなる可能性があります。さらに重要なことに、VLAN を単一のアクセス レイヤ スイッチに限定すると、ブロードキャスト ドメインのサイズが制限されます。単一の VLAN またはブロードキャスト ドメインにある多数のデバイスによって、大量のブロードキャスト トラフィックが定期的に生成される可能性があり、これが問題となる場合があります。そのため、VLAN ごとのデバイス数を 512 ほどに制限することをお勧めします。この数は、2 つのクラス C サブネット（つまり、23 ビットのサブネットがマスクされたクラス C アドレス）に相当します。一般的なアクセス レイヤ スイッチには、スタック可能な Cisco Catalyst 2950、3500XL、3550、および 3750 のほか、Cisco 3560 や、より大規模で高密度な Catalyst 4000 および 6000 スイッチがあります。

図 3-2　音声とデータに対応するアクセス レイヤ スイッチと VLAN



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

次の理由により、音声とデータの VLAN を分離することをお勧めします。

- アドレス スペースの確保と、外部ネットワークからの音声デバイスの保護

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

- QoS 信頼性境界の音声デバイスへの拡張

  音声デバイスの信頼性境界を拡張することなく、QoS 信頼性境界を音声デバイスに拡張し、次に、QoS 機能を PC や他のデータ デバイスに拡張することができます。

- 悪質なネットワーク攻撃からの保護

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

- 管理および設定の容易性

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

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

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

Spanning Tree Protocol（STP）

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

- PortFast

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

- ルート ガードまたは BPDU ガード

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

- UplinkFast と BackboneFast

  必要に応じてこれらの機能を有効にすると、レイヤ 2 ネットワークで変更が生じた場合に、STP ができるだけ迅速にコンバージして高可用性を提供することが保証されます。Catalyst 2950、3550、または 3750 などのスタック可能なスイッチを使用する場合は、Cross-Stack UplinkFast（CSUF）を有効にして、スタック内のスイッチに障害が発生したときにフェールオーバーおよびコンバージェンスが迅速に行われるようにします。

- 単方向リンク検出（UDLD）

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

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

キャンパス ディストリビューション レイヤ

キャンパス LAN のディストリビューション レイヤに含まれるネットワーク部分は、ワイヤリング クローゼットスイッチからネクストホップ スイッチまでです。また、このレイヤは LAN におけるレイヤ 2 からレイヤ 3 への最初のトラバーサルとなります。ディストリビューション レイヤ スイッチには、一般に、レイヤ 3 対応の Catalyst 4000 および 6000 スイッチと、より小規模な配置向けの Catalyst 3750 があります。

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

ホットスタンバイ ルータ プロトコル（HSRP）

すべてのルータが冗長になっていること、および障害発生時に別のルータが処理を引き継げることを保証するには、ディストリビューション レイヤで HSRP も有効にする必要があります。HSRP の設定には、次のコマンドを含める必要があります。

- standby track

  standby track コマンドは、HSRP で特定のインターフェイス（複数可）をモニタリングすることを示します。インターフェイスがダウンした場合は、そのルータの HSRP プライオリティが低下し、別のデバイスへのフェールオーバーが発生します。このコマンドは、**standby preempt** コマンドと組み合せて使用されます。

- standby preempt

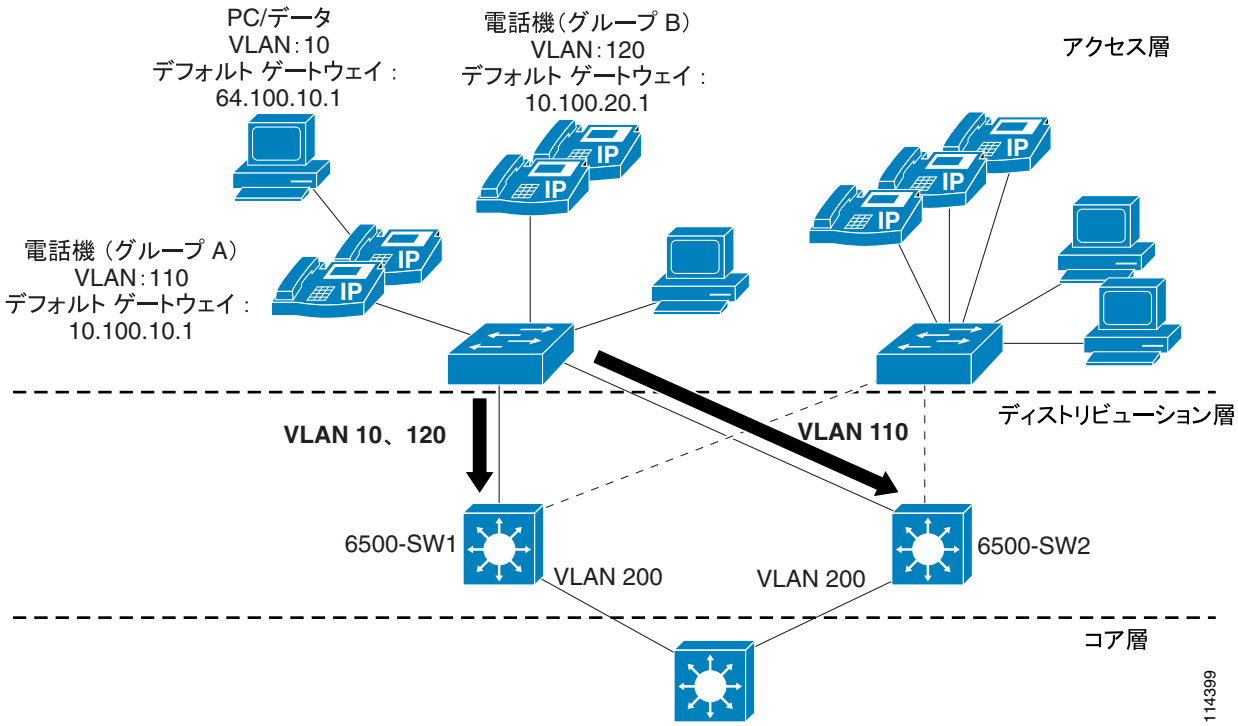
  このコマンドを使用すると、スタンバイ グループにおいて、HSRP が設定されたデバイスの中で特定のデバイスのプライオリティが最も高くなったときに、そのデバイスが HSRP スタンバイ アドレスのアクティブ レイヤ 3 ルータとして処理を引き継ぐことが保証されます。

また、HSRP には、両方の HSRP ルータ間でトラフィックをロード バランシングするように設定する必要があります。ロード バランシングを行うには、アクティブ HSRP ルータである各 HSRP デバイスを 1 つの VLAN またはインターフェイス用に設定し、スタンバイ ルータを別の VLAN またはインターフェイス用に設定します。両方の HSRP デバイスにアクティブ VLAN とスタンバイ VLAN を均等に分散させると、ロード バランシングが保証されます。1 つの VLAN 上のデバイスは、アクティブ HSRP デバイスをそのデフォルト ゲートウェイとして使用し、別の VLAN 上のデバイスは、同じ HSRP デバイスを、もう一方の HSRP デバイスに障害が発生した場合にのみスタンバイ デフォルト ゲートウェイとして使用します。このタイプの設定では、すべてのネットワーク トラフィックが単一のアクティブ ルータに送信されることが防止されるため、その他の HSRP デバイスへロード バランシングされるようになります。

図 3-3 は、HSRP 対応のネットワークの例を示しています。この図では、2 つの Catalyst 6500 スイッチ（6500-SW1 と 6500-SW2）に複数の VLAN インターフェイスが設定されています。ネットワーク内にリンク障害がないことを前提とすると、6500-SW1 は、VLAN 110（Group A の電話機の Voice VLAN）に対応するスタンバイ HSRP ルータであり、VLAN 10（データ VLAN）および VLAN 120（Group B の電話機の Voice VLAN）に対応するアクティブ HSRP ルータになっています。6500-SW2 は、その逆に設定されています。つまり、VLAN 110 に対応するアクティブ HSRP ルータであり、VLAN 10 および VLAN 120 に対応するスタンバイ HSRP ルータになっています。両方のスイッチは、設定どおり、アクティブに使用されています。両者にすべてのレイヤ 2 VLAN を均等に分散させると、負荷を両者に分散させることができます。また、各スイッチは、そのローカル VLAN 200 インターフェイスをトラックするように設定されており、VLAN 200 にリンク障害が発生した場合は、もう一方のスイッチがプリエンプション処理し、すべての VLAN に対応するアクティブ ルータとなります。同様に、一方のスイッチに障害が発生した場合は、もう一方のスイッチが 3 つの VLAN すべてのトラフィックを処理します。

図 3-3 のアクセス レイヤにある PC と電話機には、各 HSRP グループの HSRP アドレスに対応したデフォルト ゲートウェイが設定されています。Voice VLAN 110 および 120 のデバイスは、デフォルト ゲートウェイとして 10.100.10.1 と 10.100.20.1 をそれぞれ指しています。これらのデフォルト ゲートウェイは、両方のスイッチにある VLAN 110 および 120 インターフェイスの HSRP アドレスに対応しています。データ VLAN 10 のデバイスは、デフォルト ゲートウェイとして 64.100.10.1 を指しています。このデフォルト ゲートウェイは、両方のスイッチにある VLAN 10 インターフェイスの HSRP アドレスに対応しています。アクセス レイヤからディストリビューション レイヤに流れるトラフィックは 2 つのスイッチに分散されます（障害がない場合）が、リターン パスでの分散を保証するメカニズムはありません。コア レイヤから戻ってアクセス レイヤに向かうトラフィックは、最短および最小コストの、またはそのどちらかのルーテッド パスに沿って流れます。

図 3-3　standby preempt と standby track を使用した HSRP ネットワーク設定の例



例 3-1 および例 3-2 は、図 3-3 に示されている 2 つの Catalyst 6500 スイッチの設定を示しています。

例 3-1　6500-SW1 の設定

```
interface Vlan 10
 description Data VLAN 10
 ip address 64.100.10.11 255.255.255.0
 standby preempt
 standby ip 64.100.10.1
 standby track Vlan 200

interface Vlan110
 description Voice VLAN 110
 ip address 10.100.10.11 255.255.255.0
 standby preempt
 standby ip 10.100.10.1
 standby track Vlan 200
 standby priority 95

interface Vlan120
 description Voice VLAN 120
 ip address 10.100.20.11 255.255.255.0
 standby preempt
 standby ip 10.100.20.1
 standby track Vlan 200
```

例 3-2　6500-SW2 の設定

```
interface Vlan 10
 description Data VLAN 10
 ip address 64.100.10.12 255.255.255.0
 standby preempt
 standby ip 64.100.10.1
 standby track Vlan 200
 standby priority 95

interface Vlan110
 description Voice VLAN 110
 ip address 10.100.10.12 255.255.255.0
 standby preempt
 standby ip 10.100.10.1
 standby track Vlan 200

interface Vlan120
 description Voice VLAN 120
 ip address 10.100.20.11 255.255.255.0
 standby preempt
 standby ip 10.100.20.1
 standby track Vlan 200
 standby priority 95
```

障害発生時に HSRP が収束する速さは、HSRP の Hello タイマーとホールド タイマーの設定によって異なります。デフォルトでは、これらのタイマーは 3 秒と 10 秒にそれぞれ設定されています。この設定は、Hello パケットが HSRP スタンバイ グループのデバイス間で 3 秒ごとに送信されること、および Hello パケットが 10 秒間受信されないとスタンバイ デバイスがアクティブになることを意味します。これらのタイマー設定値を低くすると、フェールオーバーまたはプリエンプション処理を高速化できます。ただし、CPU 使用率の増加やスタンバイ状態の不要なフラッピングを避けるため、Hello タイマーを 1 秒未満に設定することや、ホールド タイマーを 4 秒未満に設定することはしないでください。HSRP トラッキング メカニズムを使用している場合、トラッキングしているリンクに障害が発生したときは、Hello タイマーやホールド タイマーに関係なく、ただちにフェールオーバーまたはプリエンプション処理が行われます。

ルーティング プロトコル

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

キャンパス コア レイヤ

キャンパス LAN のコア レイヤに含まれるネットワーク部分は、ディストリビューション ルータまたはレイヤ 3 スイッチから 1 つまたは複数のハイエンド コア レイヤ 3 スイッチまたはルータまでです。レイヤ 3 対応の Catalyst 6000 スイッチは、一般的なコア レイヤ デバイスであり、多数のキャンパス ディストリビューション レイヤに相互接続性を提供できます。

コア レイヤにおいても、高可用性を保証するために、次のタイプの冗長性を確保することが非常に重要です。

- 冗長なリンクまたはケーブル パス

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

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

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

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

データ センターとサーバ ファーム

一般に、メディア リソース サーバなどの Cisco Unified CallManager クラスタ サーバは、データ センターまたはサーバ ファーム環境に配置されます。また、コンファレンス ブリッジ、DSP またはトランスコーダ ファーム、およびメディア ターミネーション ポイントなどの、集中型ゲートウェイと集中型ハードウェア メディア リソースも、データ センターまたはサーバ ファームに配置されます。これらのサーバとリソースは音声ネットワークにおいて重要であるため、すべての Cisco Unified CallManager クラスタ サーバ、集中型音声ゲートウェイ、および集中型ハードウェア リソースは、複数の物理スイッチに分散させ、可能であればキャンパス内の複数の物理ロケーションにも分散させることをお勧めします。このようにリソースを分散させると、ハードウェア障害（スイッチやスイッチのライン カードの障害など）が発生しても、少なくともクラスタ内の一部のサーバを使用して、引き続きテレフォニー サービスを提供できることが保証されます。また、一部のゲート

ウェイとハードウェア リソースを使用して、引き続き公衆網へのアクセスと付加サービスを提供することもできます。物理的に分散させるだけでなく、これらのサーバ、ゲートウェイ、およびハードウェア リソースを別の VLAN またはサブネットに分散させる必要もあります。そのように分散させると、特定の VLAN 上でブロードキャスト ストームまたは DoS 攻撃が発生しても、一部の音声接続およびサービスは中断されずにすみます。

ネットワーク サービス

IP Communications システムの配置には、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の調和のとれた設計、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。

ドメイン ネーム システム（DNS）

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

DNS などの 1 つのネットワークサービスに完全に依存することは、重要な IP Communications システムを配置するときに、リスク要素になることがあります。DNS サーバが使用不能になった場合、ネットワーク デバイスがそのサーバを利用してホスト名から IP アドレスへのマッピングを取得しているときは、通信に障害が発生することがあります。そのため、Cisco Unified CallManager と IP Communications エンドポイント間の通信は、DNS 名前解決に依存しないことを強くお勧めします。DNS を使用すると、システム管理が簡素化され、Server（SRV）レコードがサポートされます。可能であれば、各 Cisco Unified CallManager クラスタを、より大きな組織の DNS ドメインの有効なサブドメインのメンバーとして定義することをお勧めします。

ホスト名の代わりに IP アドレスを使用するように、Cisco Unified CallManager、ゲートウェイ、およびエンドポイント デバイスを設定します。エンドポイント デバイス設定で、DNS サーバのアドレス、ホスト名、およびドメイン名などの DNS パラメータを設定することはお勧めできません。初めて Cisco Unified CallManager クラスタにパブリッシャをインストールするとき、パブリッシャは、システムに提供したホスト名によってサーバ テーブルで参照されます。その後のサブスクライバのインストールおよび設定、またはエンドポイントの定義の前に、このサーバ エントリをパブリッシャのホスト名ではなく IP アドレスに変更する必要があります。クラスタに追加する各サブスクライバは、ホスト名ではなく IP アドレスで、同じサーバ テーブルに最初に定義する必要があります。各サブスクライバは、1 デバイスずつこのサーバ テーブルに追加する必要があります。新しいサブスクライバをインストールするときを除き、存在しないサブスクライバは定義しないでください。

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

（注）　Cisco Unified CallManager で SRV レコードを使用するために、DNS サービスを有効にする必要はありません。

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

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

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

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

Dynamic Host Configuration Protocol（DHCP）

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

これらのデバイスの配置を簡素化するには、DHCP を使用するように IP Communications エンドポイントを設定する必要があります。任意の RFC 2131 準拠 DHCP サーバを使用して、IP Communications ネットワーク デバイスに設定情報を提供することができます。既存のデータ専用ネットワークに IP テレフォニー デバイスを配置する場合、作業としては、この新しい音声デバイスに対応する DHCP 音声スコープを既存の DHCP サーバに追加するだけで済みます。IP テレフォニー デバイスは、DHCP サーバを利用して IP 設定情報を取得するように設定されているため、DHCP サーバは冗長な方式で配置する必要があります。テレフォニー ネットワークには、2 つ以上の DHCP サーバを配置する必要があります。この配置により、いずれかのサーバに障害が発生して

も、他のサーバが引き続き DHCP クライアント要求に応答できます。また、DHCP サーバに、ネットワーク内の DHCP に依存するクライアントすべてを処理するのに十分な IP サブネット アドレスが設定されていることを確認する必要があります。

DHCP オプション 150

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

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

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

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

（注） IP Phone はオプション 150 で最大 2 つの TFTP サーバをサポートしますが、クラスタには 3 つ以上の TFTP サーバを設定できます。たとえば、Cisco Unified CallManager システムが 3 つの別々のサイトで WAN を介してクラスタ化されている場合は、3 つの TFTP サーバを（サイトごとに 1 つ）配置できます。次に、オプション 150 内にそのサイトの TFTP サーバを含む DHCP スコープを、各サイト内の電話機に付与できます。このように設定すると、TFTP サービスがエンドポイントに近くなるため、遅延が低減されるほか、サイト間で障害が分離される（1 つのサイトの障害が別のサイトの TFTP サービスに影響しない）ことが保証されます。ただし、設定ファイルが変更された場合、パブリッシャはクラスタ内の各 TFTP サーバにデータベースの新しいコピーを送信する必要があります。このようにデータベースを伝搬すると、パブリッシャの CPU リソースが消費されるため、クラスタ内に 3 つ以上の TFTP サーバが配置されている場合はパフォーマンスが低下することがあります。

DHCP のリース期間

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

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

集中型コール処理配置では、リモート サイトが中央の DHCP サーバを使用するように設定されている場合（Cisco IOS の IP ヘルパー アドレスなどの DHCP リレー エージェントを利用して）、および中央サイトへの接続が切断された場合、支店内の IP Phone はその DHCP スコープのリースを更新できなくなります。この場合、支店の IP Phone では、その DHCP のリースが期限切れになる危険性があります。その結果、その IP アドレスが使用できなくなり、サービスが中断されます。電話機はリース期間の半分が経過した時点でそのリースの更新を試みるという事実を考えると、DHCP サーバが到達不能になってからリース期間の半分が経過するとすぐに、DHCP のリースが期限切れになる可能性があります。たとえば、DHCP スコープが 4 日間に設定されている場合、WAN の障害によって支店内の電話機が DHCP サーバを使用できなくなったときは、その電話機はリース期間の半分（この場合は 2 日間）が経過した時点でリースを更新できなくなります。IP Phone は、WAN に障害が発生してから最短で 2 日後に機能を停止する可能性があります。ただし、その時点までに WAN が復旧して、DHCP サーバが使用可能になった場合は除きます。WAN の接続障害が続くと、WAN に障害が発生してから最長で 4 日後に、すべての電話機の DHCP スコープが期限切れになります。

次のいずれかの方法によって、この状況を緩和できます。

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

  この方法を使用すると、システム管理者は、少なくともリース期間の半分の時間を費やして、DHCP の到達不能に関するすべての問題に対処することができます。また、リース期間が長ければ、リースの更新に関連するネットワーク トラフィックの頻度が減少します。
- 共存 DHCP サーバの機能を設定する（たとえば、支店の Cisco IOS ルータ上で DHCP サーバ機能を実行します）

  このアプローチは、WAN 接続の中断の影響を受けません。このアプローチを使用すると、IP アドレスの管理が分散されるため、各支店で設定を更新する作業が発生します（詳細については、P.3-14 の「DHCP のネットワーク配置」を参照）。

DHCP のネットワーク配置

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

- 中央の DHCP サーバ

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

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

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

  集中型マルチサイト Cisco Unified CallManager 配置で使用する DHCP を設定する場合は、中央の DHCP サーバを使用して、中央にあるデバイスに DHCP サービスを提供することができます。リモート デバイスは、ローカルに設置されたサーバから、またはリモート サイトにある Cisco IOS ルータから、DHCP サービスを受信できます。このタイプの配置では、WAN に障害が発生しても、リモートのテレフォニー デバイスから DHCP サービスを使用できることが保証されます。例 3-3 は、Cisco IOS DHCP サーバの基本的な設定コマンドを示しています。

例 3-3　Cisco IOS DHCP サーバの設定コマンド

```
! Activate DHCP Service on the IOS Device

service dhcp

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

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

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

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

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

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

ほとんどのネットワーク インフラストラクチャで、通常、DHCP サーバは専用のマシンで、そのネットワークで使用する DNS サービスと Windows Internet Naming Service（WINS）サービスを組み合せて実行します。クラスタに登録されているデバイスが 1000 以下の小規模な Cisco Unified CallManager の配置では、DHCP を Cisco Unified CallManager サーバで実行して、これらのデバイスをサポートできます。ただし、サーバの CPU 負荷が高くなった場合は、DHCP をスタンドアロン サーバに移動する必要があります。クラスタに 1000 を超えるデバイスが登録されている場合は、DHCP を Cisco Unified CallManager サーバでは実行しないで、専用のスタンドアロン サーバで実行する必要があります。

Trivial File Transfer Protocol（TFTP）

Cisco Unified CallManager システムにおいて、エンドポイント（SCCP または SIP プロトコルを実行する IP Phone など）は、TFTP プロセスを利用して設定情報およびその他のエンドポイント デバイス情報を取得します。起動時に各エンドポイントは、要求元の MAC アドレスに基づいた名前の設定ファイルを要求します（たとえば、MAC アドレスが ABCDEF123456 の IP Phone の場合、ファイル名は SEPABCDEF123456.cnf.xml となります）。設定ファイルには、電話機で実行するソフトウェアのバージョンと、電話機を登録する Cisco Unified CallManager サーバのリストが含まれています。

設定ファイルにおいて、電話機が現在使用しているものと異なるソフトウェア ファイルを実行するように指示されている場合、電話機は新しいバージョンのソフトウェアを TFTP サーバに要求します。電話機はこのプロセスを、ソフトウェア アップグレードのたびに行います。

集中型コール処理配置では、リモート電話機は、支店の WAN リンクを介して設定ファイルと電話機のソフトウェアをダウンロードする必要があります。定期保守において新しいソフトウェアをダウンロードする場合、ダウンロード時間は、アップグレードが必要な電話機の数、ファイル サイズ、および WAN リンクの帯域幅とトラフィック使用率による関数となります。

たとえば、Cisco Unified CallManager 5.0 では、電話機設定ファイルのサイズは約 3400 バイトで、SCCP を実行する Cisco Unified IP Phone 7960 用に要求されるソフトウェア ロード ファイル（P00308000100.loads、P00308000100.sbn、および P00308000100.sb2）の合計は 830,239 バイトです。支店において 256 kbps の WAN 帯域幅を使用してソフトウェアをダウンロードする場合、1 台の電話機でアップグレード時に新しいソフトウェアをダウンロードするには、約 26 秒かかります。その同じ支店にある 10 台の電話機で新しいソフトウェアが必要な場合、ダウンロード プロセスには約 4.5 分かかります。

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

TFTP サーバの冗長性

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

TFTP のロード シェアリング

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

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

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

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

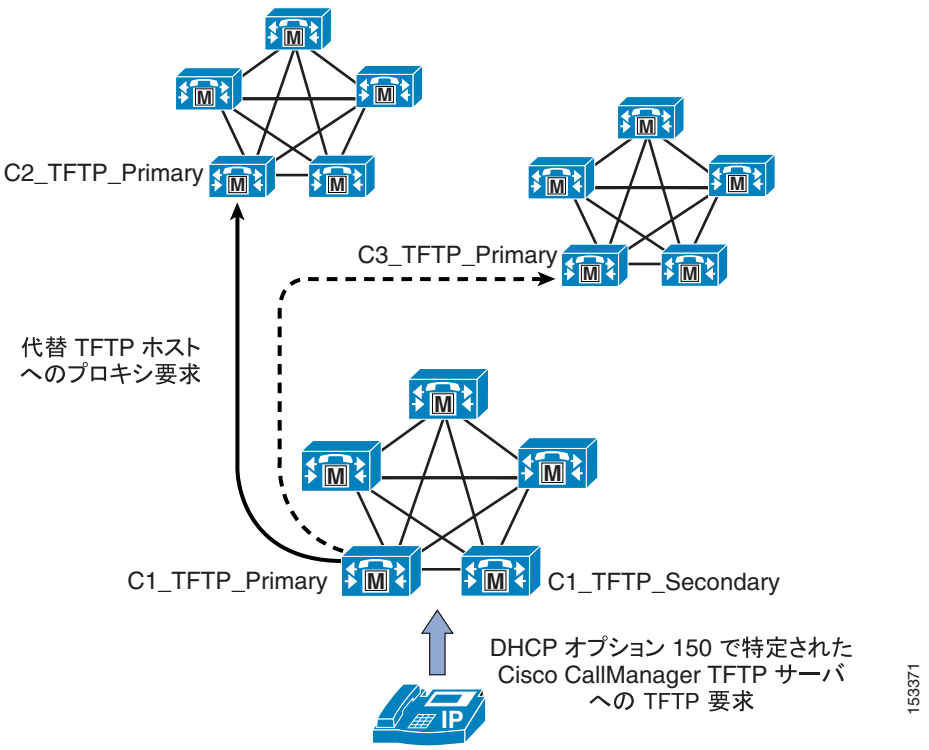
中央集中型 TFTP サービス

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

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

図 3-4 に、このプロセスの動作例を示します。Cluster 3 に登録されている電話機からの要求は、Cluster 1 で設定されている中央集中型 TFTP サーバ（C1_TFTP_Primary）に転送されます。このサーバは、次に、電話機が要求したファイルのコピーによる最初の応答があるまで、設定済みの代替 TFTP　サーバのそれぞれに対して問い合せます。中央集中型セカンダリ　TFTP　サーバ（C1_TFTP_Secondary）への要求は、要求されたファイルが見つかるか、すべてのサーバから要求されたファイルが存在しないという応答があるまで、プロキシによって別のクラスタのセカンダリ TFTP サーバに送信されます。

図 3-4　　中央集中型 TFTP サーバ



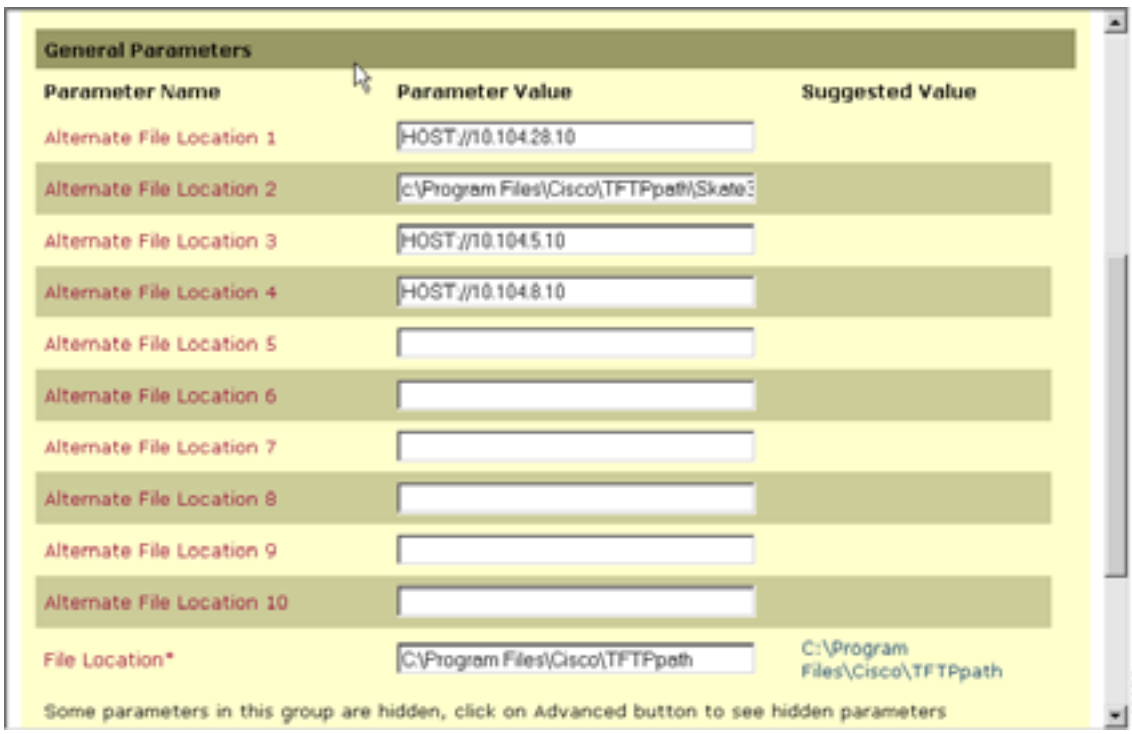
リリースの異なる Cisco Unified CallManager を実行するサーバが含まれる混在環境の中央集中型 TFTP

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

（注） Cisco Unified CallManager　Release 4.1(3)SR3a　には、混在モードの中央集中型環境をサポートする cTFTP サーバ デーモンへのアップグレードが含まれています。

Cisco Unified CallManager 4.1(3)SR3a TFTP サーバを設定するときは、HOST プロキシ要求によって Cisco Unified CallManager 5.0 サーバを指定し、リモート マウント設定プロセスを使用して Cisco Unified CallManager 4.1(3)SR3a 以前の任意のサーバを指定する必要があります。図 3-5 を参照してください（リモート マウント設定の詳細については、以下を参照してください）。Cisco Unified CallManager 4.1(3)SR3a の子クラスタは、リモート マウントとプロキシ クラスタのどちらにも設定できます。

図 3-5　デュアル モード設定



追加設定

さらに、大規模なキャンパス配置では、Maximum Serving Count サービス パラメータを、次のように調整します。

専用 TFTP サーバの推奨値は、シングル プロセッサ システムの場合が 3000 で、デュアルプロセッサ システムの場合が 5000 です。

Cisco Unified CallManager 4.1(3)SR3r 以前のリモートマウント サーバの中央集中型設定

TFTP サーバは、サーバ上にないファイル（別のクラスタの TFTP サーバによって作成および管理される設定ファイルなど）の要求を受信すると、代替ファイル ロケーションのリスト内でそのファイルを検索します。Cisco Unified CallManager 4.1(3)SR3 以前の環境をサポートするには、別のクラスタに関連付けられたリモート マウントのサブディレクトリを検索するように、中央集中型 TFTP サーバを設定する必要があります。

例 3-4　代替 TFTP ファイル ロケーション

大規模なキャンパス システムを配置する場合は、3 つのクラスタを使用します。各クラスタには TFTP サーバを含めます。Cluster1 に対応する TFTP サーバの TFTP1 は、キャンパスの中央 TFTP サーバとして設定します。それ以外のクラスタと TFTP サーバの名前は、順に、Cluster2 に対応するものを TFTP2 に、Cluster3 に対応するものを TFTP3 にします。すべてのサブネットでは、DHCP スコープがオプション 150 として TFTP1 の IP アドレスを提供します。

最初に、TFTP2 と TFTP3 が、それぞれの設定ファイルを TFTP1 のドライブに書き込むように設定します。それぞれの書き込み先は、次に示す別々のサブディレクトリとします。

- TFTP2 の代替ファイル ロケーションの設定：\\TFTP1_IP\Program Files\Cisco\TFTPpath\TFTP2
- TFTP3 の代替ファイル ロケーションの設定：\\TFTP1_IP\Program Files\Cisco\TFTPpath\TFTP3

次に、TFTP1 が代替ファイル ロケーションを検索するように設定します。設定方法は次のとおりです。

- 代替ファイル ロケーション 1：c:\Program Files\Cisco\TFTPpath\TFTP2
- 代替ファイル ロケーション 2：c:\Program Files\Cisco\TFTPpath\TFTP3

（注） この例では、TFTP1_IP は TFTP1 の IP アドレスを表しています。また、TFTP1 では、TFTP2 と TFTP3 用に Windows NT サブディレクトリを手動で作成する必要があります。

TFTP サーバで代替ファイル ロケーションを指定する場合は、Universal Naming Convention（UNC; 汎用命名規則）パス（形式は *\\<IP アドレス>\< フォルダへのフル パス>*）を使用することをお勧めします。デフォルト以外の NT「共有」を作成することや、DNS 名を使用することはお勧めできません。また、すべてのクラスタが、Cisco TFTP サービス用の適切なログイン ID、パスワード、およびセキュリティ特権（ワークグループ、ドメイン、またはディレクトリベース）を処理することを確認します。

Cisco CallManager Release 3.2 以降を使用する場合、Cisco TFTP サーバは、デフォルトで、IP Phone の設定ファイルを RAM にキャッシュします。中央の TFTP サーバに書き込むファイルについては、ファイル キャッシングを無効（オフ）にする必要があります。無効にするには、中央の TFTP サーバに書き込むように設定された TFTP サーバごとに、次のサービス パラメータを指示通りに設定します。

- Enable Caching of Configuration Files：**False**（必須）
- Enable Caching of Constant and Bin Files at Startup：**False**（推奨）

ネットワーク タイム プロトコル（NTP）

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

Cisco Unified CallManager の NTP 時刻同期

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

Cisco Unified CallManager 5.0 は、クラスタのすべてのサブスクライバの NTP 時刻をパブリッシャと自動的に同期します。インストール時に、各サブスクライバは自動的に、パブリッシャで実行されている NTP サーバをポイントするように設定されます。パブリッシャはマスタ サーバと見なされ、外部サーバと同期するように設定されている場合を除き、内部ハードウェア クロックを基にクラスタに時刻を提供します。クラスタの時刻と外部時刻源を確実に同期させるために、パブリッシャは Stratum-1、Stratum-2、または Stratum-3 NTP サーバをポイントするように設定することを強くお勧めします。

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

Cisco IOS と CatOS の NTP 時刻同期

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

例 3-5 は、Cisco IOS および CatOS デバイスに対する NTP 時刻同期の設定を示しています。

例 3-5　Cisco IOS と CatOS の NTP 設定

Cisco IOS の設定：

```
ntp server 64.100.21.254
```

CatOS の設定：

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

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

Power over Ethernet（PoE）

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

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

Cisco PoE は、データ接続に使用されるペア線を介して供給されます（ピン 1、2、3、および 6）。既存のアクセス スイッチ ポートがインライン パワーに対応していない場合は、パワー パッチパネルを使用して、ケーブル上に電力を供給することができます（この場合は、4、5、7、および 8 ピンが使用されます）。また、配置要件によっては、パワー インジェクタを使用することもできます。

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

シスコでは現在、Cisco PoE インライン パワーのほかに、IEEE 802.3af PoE 標準をサポートしています。現時点で 802.3af に準拠しているのは、一部のアクセス スイッチおよび電話機のみです。将来的には、すべての電話機とスイッチが 802.3af PoE をサポートする予定です。Catalyst 6500、4500、および 3750 は、現在、802.3af をサポートしています。802.3af PoE 標準をサポートする Cisco Unified IP Phone については、P.19-43 の「エンドポイント機能の要約」を参照してください。

カテゴリ 3 ケーブリング

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

- PC ポートを持ち、そのポートに PC が接続された IP Phone（Cisco Unified IP Phone 7971、7970、7961、7960、7941、7940、7911、および 7910+SW）は、10 Mb 全二重に設定されている必要があります。

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

- PC ポートを持たずに 10 Mb スイッチ ポートを持つ IP Phone（Cisco Unified IP Phone 7902、7905、および 7910）は、10 Mb 半二重に自動ネゴシエートできるようになっている必要があります。

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

- PC ポートを持つが、そのポートに PC が接続されていない IP Phone（Cisco Unified IP Phone 7971、7970、7961、7960、7941、7940、7912、7911、および 7910+SW）は、10Mb 半二重にネゴシエートできるようにしてもかまいません。

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

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

IBM タイプ 1A および 2A ケーブリング

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

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

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

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

IBM ケーブリングの使用に関する詳細については、次の Web サイトで入手可能な製品情報『*Shielded Twisted-Pair Cabling Support for Cisco Fast Ethernet Products*』を参照してください。

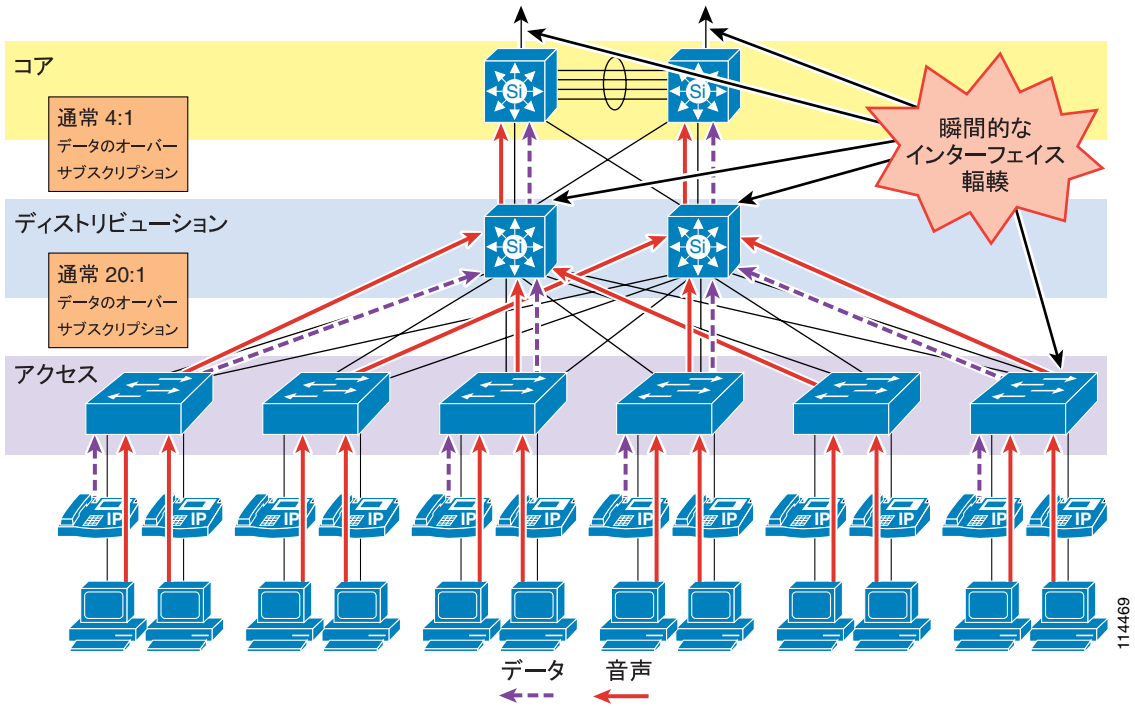
http://www.cisco.com

LAN の QoS

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

図 3-6 は、LAN インフラストラクチャで発生する一般的なオーバーサブスクリプションを示しています。

図 3-6　LAN におけるデータ トラフィックのオーバーサブスクリプション



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

ファイル共有などのアプリケーション（ピアツーピアとサーバベースの両方）、リモート ネットワーク上のストレージ、ネットワークベースのバックアップ ソフトウェア、およびサイズの大きな添付ファイルを持つ電子メールによって、ネットワークの輻輳がより頻繁に発生したり、より長期間発生したりする場合があります。最近のワーム攻撃の弊害に、膨大な量のネットワーク トラフィック（ユニキャスト ベースとブロードキャストストームベースの両方）があります。この攻撃により、ネットワークの輻輳が増加します。バッファの管理ポリシーが適用されていない場合は、すべてのトラフィックにおいて、LAN の損失、遅延、およびジッタ特性が影響を受けることがあります。

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

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

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

- トラフィック分類

  分類では、ネットワークの Class of Service（CoS; サービス クラス）に関する要件を示す特定のプライオリティがパケットにマークされます。このパケット マーキングが信頼されるかどうかが一定していない地点は、信頼性境界と見なされます。信頼性は、一般に、音声デバイス（電話機）までは拡張されますが、データ デバイス（PC）には拡張されません。
- キューイングまたはスケジューリング

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

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

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

- トラフィック分類（P.3-24）
- インターフェイス キューイング（P.3-26）
- 帯域幅のプロビジョニング（P.3-26）
- QoS が使用されない場合の IP コミュニケーションの障害（P.3-27）

トラフィック分類

できるだけネットワークのエッジの近くでトラフィックを分類したり、マークすることは、常に Cisco ネットワーク デザイン アーキテクチャの必須部分でした。トラフィック分類は、キャンパス スイッチおよび WAN インターフェイス内で使用される各種キューイング体系にアクセスするための基本的基準です。IP Phone は、その音声制御シグナリングと音声 RTP ストリームを送信元でマークします。その際は、表 3-2 に示されている値に従います。IP Phone は、このようにトラフィック フローを分類でき、実際に分類する必要があります。

表 3-2 は、LAN インフラストラクチャのトラフィックを分類する場合の要件をリストしています。

表 3-2　各種タイプのネットワーク トラフィックのトラフィック分類ガイドライン

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

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

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

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

ビデオ テレフォニーのトラフィック分類

IP ビデオ テレフォニーに関係する主なクラスは、次のとおりです。

- 音声

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

  ビデオ会議は、CoS 4（IP Precedence 4、PHB AF41、または DSCP 34）に分類されます。
- コール シグナリング

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

Cisco Unified Communications ネットワークでは、これらの分類を*ベスト プラクティス*として強くお勧めします。

コールの音声コンポーネントは、進行中のコールのタイプに応じて、2 つのいずれかに分類できます。音声のみ（通常）の通話呼のメディアは、CoS 5（IP Precedence 5 または PHB EF）に分類されますが、ビデオ会議のオーディオ チャネルのメディアは CoS 4（IP Precedence 4 または PHB AF41）に分類されます。Cisco IP Video Telephony 製品は、Cisco Corporate QoS Baseline 標準に準拠し、ビデオ コールのオーディオ チャネルとビデオ チャネルの両方が CoS 4（IP Precedence 4 または PHB AF41）にマークされている必要があります。この推奨事項には次の理由がありますが、これら以外にもあります。

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

シグナリング クラスは、すべての音声シグナリング プロトコル（SCCP、MGCP など）、およびビデオ シグナリング プロトコル（SCCP、H.225、RAS、CAST など）に適用されます。これらのプロトコルについては、P.19-33 の「ソフトウェアベースのエンドポイント」の項で詳しく説明します。

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

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

インターフェイス キューイング

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

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

キャンパス内の送信インターフェイス バッファは、ネットワーク トラフィック自体にバースト性があるため、短い時間間隔で散発的に輻輳する傾向があります。輻輳が起きると、その送信インターフェイスを宛先とするすべてのパケットがドロップされます。音声トラフィックのドロップを防止する唯一の方法は、キャンパス スイッチ上で複数のキューを設定することです。このため、ポートごとに 2 つ以上の出力キューを持ち、レイヤ 2、レイヤ 3、またはその両方の QoS 分類に基づいてこれらのキューにパケットを送信する機能を持つスイッチを常に使用することをお勧めします。Cisco Catalyst 6000、4000、3750、35XX、および 2950 スイッチはすべて、ポートごとに 2 つ以上の出力キューをサポートします。

帯域幅のプロビジョニング

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

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

QoS が使用されない場合の IP コミュニケーションの障害

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

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

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

WAN ベースの配置モデルでは、トラフィックの輻輳によって、リンクの中断が続いたり、より高い頻度で発生したりする可能性が高くなります。これは、使用可能な帯域幅が LAN よりもはるかに小さい（一般に 2 Mbps 未満）ためです。そのため、リンクがより簡単に飽和します。リンクの中断は、音声メディアがパケット ネットワークを通過するかどうかに関係なく、ユーザに大きな影響を与えます。

WAN インフラストラクチャ

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

- WAN の設計と設定（P.3-28）
- WAN の QoS（P.3-31）
- リソース予約プロトコル（RSVP）（P.3-38）
- 帯域幅のプロビジョニング（P.3-48）

WAN の設計と設定

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

- 配置上の考慮事項（P.3-28）
- 保証帯域幅（P.3-30）
- ベストエフォート型の帯域幅（P.3-30）

配置上の考慮事項

音声ネットワークの WAN 配置は、ハブアンドスポークまたは任意のトポロジです。ハブアンドスポーク トポロジは、1 つの中央ハブ サイトと、中央ハブ サイトに接続された複数のリモート スポーク サイトで構成されます。このシナリオでは、各リモート（スポーク）サイトは、中央（ハブ）サイトから 1 WAN リンク ホップ離れており、他のすべてのスポーク サイトから 2 WAN リンク ホップ離れています。任意のトポロジには複数の WAN リンクが含まれ、サイト間のホップ数は任意です。このシナリオでは、同じサイトに対して複数の異なるパスがあり、別のサイトと異なるリンクで通信が行われるサイトがあります。最も単純な例として、他の 2 つのサイトとの WAN リンクを持つ 3 つのサイトが三角形を形成している例があります。この場合、あるサイトから別のサイトへのパスは 2 つあります。

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

トポロジ対応コール アドミッション制御は、ハブアンドスポークと任意の WAN トポロジの両方で使用できます。このコール アドミッション制御の形式には、リソース予約プロトコル（RSVP）をサポートする WAN インフラストラクチャの部分が必要です。詳細については、P.3-38 の「リソース予約プロトコル（RSVP）」および P.9-1 の「コール アドミッション制御」を参照してください。

集中型および分散型マルチサイト配置モデルや、これらの配置モデルに対する Multiprotocol Label Switching（MPLS）の影響に関する詳細については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

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

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

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

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

最後に、International Telecommunication Union（ITU; 国際電気通信連合）の G.114 勧告には、音声ネットワークにおける片方向の遅延は 150 ミリ秒以下でなければならないと明記されています。ネットワーク内に低速 WAN リンクを実装する場合は、この要件に留意することが重要です。片方向の遅延がこの 150 ミリ秒の勧告を超えないように、WAN リンクのトポロジ、テクノロジー、および物理的な距離を考慮する必要があります。WAN を介したクラスタ化を使用する配置では、クラスタ間のシグナリング トラフィックの一方向の遅延が 20 ミリ秒を超えないようにする必要があります（P.2-19 の「IP WAN を介したクラスタ化」を参照）。

保証帯域幅

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

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

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

ベストエフォート型の帯域幅

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

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

- インターネット
- DSL
- ケーブル
- 衛星
- 無線

ほとんどの場合、これらのリンク タイプはいずれも、重要な音声および音声アプリケーションに必要となる、保証されたネットワーク接続性および帯域幅を提供できません。ただし、これらのテクノロジーは、個人用または在宅勤務者用のネットワーク配置に適している場合があります。これらのトポロジは、可用性の高いネットワーク接続性と、十分なネットワーク スループットを提供できる一方で、長期間にわたって使用不能になる場合や、速度が抑制されるために音声などのリアルタイム アプリケーションでネットワーク スループットが不足する場合、あるいは大量のパケット損失を引き起こすために繰り返し再送信することが必要になる場合があります。言い換えると、これらのリンクとトポロジは、保証帯域幅を提供できません。また、トラフィックをこれらのリンク上

で送信する場合は、ベストエフォートで送信されるため、その宛先に到達することが保証されません。このため、企業クラスの音声サービスおよび品質が要求される音声対応のネットワークには、ベストエフォート型の WAN トポロジを使用しないことをお勧めします。

（注） DSL およびケーブル テクノロジーの新しい QoS メカニズムの中には、保証帯域幅を提供できるものがあります。しかし、これらのメカニズムは、サービス プロバイダーによって配置されることが一般的ではないため、依然としてこれらのサービスは大幅なオーバーサブスクリプションになります。

WAN の QoS

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

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

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

これらの QoS メカニズムの目標は、音声トラフィックの遅延、パケット損失、およびジッタを低減することによって、信頼できる高品質の音声を保証することにあります。表 3-3 は、WAN インフラストラクチャをこの目標に導くために必要な QoS 機能およびツールを示しています。

表 3-3　WAN テクノロジーとリンク速度ごとの IP テレフォニー サポートに必要な QoS 機能とツール

WAN テクノロジー	リンク速度：56 kbps ～ 768 kbps	リンク速度：768 kbps 以上
専用回線	• MLP（マルチリンク ポイントツーポイント プロトコル） • MLP LFI（Link Fragmentation and Interleaving） • LLQ（低遅延キューイング） • オプション：cRTP（RTP ヘッダー圧縮）	• LLQ
フレームリレー（FR）	• トラフィック シェーピング • LFI（FRF.12） • LLQ • オプション：cRTP • オプション：Voice-Adaptive Traffic Shaping（VATS） • オプション：Voice-Adaptive Fragmentation（VAF）	• トラフィック シェーピング • LLQ • オプション：VATS

表 3-3　WAN テクノロジーとリンク速度ごとの IP テレフォニー サポートに必要な QoS 機能とツール（続き）

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

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

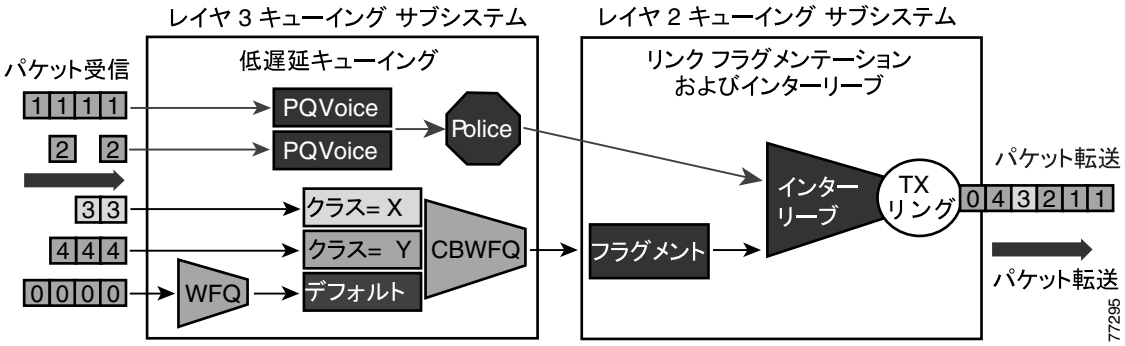
- トラフィックの優先順位（P.3-32）
- リンク効率手法（P.3-34）
- トラフィック シェーピング（P.3-36）

トラフィックの優先順位

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

図 3-7 は、優先順位体系の例を示しています。

図 3-7　WAN を介した VoIP 用の最適化キューイング



LLQ には、次の優先順位の基準を使用することをお勧めします。

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

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

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

（注） シスコでは、音声制御プロトコルのマーキングを DSCP 26（PHB AF31）から DSCP 24（PHB CS3）に変更し始めています。ただし、多くの製品は、引き続きシグナリング トラフィックを DSCP 26（PHB AF31）としてマークします。したがって、当面は、コール シグナリング用に AF31 と CS3 の両方を予約することをお勧めします。

- 場合によっては、特定のデータ トラフィックで、ベストエフォート型よりも優れた処理が必要になることがあります。このトラフィックは、*ミッションクリティカル データ*と呼ばれ、必要な帯域幅を持つ 1 つ以上のキューに入ります。このクラス内のキューイング方式は、最小帯域幅が割り当てられた FIFO（ファーストイン ファーストアウト）です。このクラスのトラフィッ

クは、設定された帯域幅限界を超えると、デフォルト キューに入れられます。このキューへの入力基準は、Transmission Control Protocol（TCP）ポート番号、レイヤ 3 アドレス、または DSCP/PHB 値にすることができます。

- 残りのトラフィックはすべて、ベストエフォート型処理のデフォルト キューに入れることができます。キーワード **fair** を指定すると、キューイング アルゴリズムは WFQ になります。

リンク効率手法

次のリンク効率技術によって、低速 WAN リンクの品質と効率が向上します。

Compressed Real-Time Transport Protocol（cRTP;RTP ヘッダー圧縮）

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

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

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

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

cRTP 圧縮は、パケットが出力インターフェイスを通過する前、つまり、LLQ クラスベース キューイングが行われた後の最終段階として行われます。Cisco IOS Release 12.(2)2T からは、cRTP により、*音声*クラスの帯域幅を圧縮パケット値に基づいて設定できる LLQ クラスベース キューイング メカニズムからフィードバック メカニズムを使用できるようになりました。12.(2)2T より前の Cisco IOS リリースでは、このメカニズムは使用されていないため、LLQ は圧縮帯域幅を認識しません。したがって、圧縮が行われないものとして、*音声*クラスの帯域幅をプロビジョニングする必要があります。表 3-4 は、512 Kbps リンクで G.729 コーデックを使用して 10 コールに対応する場合の、*音声*クラスの帯域幅の設定における違いの例を示しています。

表 3-4 では、cRTP 以外の G.729 コールの場合が 24 Kbps で、cRTP の G.729 コールの場合が 10 Kbps であることを前提としていることに注意してください。これらの帯域幅の数値は、音声ペイロードと IP/UDP/RTP ヘッダーのみに基づいています。レイヤ 2 ヘッダーの帯域幅は考慮に入れていません。ただし、実際の帯域幅プロビジョニングでは、レイヤ 2 ヘッダーの帯域幅も、WAN リンクで使用されたタイプに基づいて考慮に入れられます。

表 3-4　512 Kbps リンク帯域幅と G.729 コーデックを使用して 10 コールに対応する場合の LLQ 音声クラスの帯域幅要件

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

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

また、Cisco IOS Release 12.2(13)T からは、Class-Based cRTP 機能を使用して、cRTP を音声クラスの一部として設定できるようになったことにも注意してください。このオプションを使用すると、サービス ポリシーを介してインターフェイスに接続されているクラス内で cRTP を指定することが

できます。この新しい機能により、**show policy interface** コマンドを使用して、圧縮の統計情報や帯域幅の状況を表示することができます。このコマンドは、cRTP が IP/RTP ヘッダーを圧縮している事実を踏まえて、インターフェイス サービス ポリシー クラスに対して提供されるレートを確認するときに非常に役立つ場合があります。

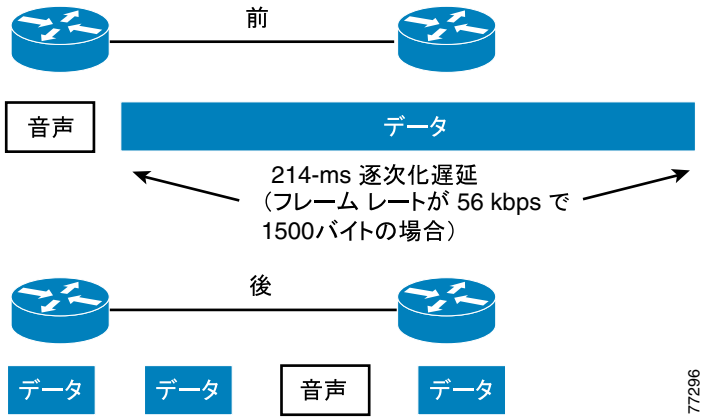
音声およびビデオに対応した IPSec VPN（V3PN）で cRTP を使用する場合の追加の推奨事項については、次の Web サイトで入手可能な V3PN 資料を参照してください。

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

LFI（Link Fragmentation and Interleaving）

低速リンク（768 Kbps 未満）の場合、許容できる音声品質を確保するには、LFI メカニズムを使用する必要があります。この手法は、図 3-8 に示されているように、大きなデータ フレームの背後で、音声トラフィックが遅延しないようにして、ジッタを制限します。この目的のための 2 つの手法は、マルチリンク ポイントツーポイント プロトコル（MLP）LFI（専用回線、ATM、および SIW 用）と、フレームリレー用の FRF.12 です。

図 3-8　LFI（Link Fragmentation and Interleaving）



Voice-Adaptive Fragmentation（VAF）

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

VAF は、一般に、Voice-Adaptive Traffic Shaping と組み合せて使用されます（P.3-37 の「Voice-Adaptive Traffic Shaping（VATS）」を参照）。VAF はオプションの LFI ツールです。VAF を有効にする場合は注意が必要です。これは、音声アクティビティが検出されるタイミングと LFI メカニズムが連動するタイミングの間に多少の遅延が生じるためです。また、最後の音声パケットが検出されてから、VAF が非アクティブになるまでの間に、設定可能な非アクティブ化タイマー（デフォルトは 30 秒）が期限切れになる必要があります。そのため、この期間は LFI が不必要に発生します。VAF は、Cisco IOS Release 12.2(15)T 以降で使用できます。

トラフィック シェーピング

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

図 3-9 は、同一 IP WAN 上での音声とデータの転送時にトラフィック シェーピングが必要な主な理由を示しています。

図 3-9　フレームリレーと ATM を使用したトラフィック シェーピング

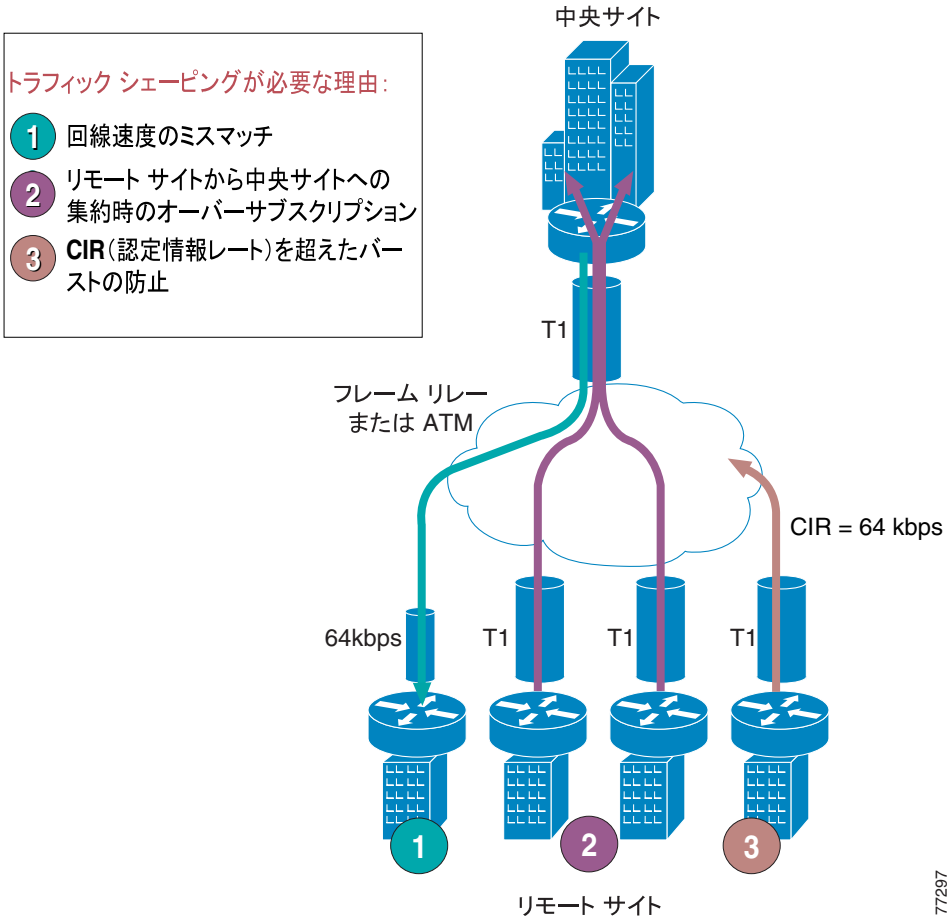


図 3-9 は、次の 3 つのシナリオを示しています。

1. 回線速度のミスマッチ

   中央サイトのインターフェイスは、一般に高速インターフェイス（たとえば、T1 以上）ですが、小規模なリモート サイトの支店のインターフェイス回線速度はかなり遅くなります（たとえば、64 Kbps）。データが中央サイトから低速リモート サイトにフル レートで送信される場合、リモート サイトのインターフェイスが輻輳し、音声パフォーマンスが低下する可能性があります。

2. 中央サイトとリモート サイト間のリンクのオーバーサブスクリプション

   複数のリモート サイトを 1 つの中央サイトに集約する場合、帯域幅をオーバーサブスクリプションにするのは、フレームリレーまたは ATM ネットワークでは一般的な方法です。たとえば、T1 インターフェイスで WAN に接続するリモート サイトが複数あるにもかかわらず、中

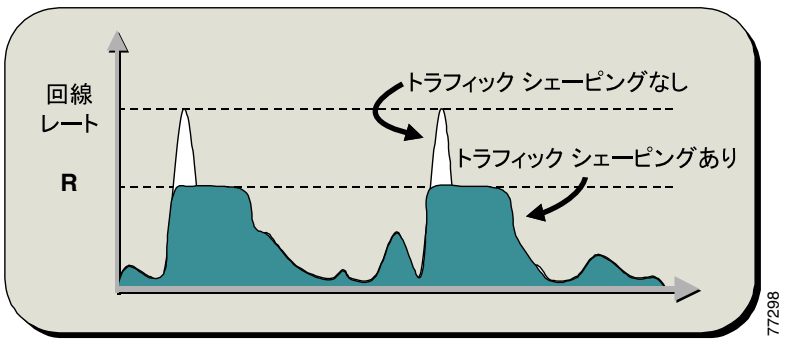
央サイトには 1 つの T1 インターフェイスしかない場合があります。この設定により、配置されたネットワークは統計多重化による恩恵を受けますが、中央サイトのルータ インターフェイスが、トラフィックのバースト時に輻輳し、音声品質が低下することがあります。

3. 認定情報レート（CIR）を超えたバースト

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

トラフィック シェーピングは、インターフェイスから送出されるトラフィックを、回線レート未満のレートに制限して、WAN の両端で輻輳が起きないようにし、こうした問題を解決します。図 3-10 は、このメカニズムの一般的な例を説明しています。ここで、R は、トラフィック シェーピングが適用される場合のレートです。

図 3-10　トラフィック シェーピングのメカニズム



Voice-Adaptive Traffic Shaping（VATS）

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

VATS を Voice-Adaptive Fragmentation（VAF）と組み合せて使用する場合（P.3-35 の「LFI（Link Fragmentation and Interleaving）」を参照）、インターフェイス上で音声アクティビティが検出されたときは、音声以外のトラフィックはすべてフラグメント化され、トラフィックはすべて WAN リンクの CIR に合せてシェーピングされます。

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

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_vats.htm

リソース予約プロトコル（RSVP）

リソース予約プロトコル（RSVP）は、異種ネットワークにわたってエンドツーエンドの QoS を動的にセットアップするための、実質上最初の業界標準プロトコルです。RSVP は IP を基盤として機能し、IETF によって RFC 2205 で最初に導入されました。RSVP を使用すると、アプリケーションがネットワーク帯域幅を動的に予約できます。RSVP を使用すると、ネットワークを流れるデータ フローに関して、アプリケーションが一定レベルの QoS を要求できます。分散型ネットワークに対応し、動的に機能する性質を持っているため、RSVP はあらゆるネットワーク トポロジにわたって帯域幅を予約できます。つまり、音声コールとビデオ コールにトポロジ対応コール アドミッション制御を提供できます。

この項では、RSVP プロトコルの原理と、このプロトコルと WAN インフラストラクチャとの対話を中心に、特に QoS について説明します。RSVP に基づくコール アドミッション制御の目的とメカニズムについては、P.9-1 の「コール アドミッション制御」の章で説明します。

この項では、次のトピックを扱います。

- RSVP の原理（P.3-38）
- WAN ルータでの RSVP と QoS（P.3-41）
- RSVP のアプリケーション ID（P.3-45）
- RSVP 設計上のベスト プラクティス（P.3-47）

RSVP の原理

RSVP は、データ フローのソース デバイスと宛先デバイスの間で交換され、パス上に存在する中間ルータで処理されるシグナリング メッセージを定義することによって、指定されたデータ フローのリソース予約をネットワークをまたいで実行します。RSVP シグナリング メッセージは、IP ヘッダーのプロトコル番号が 46 に設定されている IP パケットで、既存のルーティング プロトコルに従ってネットワーク内でルーティングされます。

パス上のすべてのルータで RSVP をサポートする必要はありません。このプロトコルは、RSVP に対応していないノードでは透過的に動作するように設計されています。各 RSVP 対応ルータで、RSVP プロセスがシグナリング メッセージを代行受信し、帯域幅リソースを「予約」するために、データ フローに含まれるルータ インターフェイスの QoS マネージャと対話します。パスの任意の場所で、使用可能なリソースがそのデータ フローには不十分な場合、ルータは予約要求を発信したアプリケーションに、失敗を示す信号を返します。

RSVP シグナリングの原理は、図 3-11 に示す例で説明できます。この図では、デバイス 1（IP アドレス 10.10.10.10）からデバイス 2（IP アドレス 10.60.60.60）に流れるデータ ストリーム用に、アプリケーションがネットワーク リソースを予約しようとします。

図 3-11　RSVP Path と Resv メッセージ フローの例

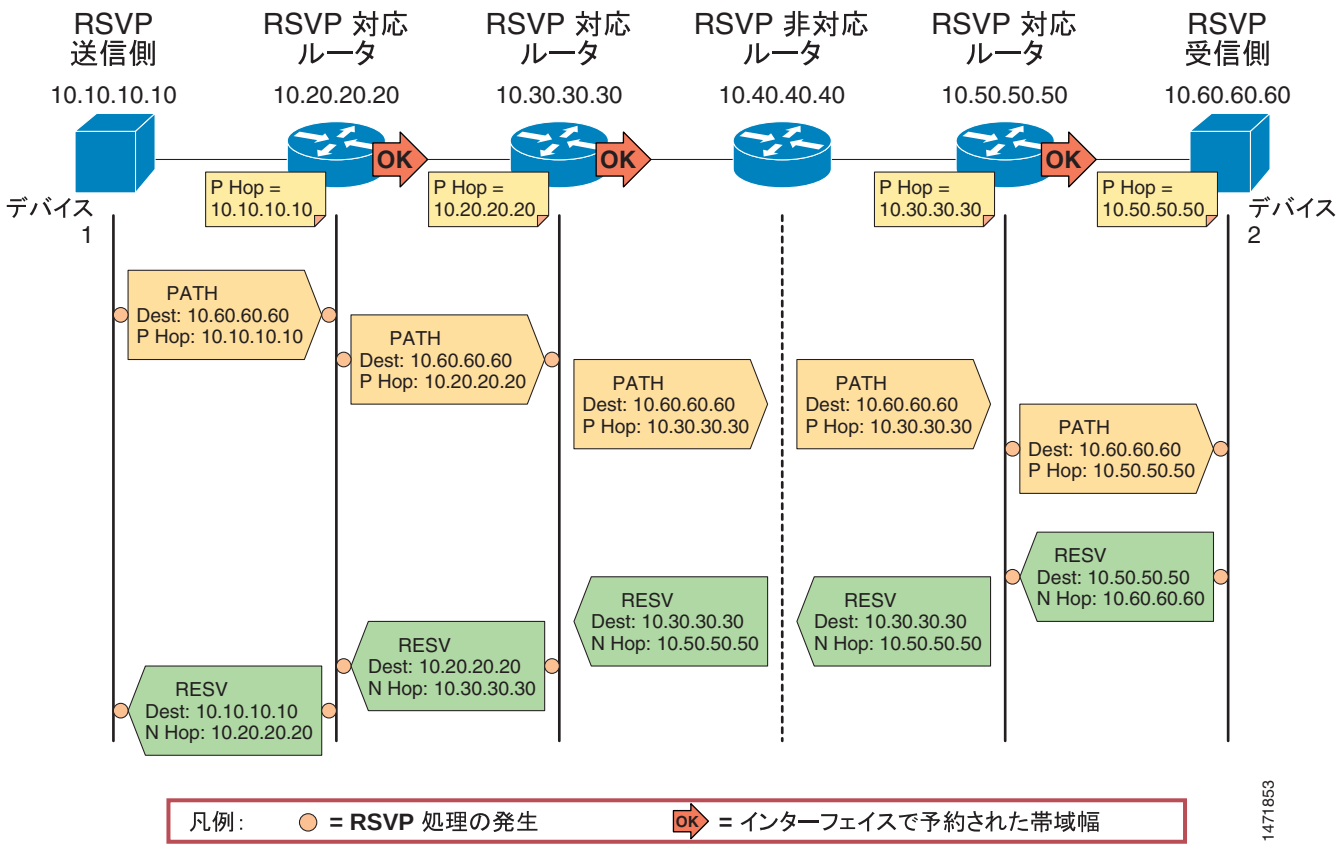


図 3-11 の例の RSVP シグナリング プロセスは、次の手順で行われます。

1. デバイス 1 にあるアプリケーションが Path という RSVP メッセージを発信します。このメッセージは、予約を要求するデータ フローと同じ宛先 IP アドレス（10.60.60.60）に送信され、IP ヘッダーの「router alert」オプションがオンにされて送信されます。Path メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。宛先 IP アドレス、プロトコル番号、および UDP/TCP ポートで構成され、RSVP 対応ルータでデータ フローを識別するために使用します。
   - 「sender Tspec」（トラフィック仕様）オブジェクト。予約が要求されたデータ フローの特性を示します。通常、データ レートとバースト サイズ（またはバケットの深さ）を指定するトークン バケット モデルに変換されます。
   - 「P Hop」（以前のホップ）オブジェクト。Path メッセージを最後に処理したルータ インターフェイスの IP アドレスが含まれます。この例では、P Hop は最初にデバイス 1 で 10.10.10.10 に設定されます。
2. 「router alert」オプションによって、Path メッセージは RSVP 対応ルータ（図 3-11 の 10.20.20.20）の CPU が代行受信し、RSVP プロセスに送信されます。RSVP は、このデータ フローのパス状態を作成し、Path メッセージに含まれる session オブジェクト、sender Tspec オブジェクト、および P Hop オブジェクトの値を格納します。次に、P Hop 値を発信インターフェイスの IP アドレス（この例では 10.20.20.20）で置き換えて、メッセージをダウンストリームに転送します。

3. 同様に、次の RSVP 対応ルータ（図 3-11 の 10.30.30.30）の CPU が Path メッセージを代行受信します。パス状態を作成し、P Hop 値を 10.30.30.30 に変更した後、このルータもメッセージをダウンストリームに転送します。
4. 次に、Path メッセージは、RSVP 非対応ルータ（図 3-11 の 10.40.40.40）に到達します。このルータでは RSVP が有効でないため、このメッセージは他の IP パケットと同様に、追加の処理やメッセージ オブジェクトの内容の変更は行われずに、既存のルーティング プロトコルに従ってルーティングされます。
5. その結果、Path メッセージは RSVP 対応ルータ（10.50.50.50）に転送され、ここでメッセージが処理され、対応するパス状態が作成され、メッセージがダウンストリームに転送されます。このルータで記録される P Hop には、ネットワーク パスの最後の RSVP 対応ルータの IP アドレス（この例では 10.30.30.30）がまだ含まれていることに注意してください。
6. デバイス 2 の RSVP 受信側は、P Hop 値が 10.50.50.50 の Path メッセージを受信します。ここで、Resv というメッセージを発信することによって、実際の予約が開始されます。このため、RSVP は受信側開始プロトコルと呼ばれます。Resv メッセージは、セッションのデータ フローの逆方向のパスに従って、予約要求を受信側から送信側にホップごとに伝達します。各ホップでの Resv メッセージの IP 宛先アドレスは、パス状態から取得した直前のホップ ノードの IP アドレスです。したがって、この例では、デバイス 2 は宛先 IP アドレスが 10.50.50.50 の Resv メッセージを送信します。Resv メッセージには、特に次のオブジェクトが含まれています。
   - 「session」オブジェクト。データ フローの識別に使用します。
   - 「N Hop」（次のホップ）オブジェクト。メッセージを生成したノードの IP アドレスが含まれます。この例では、N Hop は最初にデバイス 2 で 10.60.60.60 に設定されます。
7. 10.50.50.50 の RSVP 対応ルータがこのデータ フローの Resv メッセージを受信すると、受信した session オブジェクトを使用してパス状態情報と照合され、次の基準に基づいて予約要求を受け入れることができるかどうかが確認されます。
   - ポリシー制御：このユーザやアプリケーションが、この予約要求を行えるかどうか。
   - アドミッション制御：関連する発信インターフェイスに、この予約要求を満たせるだけの帯域幅リソースがあるかどうか。
8. この例では、10.50.50.50 でポリシー制御とアドミッション制御の両方が成功したとします。つまり、このセッションのパス状態の Tspec で提供される帯域幅は、発信インターフェイス（データ フローと同じ方向で、デバイス 1 からデバイス 2）で予約され、対応する「予約状態」が作成されるものとします。次に、10.50.50.50 のルータは、このセッションの P Hop に格納されている宛先 IP アドレス（10.30.30.30）にユニキャスト IP パケットとして送信することによって、Resv メッセージをアップストリームに送信できます。N Hop オブジェクトも、値 10.50.50.50 に更新されます。
9. 次に、Resv メッセージは、10.40.40.40 の RSVP 非対応ルータを通過します。ここでは、他の IP パケットと同様に、宛先 10.30.30.30 にルーティングされます。このメカニズムによって、RSVP シグナリングは、RSVP に対応していないノードが含まれる異種ネットワークで機能します。
10. 10.30.30.30 の RSVP 対応ルータは、Resv メッセージを受信し、手順 7 および 8 で説明したメカニズムに従って処理します。このホップでも、ポリシー制御およびアドミッション制御が成功したとします。帯域幅が発信インターフェイスで予約され、Resv メッセージが前のホップ（この例では 10.20.20.20）に送信されます。
11. 10.20.20.20 のルータで同様の処理が行われた後、Resv は最終的に RSVP 送信側のデバイス 1 に到達します。これによって、要求元のアプリケーションに対して、エンドツーエンド予約が確立され、ネットワークのすべての RSVP 対応ルータで、帯域幅がこのデータ フロー用に確保されたことが示されます。

この例では、2 つの主な RSVP シグナリング メッセージである Path と Resv がネットワークを通過し、予約を確立する方法を示しました。RSVP 標準では、エラー状態、予約失敗、およびリソースの解放を扱うその他のメッセージがいくつか定義されています。特に、ResvErr メッセージは、要求されたリソースがネットワーク上のどこかでポリシー制御またはアドミッション制御によって

予約できなかったことを示すために使用されます。たとえば、図 3-11 のノード 10.50.50.50 でアドミッション制御が失敗した場合、このノードは失敗の原因を示す ResvErr メッセージをデバイス 2 に送信して、アプリケーションがこの通知を受け取ります。

もう 1 つの RSVP プロトコルの重要な点として、ソフト状態アプローチの採用があります。これは、同一の Path メッセージと Resv メッセージを送信することによって、ネットワーク上でセッションごとにパス状態と予約状態をアプリケーションで定期的にリフレッシュする必要があるという意味です。あるセッションについて、一定の時間、ルータがリフレッシュ メッセージを受信しない場合、対応する状態が削除され、予約されたリソースが解放されます。これによって、RSVP は動的に、リンク障害によるネットワーク トポロジの変更またはルーティングの変更に対応できます。予約では、単純に、ルーティング プロトコルの決定に従って新しいルートのフローが開始され、古いルートの予約はタイムアウトして最終的に削除されます。

(注)　この項では、RSVP の原理とメカニズムの概要を中心に説明しています。プロトコルの動作および拡張の詳細、完全なメッセージ形式、および他のプロトコルとの対話については、http://www.ietf.org で入手可能な RSVP に関する多くの RFC ドキュメントを参照してください。

WAN ルータでの RSVP と QoS

RSVP は、長い間 Cisco ルータでサポートされていましたが、このマニュアルで推奨するほとんどの設定は、Cisco IOS Release 12.2(2)T で最初に導入された RSVP Scalability Enhancements 機能に基づいています。

各 Cisco IOS ルータ インターフェイス上で、次の Cisco IOS コマンドをインターフェイス設定モードで発行すると、RSVP を有効にし、RSVP で制御できる帯域幅の最大量を定義することができます。

```
ip rsvp bandwidth [interface-kbps] [single-flow-kbps]
```

interface-kbps パラメータには、RSVP が所定のインターフェイス上で予約できる帯域幅の上限を指定します。*single-flow-kbps* パラメータには、予約 1 つあたりの帯域幅の上限を指定します（要求している帯域幅がこれより大きいフローは、インターフェイス上に使用可能な帯域幅がある場合でも拒否されます）。

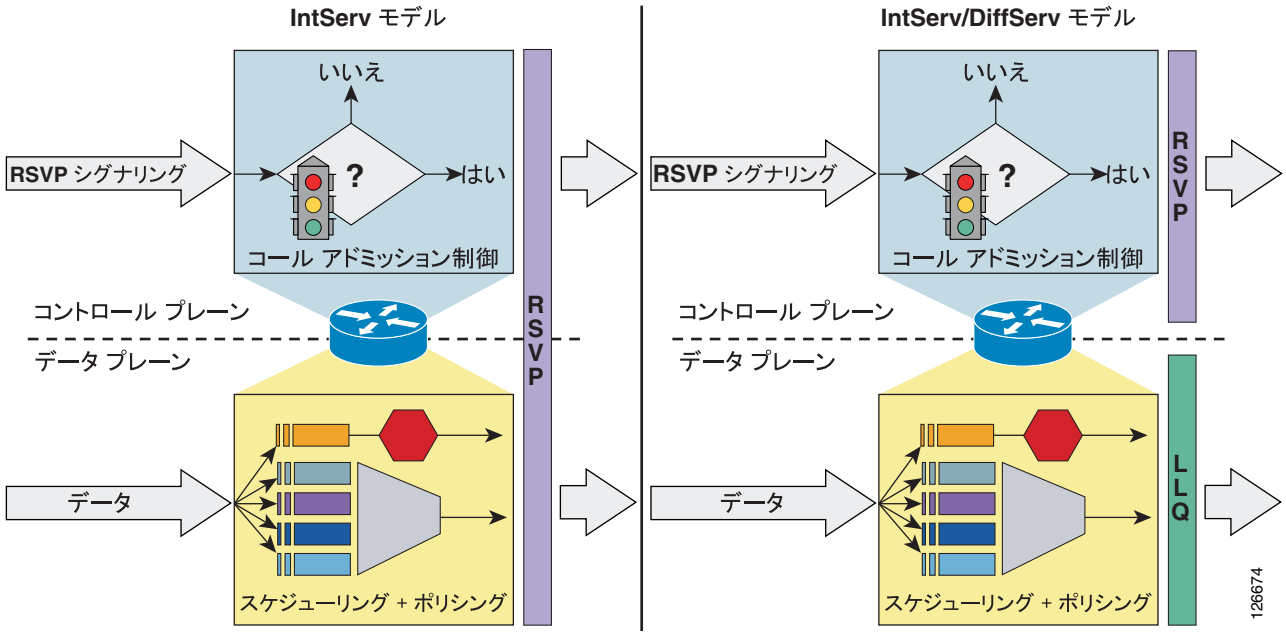
(注)　ルータ インターフェイスで RSVP を有効にすると、そのルータで RSVP に対応していないその他のすべてのインターフェイスが、RSVP メッセージをドロップします。RSVP メッセージのドロップを防ぐには、RSVP シグナリングが通過すると予想されるすべてのインターフェイスで RSVP を有効にします。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。

Cisco IOS では、2 つの異なるモデルに従って運用するように RSVP を設定できます。RFC 2210 で記述されている統合サービス（IntServ）モデル、および RFC 2998 で記述されている統合サービス / ディファレンシエーテッド サービス（IntServ/DiffServ）モデルです。どちらの RFC ドキュメントも、次の IETF Web サイトで入手できます。

http://www.ietf.org

図 3-12 に、Cisco IOS ルータから見た、これらの 2 つのアプローチの相違点を示します。

図 3-12　2 つの RSVP 運用モデル：IntServ と IntServ/DiffServ

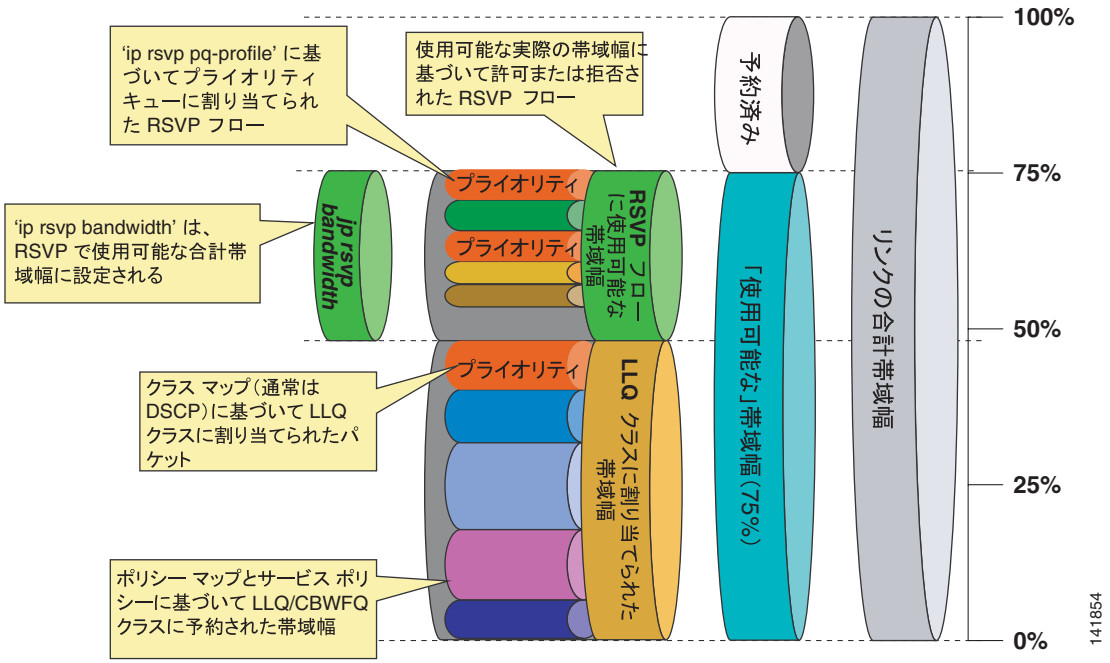


IntServ モデル

図 3-12 の左側に示すように、IntServ モデルの RSVP には、コントロール プレーンとデータ プレーンの両方が関係します。コントロール プレーンでは、RSVP が予約要求を許可または拒否します。データ プレーンでは、データ パケットを分類し、RSVP メッセージに含まれているトラフィック記述に基づいてポリシングし、適切なキューに入れます。RSVP が実行する分類は、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート、およびプロトコル番号を構成している、5 つのタプルに基づいています。このモデルでは、ルータを通過するすべてのデータ パケットを RSVP で代行受信して、RSVP でこの 5 タプルを検査し、確立済みの予約と一致するかどうかを検索できるようにする必要があります。一致が見つかった場合は、その予約のトラフィック仕様に従って、パケットが RSVP によってスケジューリングされ、ポリシングされます。

図 3-13 で示すように、IntServ モデルを Low Latency Queuing（LLQ）と組み合せる場合、使用可能な帯域幅が RSVP と事前定義済みの LLQ キューで分割されます。RSVP は、RSVP 予約された帯域幅への入力基準を制御します。ポリシー マップは、事前定義済みキューの入力基準を制御します。

図 3-13　IntServ モデルと LLQ の組み合せ



Cisco IOS ルータで IntServ 運用モデルを使用するには、インターフェイス設定モードで次のコマンドを使用します。

```
ip rsvp resource-provider wfq [interface | pvc]
no ip rsvp data-packet classification
```

これらのコマンドがアクティブになっている場合、RSVP は、新しい予約を許可または拒否するとき、**ip rsvp bandwidth** コマンドで定義した帯域幅上限に加えて、使用可能な実際の帯域幅リソースも基準にします。たとえば、bandwidth ステートメントを持つ LLQ クラスが存在する場合は、RSVP 予約に割り当てることのできる帯域幅プールから、それらの量が減分されます。LLQ クラスは、設定すると帯域幅を静的に割り当てます。これに対して、RSVP は、予約要求を受信するまでは帯域幅を一切割り当てません。このため、LLQ クラスに割り当てられることがない使用可能インターフェイス帯域幅を適度に確保して、予約要求を受信したときに RSVP が使用できるようにしておくことが重要です。

リンクで QoS メカニズムに割り当てることができる合計最大帯域幅はリンク速度の 75% なので、リンク帯域幅の 33% を RSVP で許可されるフローに予約するには、LLQ クラスに割り当てる帯域幅がリンク帯域幅の（75 - 33）= 42% を超えないようにする必要があります。

このモデルでは、各種キューへのパケットの割り当てを RSVP が制御します。このため、次の Cisco IOS コマンドをインターフェイス設定モードで使用すると、フローをプライオリティ キュー（PQ）に配置するかどうかを RSVP に通知するメカニズムを定義できます。

```
ip rsvp pq-profile [r [b [p-to-r]]]
```

RSVP は、パラメータ *r*、*b*、および *p-to-r* を使用して、シグナリングの対象になっているフローが PQ 処理を必要とする音声フローかどうかを判定します。これらのパラメータは、次の値を表しています。

- *r* = トラフィックの平均レート（単位：バイト / 秒）
- *b* = フローの最大バースト（単位：バイト）
- *p-to-r* = ピーク レートと平均レートの比率（単位：%）

特定のフローに関して RSVP メッセージで指定されているトラフィック特性が、このコマンドのパラメータ以下である場合、RSVP はフローを PQ に入れます。このコマンドにパラメータを指定しない場合は、一般に利用されている音声コーデック（G.711）の最大値である、次の値がデフォルトとして使用されます。

- *r* = 12,288 バイト / 秒
- *b* = 592 バイト
- *p-to-r* = 110%

IntServ/DiffServ モデル

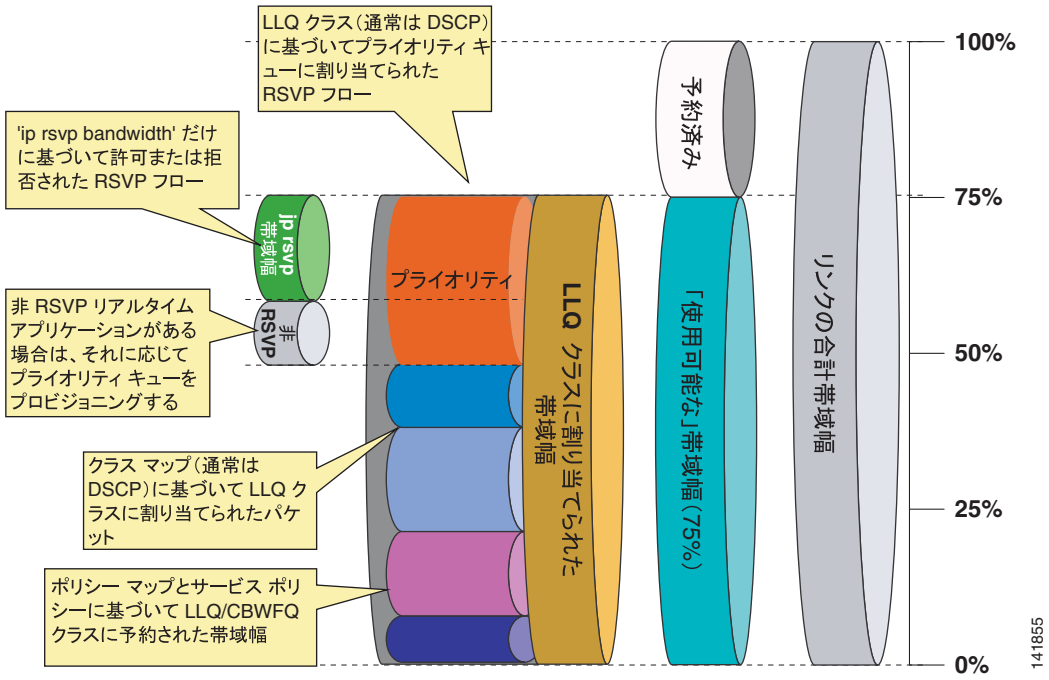
図 3-12 の右側に示すように、IntServ/DiffServ モデルの RSVP では、アドミッション制御を実行するコントロール プレーンのみが関係し、データ プレーンは関係しません。つまり、コール アドミッション制御機能は、スケジューリング機能およびポリシング機能とは独立しています。スケジューリングとポリシングは、事前定義済みのクラス マップ、ポリシー マップ、およびサービス ポリシーに従って、低遅延キュー（LLQ）アルゴリズムによって実行できます。

このため、IntServ/DiffServ モデルでは、すでに QoS にディファレンシエーテッド サービス アプローチを使用しているネットワークに対して、RSVP コール アドミッション制御を追加することができます。RSVP は、事前に設定された帯域幅量に基づいてコールを許可または拒否しますが、実際のスケジューリングは、各パケットの DSCP 値など、既存の LLQ 基準に基づいています。

図 3-14 に示すように、使用可能な帯域幅全体（リンク速度の 75%）を LLQ クラスに割り当てることができます。これが現在、一般的に行われている割り当てです。ポリシー マップは、各キューに許可されるトラフィックを定義します。RSVP は通常、優先トラフィック用に定義されている帯域幅の量までのフローを許可するように設定されますが、このモデルでは、RSVP がスケジューリングを調整しないため、事前定義済みのプライオリティ キューを超えて RSVP で許可されるトラフィックがドロップされたり、より低い優先度のキューにマッピングし直される可能性があることに注意してください。

優先トラフィックを送信するすべてのアプリケーションが RSVP 対応の場合は、RSVP 帯域幅がプライオリティ キューのサイズと一致するように設定できます。一方、図 3-14 に示すように、優先トラフィックを送信する必要がある RSVP 未使用アプリケーション（Cisco Unified CallManager スタティック ロケーション、ゲートキーパーなど）がある場合は、非 RSVP メカニズムで制御される優先トラフィックと RSVP で制御される優先トラフィックの間で、プライオリティ キューが分割されます。非 RSVP アドミッション制御と RSVP アドミッション制御のメカニズムを組み合せた場合は、プライオリティ キューでオーバーサブスクリプションが発生しないように、割り当てられた量を超える帯域幅を使用しないでください。

図 3-14　RSVP との LLQ 帯域幅割り当て



Cisco IOS ルータで IntServ/DiffServ 運用モデルを使用するには、インターフェイス設定モードで次のコマンドを使用します。

```
ip rsvp resource-provider none
ip rsvp data-packet classification none
```

これらのコマンドがアクティブになっている場合、RSVP は、**ip rsvp bandwidth** コマンドで定義された帯域幅上限のみに基づいて新しい予約を許可または拒否します。インターフェイス上で使用可能な実際の帯域幅リソースは考慮されません。許可された RSVP フローは、RSVP 以外の他のすべてのトラフィックと同じスケジューリング規則（たとえば、LLQ クラスとポリシー マップ）に従います。このため、RSVP 対応トラフィックを適切な DSCP 値を使用してマーキングし、対応する PQ または CBWFQ キューの帯域幅は、RSVP 対応トラフィックと他のすべてのトラフィックの両方に対応できるように設定することが重要です。

この運用モデルでは、RSVP はスケジューリング機能を制御しないため、**ip rsvp pq-profile** コマンドは非アクティブです。

RSVP のアプリケーション ID

アプリケーション ID（app-id）は、RSVP メッセージのポリシー要素に挿入可能な RSVP オブジェクトです。このオブジェクトは、RFC 2872 で説明されています。このポリシー オブジェクトは、アプリケーションを識別し、RSVP 予約要求に関連付けるために役立ちます。これによって、パスのルータは、アプリケーション情報に基づいて適切な決定ができます。

RSVP は、音声とビデオなど複数のアプリケーションのサポートに使用されるため、app-id が必要です。

app-id を使用しないと、RSVP でインターフェイスごとに設定できる帯域幅の値が 1 つだけになります。RSVP は、この帯域幅の上限に達するまで、要求を許可します。要求は区別されず、帯域幅が要求されているアプリケーション タイプも認識されません。その結果、RSVP が 1 つのタイプのアプリケーションだけに対応する要求を許可して、許可されている帯域幅を使い切ってしまい、帯域幅が使用できずに、後続のすべての要求を拒否する可能性があります。この場合、少数のビデオ コールが原因で、すべてまたはほとんどの音声コールが許可されないことがあります。たとえば、1000 ユニットを RSVP に割り当てた場合に、RSVP が 2 つの 384 kbps ビデオ コールで帯域幅のほとんどを使い切ってしまい、音声コール用の帯域幅がほとんど残らない可能性があります。

この問題は、個別のアプリケーションまたはトラフィック クラスごとに、個別の帯域幅上限を設定すると解決できます。アプリケーションごとに帯域幅を制限するには、アプリケーション帯域幅制限と対応する RSVP ローカル ポリシーをルータ インターフェイスに適用する必要があります。また、適切な帯域幅制限に対して許可できるように、アプリケーションを各予約要求フラグに割り当てる必要があります。

app-id は単一の情報ではなく、複数の可変長文字列になっています。RFC 2872 で説明されているように、オブジェクトには次の属性を含ることができます。

- アプリケーションの ID（APP）。この属性は必須です。
- グローバル固有識別情報（GUID）。オプションです。
- アプリケーションのバージョン番号（VER）。この属性は必須です。
- サブアプリケーション ID（SAPP）。任意の数のサブアプリケーション要素を含めることができます。オプションです。

次の例を参考にしてください。

- APP = AudioStream
- GUID = CiscoSystems
- VER = 5.0.1.0
- SAPP =（指定なし）

Cisco Unified CallManager でのアプリケーション ID の使用方法

RSVP のアプリケーション ID 機能をサポートできるよう、Cisco Unified CallManager には、RSVP を使用するオーディオおよびビデオ コール予約のタグ付けに使用するアプリケーション ID を定義するクラスタ全体の 2 つのサービス パラメータがあります。

- RSVP Audio Application ID（デフォルトは「AudioStream」）
- RSVP Video Application ID（デフォルトは「VideoStream」）

これらのサービス パラメータは変更可能ですが、あるクラスタの予約と、同じリンクを使用する別のクラスタの予約を区別する機能が必要な場合を除き、デフォルト値のまま使用することをお勧めします。

音声コールにタグを付ける方法

RSVP ポリシーを使用してロケーション間の音声コールを作成すると、オーディオ ストリームの予約に RSVP Audio Application ID のタグが付きます。

ビデオ コールにタグを付ける方法

RSVP ポリシーを使用してロケーション間のビデオ コールを作成すると、オーディオ ストリームの予約に RSVP Audio Application ID のタグが付き、ビデオ ストリームの予約に RSVP Video Application ID のタグが付きます。

アプリケーション ID コール アドミッション制御モデル

P.9-1 の「コール アドミッション制御」の章で説明するように、アプリケーション ID でサポートされるコール アドミッション制御モデルは、「静的」ロケーションでサポートされるモデルとは異なります。ビデオ コールのオーディオ ストリームは、RSVP Audio Application ID でマークされるため、音声コールの最小数を保証でき、使用可能な帯域幅全体を占有することもできます。ビデオ コールは、一定の最大帯域幅まで許可されますが、先に確立されている音声コールで帯域幅全体が消費されている場合は拒否されます。

RSVP 設計上のベスト プラクティス

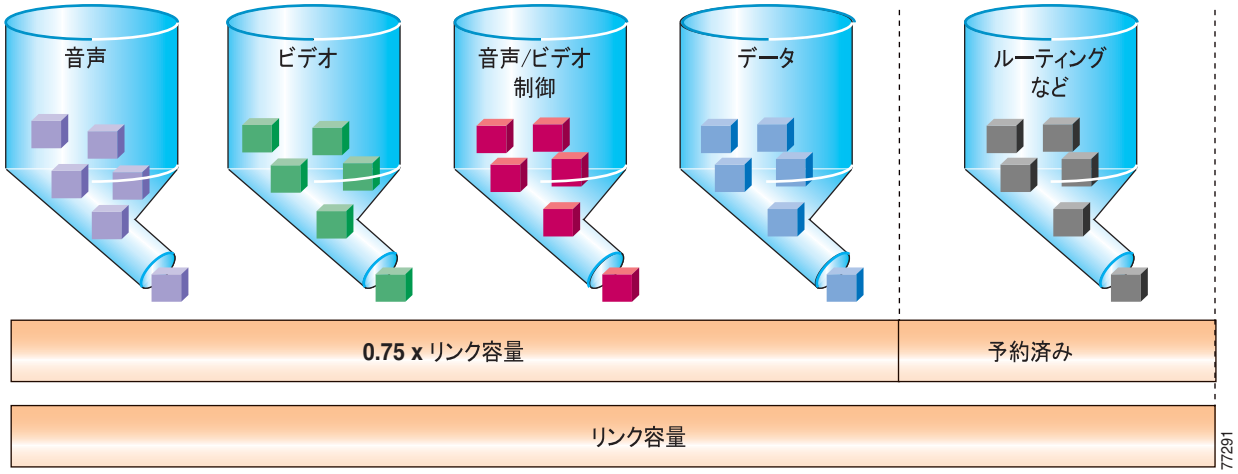
Cisco Unified CallManager と組み合せて RSVP を IP WAN に配置する場合は、次の設計上のベスト プラクティスに従います。

- 次のいずれかの条件に該当する場合は、IntServ/DiffServ モデルを採用することをお勧めします。
  - IP WAN インターフェイスのプライオリティ キュー（PQ）に入るトラフィックは、RSVP 対応トラフィックのみである。
  - PQ に入る RSVP 未使用トラフィックは、アウトバンドのコール アドミッション制御メカニズム（Cisco Unified CallManager ロケーションや Cisco IOS ゲートキーパーなど）によって、すべて確定的に一定量に制限される。
- レイヤ 2 のオーバーヘッドを考慮すると、すべての PQ トラフィックが RSVP 対応の場合、**ip rsvp bandwidth** コマンドで指定した値と **priority** コマンドで指定した値は一致する必要があります。
- ルータの 1 つ以上のインターフェイスで RSVP を有効にする場合は、RSVP メッセージがドロップされないように、RSVP シグナリングが通過すると考えられるすべてのインターフェイスでも RSVP を有効にする必要があります。インターフェイスでコール アドミッション制御を使用しない場合は、帯域幅の値をインターフェイス帯域幅の 75% に設定します。
- 一部の PQ トラフィックが RSVP 非対応の場合は、**ip rsvp bandwidth** コマンドとアウトバンド コール アドミッション制御メカニズムで指定した値の合計が、**priority** コマンドで指定した帯域幅値を超えないようにする必要があります。
- ビデオ コールで使用する最大帯域幅を制限する必要がある場合は、RSVP アプリケーション ID のサポートを有効にします。アプリケーション ID のサポートは、Cisco IOS Release 12.4(6)T で導入されました。詳細については、P.3-45 の「RSVP のアプリケーション ID」を参照してください。
- WAN リンクの両側のルータの WAN インターフェイスなど、ネットワークの両端で RSVP を有効にします。
- 速度が異なる冗長リンクなど、可能性があるすべての WAN 輻輳ポイントで RSVP を有効にします。
- ロードバランスされた MPLS WAN リンクでは、対称ルーティングを確保します。
- MLPPP、ATM-IMA、および FRF.16 を含むバンドル インターフェイスでは、RSVP 帯域幅を 1 つの物理リンクのサイズに設定します。
- トンネル インターフェイスでは、現在、RSVP を使用できません。
- Catalyst スイッチング プラットフォームでは、現在、RSVP を使用できません。

帯域幅のプロビジョニング

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

図 3-15　リンクの帯域幅プロビジョニング



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

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

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

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

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

- すべてのマルチサイト WAN 配置における音声およびビデオ ベアラ トラフィック（P.3-49 の「ベアラ トラフィック用のプロビジョニング」を参照）
- 集中型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-56 の「集中型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）
- 分散型コール処理を使用するマルチサイト WAN 配置におけるコール制御トラフィック（P.3-61 の「分散型コール処理を使用したコール制御トラフィック用のプロビジョニング」を参照）

ベアラ トラフィック用のプロビジョニング

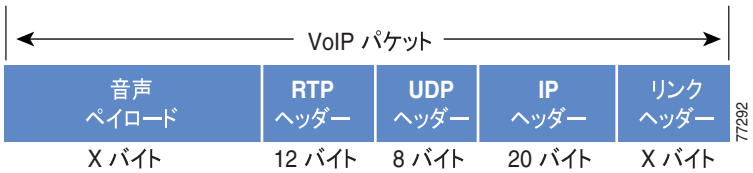
この項では、次のトラフィック タイプの帯域幅プロビジョニングについて説明します。

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

音声ベアラ トラフィック

図 3-16 に示されているように、VoIP（Voice-over-IP）パケットは、ペイロード、IP ヘッダー、ユーザ データグラム プロトコル（UDP）ヘッダー、Real-Time Transport Protocol（RTP）ヘッダー、およびレイヤ 2 リンク ヘッダーから構成されています。デフォルトのパケット レート 20 ms では、VoIP パケットには、G.711 の場合は 160 バイトのペイロードがあり、G.729 の場合は 20 バイトのペイロードがあります。SRTP（Secure Real-Time Transport Protocol）暗号化を使用すると、各パケットのペイロードは 4 バイト増加します。デフォルトのパケット レート 20 ms では、SRTP VoIP パケットには、G.711 の場合は 164 バイトのペイロードがあり、G.729 の場合は 24 バイトのペイロードがあります。IP ヘッダーは 20 バイト、UDP ヘッダーは 8 バイト、RTP ヘッダーは 12 バイトです。リンク ヘッダーの大きさは、使用されるレイヤ 2 メディアによって異なります。

図 3-16　一般的な VoIP パケット



VoIP ストリームによって消費される帯域幅を計算するには、パケットのペイロードとすべてのヘッダーを加算し（ビット単位）、1 秒当たりのパケット レート（デフォルトでは、毎秒 50 パケット）を掛けます。表 3-5 では、デフォルトのパケット レートである毎秒 50 パケット（pps）での VoIP フロー当たりの帯域幅を詳しく記述しています。表 3-5 には、レイヤ 2 ヘッダーのオーバーヘッドは含まれていません。また、RTP ヘッダー圧縮（cRTP）などの可能な圧縮方式を考慮していません。Cisco Unified CallManager Administration の Service Parameters メニューを使用すると、パケット レートを調整できます。

表 3-5 は、音声ペイロードと IP ヘッダーのみによって消費される帯域幅を示しています。ここでは、パケット レートとして、デフォルトのパケット レートである 50 パケット / 秒（pps）と、暗号化されていないペイロードと暗号化されたペイロードの両方のレートである 33.3 pps を使用しています。

表 3-5　音声ペイロードと IP ヘッダーのみの帯域幅使用量

コーデック	サンプリング レート	音声ペイロード（バイト数）	1 秒当たりのパケット数	1 会話当たりの帯域幅
G.711	20 ms	160	50.0	80.0 kbps
G.711（SRTP）	20 ms	164	50.0	81.6 kbps
G.711	30 ms	240	33.3	74.7 kbps
G.711（SRTP）	30 ms	244	33.3	75.8 kbps
G.729A	20 ms	20	50.0	24.0 kbps
G.729A（SRTP）	20 ms	24	50.0	25.6 kbps
G.729A	30 ms	30	33.3	18.7 kbps
G.729A（SRTP）	30 ms	34	33.3	19.8 kbps

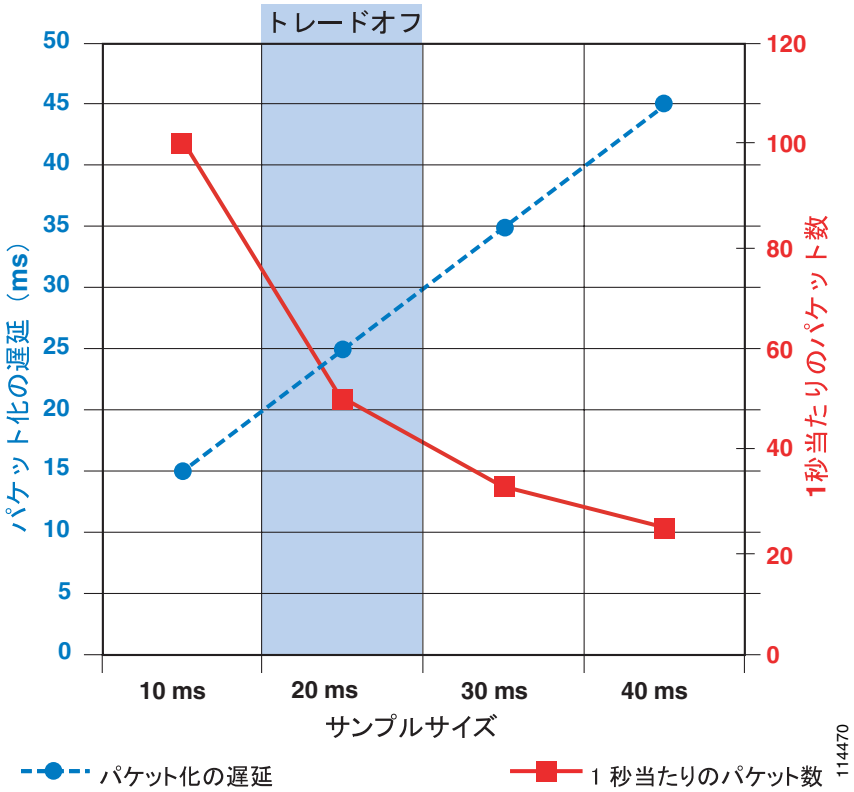
より正確な方法でプロビジョニングするには、帯域幅の計算にレイヤ 2 ヘッダーを含めます。表 3-6 は、レイヤ 2 ヘッダーを計算に含めたときの、音声トラフィックによって消費される帯域幅の量を示しています。

表 3-6　レイヤ 2 ヘッダーが含まれた帯域幅使用量

	ヘッダー タイプとサイズ						
コーデック	イーサネット 14 バイト	PPP 6 バイト	ATM 53 バイトのセルと 48 バイトのペイロード	フレームリレー 4 バイト	MLPPP 10 バイト	MPLS 4 バイト	WLAN 24 バイト
G.711（50.0 pps）	85.6 kbps	82.4 kbps	106.0 kbps	81.6 kbps	84.0 kbps	81.6 kbps	89.6 kbps
G.711（SRTP）（50.0 pps）	87.2 kbps	84.0 kbps	106.0 kbps	83.2 kbps	85.6 kbps	83.2 kbps	適用対象外
G.711（33.3 pps）	78.4 kbps	76.3 kbps	84.8 kbps	75.7 kbps	77.3 kbps	75.7 kbps	81.1 kbps
G.711（SRTP）（33.3 pps）	79.5 kbps	77.4 kbps	84.8 kbps	76.8 kbps	78.4 kbps	76.8 kbps	適用対象外
G.729A（50.0 pps）	29.6 kbps	26.4 kbps	42.4 kbps	25.6 kbps	28.0 kbps	25.6 kbps	33.6 kbps
G.729A（SRTP）（50.0 pps）	31.2 kbps	28.0 kbps	42.4 kbps	27.2 kbps	29.6 kbps	27.2 kbps	適用対象外
G.729A（33.3 pps）	22.4 kbps	20.3 kbps	28.3 kbps	19.7 kbps	21.3 kbps	19.7 kbps	25.1 kbps
G729A（SRTP）（33.3 pps）	23.5 kbps	21.4 kbps	28.3 kbps	20.8 kbps	22.4 kbps	20.8 kbps	適用対象外

30 ms を超えるサンプリング レートを設定することは可能ですが、これを行うと、通常、音声品質が非常に低下します。図 3-17 に示されているように、サンプリング サイズが増加すると、1 秒当たりのパケット数が減少するため、デバイスの CPU に与える影響は小さくなります。同様に、サンプル サイズが増加すると、1 パケット当たりのペイロードが大きくなるため、IP ヘッダーのオーバーヘッドが低下します。ただし、サンプル サイズが増加すると、パケット化の遅延も増加するため、音声トラフィックのエンドツーエンドの遅延が増加します。サンプル サイズを設定する場合は、パケット化の遅延と 1 秒当たりのパケット数とのトレードオフを考慮する必要があります。このトレードオフが 20 ms で最適化されている場合、30 ms のサンプル サイズでも、1 秒当たりのパケット数に対する遅延の比率は妥当なものになります。しかし、40 ms のサンプル サイズでは、パケット化の遅延が大きくなりすぎます。

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



ビデオ ベアラ トラフィック

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

ビデオの正確なオーバーヘッド率を計算できないという問題を解決するために、パケットが通過するレイヤ 2 メディアのタイプにかかわらず、コール速度に 20% を加算することをお勧めします。追加の 20% は、イーサネット、ATM、フレーム リレー、PPP、HDLC、およびその他の転送プロトコル間の差を吸収するための余裕となり、ビデオ トラフィックのバースト性に対するクッションにもなります（表 3-7 を参照）。

表 3-7　さまざまなビデオ コールの速度に対する推奨帯域幅

エンドポイントで要求されるコール速度	必要な実際のレイヤ 2 帯域幅
128 kbps	153.6 kbps
256 kbps	307.2 kbps
384 kbps	460.8 kbps
512 kbps	614.4 kbps
768 kbps	921.6 kbps
1.5 Mbps	1.766 Mbps
2.048 Mbps	2.458 Mbps
7 Mbps	8.4 Mbps

表 3-7 の値はコールの最大バースト速度を表し、クッションとして追加分が含まれていることに注意してください。コールの平均速度は、通常、この値を大幅に下回ります。メディア チャネルと帯域幅の使用に関する概念は、コール アドミッション制御の設定に使用する値を理解するために重要です。

RSVP を使用するベアラ トラフィックに関する追加の考慮事項

RSVP は、音声またはビデオだけに限らず、レイヤ 2 テクノロジーの広範囲にわたる任意のトラフィック フローの Quality of Service（QoS）の要求をサポートするように構築されました。このような処理を実現するために、RSVP は、QoS を要求しているトラフィック フローを詳細に記述して、中間ルータが正しくアドミッションを決定できるようにする必要があります。

RSVP 送信側は、ストリームの帯域幅要件を含む Path メッセージをトラフィック仕様（Tspec）の形式で生成します。RFC 2210 で説明されているように、Tspec にはトラフィック フローを詳細に記述する次の属性が含まれています。

- Token Bucket Rate [r]：平均トラフィック レート（バイト / 秒単位）
- Token Bucket Size [b]：フローの最大バースト（バイト単位）
- Peak Data Rate [p]：ピーク トラフィック レート（バイト / 秒単位）
- Minimum Policed Unit [m]
- Maximum Packet Size [M]

Cisco Unified CallManager で使用する RSVP 帯域幅の値の計算

Cisco Unified CallManager が Cisco RSVP Agent にコール フローの初期予約を行うよう指示する時点では、コールに関係するエンドポイントは、コーデック能力を完全には交換していません。この情報がないため、Cisco Unified CallManager がトラフィック フローの記述方法を決定するには、リージョン設定に依存する必要があります。トラフィック フローのサイズは、コーデック ビットレートとサンプリング レート（パケット / 秒）の関数です。リージョン設定にコーデックは含まれていますが、サンプリング レートは記述されていません。G.729 および G.711 音声コーデックの優先サンプリング レートは、クラスタ全体の次のサービス パラメータで定義されます。

- Preferred G711 millisecond packet size：デフォルトは 20 ms
- Preferred G729 millisecond packet size：デフォルトは 20 ms

ただし、コーデックのサンプリング レートはコールごとにネゴシエートされ、1 つ以上のエンドポイントでサポートされないために、優先設定が使用されないことがあります。呼び出し後の失敗の原因となる、能力が完全に交換された後で予約サイズが増加することを防ぐには、この初期予約を

コーデックの最悪のケース、または最小パケット サイズに対応したものにします。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。ほとんどの場合、デフォルトのサンプリング レートが使用され、結果として予約が削減されます。

(注)　Cisco Unified CallManager は、RSVP 予約に SRTP オーバーヘッドまたはレイヤ 2 オーバーヘッドを含めません。RSVP 帯域幅の値と比較するときに、プライオリティ キューを多めにプロビジョニングする必要があります（表 3-6 および表 3-7 を参照）。

音声ベアラ トラフィック

音声コーデックが G729 に設定されているリージョン間コール

- 初期要求：40 kbps。最悪ケースのシナリオの 10 ms を使用。
- 更新後の要求：24 kbps。優先サンプル サイズの 20 ms を使用。

音声コーデックが G711 に設定されているリージョン間コール

- 初期要求：96 kbps。最悪ケースのシナリオの 10 ms を使用。
- 更新後の要求：80 kbps。優先サンプル サイズの 20 ms を使用。

ビデオ ベアラ トラフィック

オーディオ ストリームと同様に、ビデオ ストリームの初期予約も、予約の時点でエンドポイントのコーデック能力が完全にはネゴシエートされていないため、リージョン設定に依存します。ビデオ コールのリージョン設定には、オーディオ ストリームの帯域幅が含まれます（詳細については、P.15-1 の「IP ビデオ テレフォニー」を参照）。オーディオ ストリームには独自の予約があるため、最終的なビデオ ストリームの予約は、リージョン設定から音声コーデックのビットレートを減算した値になります。ただし、これらのコーデックは完全にはネゴシエートされていないため、ビデオ ストリーム予約は、オーディオ ストリームがないという前提で、最悪のケースのシナリオで行われます。エンドポイント間でメディア能力が交換されると、予約は正しい帯域幅割り当てに修正されます。

ビデオは本質的にバースト性が高いため、ストリーム要件にオーバーヘッドを追加する必要があります（詳細については、P.3-51 の「ビデオ ベアラ トラフィック」を参照）。Cisco Unified CallManager は、次のように、ストリーム帯域幅を使用してオーバーヘッドの計算方法を決定します。

- ストリームが 256 kbps 未満の場合は、オーバーヘッドが 20% になる。
- ストリームが 256 kbps 以上の場合は、オーバーヘッドが 7% になる。

音声コーデックが G.729 で、ビデオ設定が 384 kbps のリージョン間ビデオ コールの場合

- 初期要求：384 * 1.07 = 410 kbps
- 更新後の要求：(384 - 8) * 1.07 = 402 kbps

音声コーデックが G.711 で、ビデオ設定が 384 kbps のリージョン間ビデオ コールの場合

- 初期要求：384 * 1.07 = 410 kbps
- 更新後の要求：(384 - 64) * 1.07 = 342 kbps

設定の推奨事項

初期予約は実際のパケット フローよりも大きくなるため、必要なコール数に対応するには、RSVP 帯域幅および LLQ 帯域幅を多めにプロビジョニングする必要があります。

N コールの RSVP 帯域幅をプロビジョニングする場合、N 番目のコールが許可されるように、N 番目の値を最悪のケースの帯域幅にすることをお勧めします。

次の例を参考にしてください。

- 4 つの G.729 ストリームをプロビジョニングする場合
  (3 * 24) + 40 = 112 kbps
- 4 つの G.711 ストリームをプロビジョニングする場合
  (3 * 80) + 96 = 336 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.729 オーディオ）をプロビジョニングする場合
  (3 * (384 - 8) + 384) * 1.07 = 1618 kbps
- 4 つの 384 kbps ビデオ ストリーム（G.711 オーディオ）をプロビジョニングする場合
  (3 * (384 - 64) + 384) * 1.07 = 1438 kbps

アプリケーション ID をサポートする Cisco IOS 設定

RSVP アプリケーション ID 機能のサポートは、Cisco IOS Release 12.4(6)T で導入されました。次の例では、このリリース以降が必要です。

プライオリティ キューの組み合せ

Cisco Unified CallManager によるアプリケーション ID サポートの実装で許可される機能（プライオリティ キューで使用可能なすべての帯域幅を音声コールで消費可能にする機能）を利用するために、音声とビデオのプライオリティ キューを分離するという以前の推奨事項を変更する必要があります（P.3-47 の「アプリケーション ID コール アドミッション制御モデル」を参照）。この機能を使用するには、音声とビデオの両方の一致基準を 1 つのクラスマップに組み合せる必要があります。音声トラフィックまたはビデオ トラフィックのいずれかが一致することが要件になるため、次のように、クラスマップの一致基準 **match-all** の代わりに **match-any** を使用する必要があります。

```
class-map match-any IPC-RTP
 match ip dscp ef
 match ip dscp af41  af42
```

音声トラフィックとビデオ トラフィックの両方をサポートするように、プライオリティ キューを設定します。次の設定例では、リンク帯域幅の 33% がプライオリティ キューに割り当てられます。

```
policy-map Voice-Policy
 class IPC-RTP
  priority percent 33
```

アプリケーション ID から RSVP ポリシー ID へのマッピング

RSVP ローカル ポリシーによって、アプリケーション ID を基に予約を制御するメカニズムが提供されます。アプリケーション ID は、**ip rsvp policy identity** コマンドで、RSVP ローカル ポリシーにマッピングされます。RSVP ローカル ポリシー ID はグローバルに定義され、コマンドにより、各インターフェイスで使用できます。各 ID には、アプリケーション ID と照合するために定義された 1 つのポリシー ロケータがあります。

ユーザができるだけ柔軟にアプリケーション ポリシー ロケータとローカル ポリシーを照合できるように、RSVP ローカル ポリシー コマンドライン インターフェイス（CLI）は、Unix 形式の正規表現によるポリシー ロケータに対するアプリケーション ID 一致基準を受け付けます。Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）など、既存の Cisco IOS コンポーネントの CLI では、正規表現が常に使用されます。Cisco IOS で正規表現を使用する方法の詳細については、次のマニュアルを参照してください。

- *Access and Communication Servers Command Reference*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios103/acscr103/index.htm

- *Using Regular Expressions in BGP*
  http://www.cisco.com/warp/public/459/26.html
- *Regex Engine Performance Enhancement*
  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_4/gt_rexpe.htm

デフォルトの Cisco Unified CallManager アプリケーション ID を照合するための RSVP ポリシー ID

```
ip rsvp policy identity rsvp-video policy-locator .*VideoStream.*
ip rsvp policy identity rsvp-voice policy-locator .*AudioStream.*
```

インターフェイスの RSVP ローカル ポリシー

アプリケーション ID サポートを設定するかどうかにかかわらず、RSVP をサポートするインターフェイスでは、**ip rsvp bandwidth** < *値* > コマンドを設定する必要があります。この値は、アプリケーション ID サポートの有無にかかわらず、そのインターフェイス上での 1 つの RSVP 予約または RSVP 予約の合計を超えることはできません。予約がローカル ポリシー チェックをパスした場合、予約の前に、インターフェイスの RSVP 帯域幅チェックにパスする必要があります。

アプリケーション ID に基づくローカル ポリシーは、**ip rsvp policy local identity** コマンドでインターフェイスに適用されます。

ポリシー ロケータ値と一致する予約については、ローカル ポリシーによって次の機能を実行できます。

- その予約がグループまたは単一の送信者として予約できる最大帯域幅の定義
- RSVP メッセージを転送するかどうか
- RSVP メッセージを受け入れるかどうか
- グループまたは送信者が予約できる最大帯域幅の定義

たとえば、Serial T1 でビデオ帯域幅の量を 384 kbps に制限するには、次のコマンドを使用します。

```
interface Serial0/0/1:0
 ip rsvp bandwidth 506
 ip rsvp policy local identity rsvp-video
  maximum bandwidth group 384
  forward all
```

catch-all ローカル ポリシーというデフォルト ローカル ポリシーもあります。このローカル ポリシーは、リンクで設定されているその他の RSVP ローカル ポリシーと一致しなかったすべての RSVP 予約と一致します。デフォルト ローカル ポリシーは、アプリケーション ID のタグ予約、またはタグなしトラフィックとして処理するアプリケーション ID のタグ予約と照合するために使用できます。

例

次の例は、P.3-46 の「Cisco Unified CallManager でのアプリケーション ID の使用方法」で説明したモデルを使用する音声コールとビデオ コールの両方をサポートします。音声コールには 352 kbps の帯域幅が保証され、ビデオ コールは 154 kbps の帯域幅に制限されます。音声コールは、使用可能な RSVP 帯域幅のすべてを使用できます。

```
interface Serial0/0/1:0
 ip address 10.2.101.5 255.255.255.252
 service-policy output Voice-Policy
 ip rsvp bandwidth 506
 ip rsvp data-packet classification none
 ip rsvp resource-provider none
 ip rsvp policy local identity rsvp-voice
  maximum bandwidth group 506
  forward all
 ip rsvp policy local identity rsvp-video
  maximum bandwidth group 154
  forward all
 ip rsvp policy local default
  no accept all ! Will not show in the configuration
  no forward all! Will not show in the configuration
```

この例では、アプリケーション ID を持たない RSVP 予約を受信したとき、またはアプリケーション ID が 2 つの設定済みオプションと一致しない RSVP 予約を受信したときに、予約が失敗します。この設定は、RSVP トラフィックが Cisco Unified CallManager で制御される Cisco RSVP Agent からのみ発信される場合に機能します。ただし、IP-IP ゲートウェイを経由するクラスタ間 RSVP トラフィックがある場合、または Cisco Unified CallManager 以外のコントローラからの RSVP メッセージがこのリンクを通過する場合は、予約を受け付けて転送するデフォルト ローカル ポリシーを設定し、このポリシーで最大帯域幅の値を設定する必要があります。複数の RSVP ローカル ポリシーを使用すると（ポリシーの合計が RSVP インターフェイス帯域幅より大きい場合）、RSVP 帯域幅をオーバーサブスクリプションにすることは可能ですが、予約は先着順になります。

集中型コール処理を使用したコール制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

その結果、制御トラフィック用の帯域幅を提供しなければならない領域は、支店のルータと、中央サイトの WAN アグリゲーション ルータとの間にあります。

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

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

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

(注)　この平均数が、特定の配置のニーズを満たさない場合、P.3-59 の「拡張公式」に記載されている拡張公式を使用して、推奨帯域幅を計算できます。

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

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

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

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

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

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

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

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

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

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

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

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

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

表 3-8　コール制御トラフィック用の推奨レイヤ 3 帯域幅（シグナリングの暗号化の有無別）

支店の規模（IP Phone とゲートウェイの数）	SCCP 制御トラフィック用の推奨帯域幅（暗号化なし）	SCCP 制御トラフィック用の推奨帯域幅（暗号化あり）	SIP 制御トラフィック用の推奨帯域幅（暗号化なし）	SIP 制御トラフィック用の推奨帯域幅（暗号化あり）
1 ～ 10	8 kbps	8 kbps	8 kbps	8 kbps
20	8 kbps	9 kbps	11 kbps	12 kbps
30	8 kbps	13 kbps	16 kbps	19 kbps
40	11 kbps	17 kbps	22 kbps	25 kbps
50	14 kbps	21 kbps	27 kbps	31 kbps
60	16 kbps	25 kbps	32 kbps	37 kbps
70	19 kbps	29 kbps	38 kbps	43 kbps
80	21 kbps	33 kbps	43 kbps	49 kbps
90	24 kbps	38 kbps	48 kbps	56 kbps
100	27 kbps	42 kbps	54 kbps	62 kbps
110	29 kbps	46 kbps	59 kbps	68 kbps
120	32 kbps	50 kbps	65 kbps	74 kbps
130	35 kbps	54 kbps	70 kbps	80 kbps
140	37 kbps	58 kbps	75 kbps	87 kbps
150	40 kbps	62 kbps	81 kbps	93 kbps

（注） 表 3-8 では、電話機あたりの毎時平均コール数を 10 と想定し、RSVP 制御トラフィックを含みません。この表の値に追加する RSVP 関連の帯域幅を判断するには、P.3-59 の「RSVP を使用するコールに関する考慮事項」を参照してください。

（注） サイト間コールに RSVP ベースのロケーション ポリシーを使用する場合は、表 3-8 の値を増やし、Cisco RSVP Agent の制御トラフィックの分を補正する必要があります。たとえば、コールの 10% が WAN を経由する場合、表 3-8 の値に 1.1 を掛けます。

拡張公式

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

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

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

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

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

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

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

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

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

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

RSVP を使用するコールに関する考慮事項

コール アドミッション制御で RSVP を使用するシステムでは、WAN を経由する IP コールが発生したときに、Cisco Unified CallManager と支店の Cisco RSVP Agent の間に追加の SCCP コール制御トラフィックが発生します。関連する帯域幅を計算するには、次の公式を使用します。

公式 5：SCCP 制御トラフィックに必要な推奨帯域幅、Cisco RSVP Agent 用

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

CHW は、異なる支店の IP Phone 間のコールや、異なるサイトにあるゲートウェイを通過するコールなど、IP WAN を経由する電話機あたりの毎時のコール数を表します。たとえば、20 台の電話機があり、電話機あたり毎時 10 コールが発生するサイトで、コールの 20% が IP WAN を経由する場合、CHW = 2 です。そこで、公式は (21*2)*20 = 840 bps になります。

公式 5 で計算される帯域幅を電話コール制御に必要な帯域幅に追加する必要があります。

シェアドライン アピアランスに関する考慮事項

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

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

  CHS = CHL *（ライン アピアランス数）/（回線数）

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

回線数 = 5

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

CHL = 6

CHS = 6 * (11 / 5) = 13.2

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

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

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

  - SCCP プロトコルと Cisco Unified CallManager 4.*x*：シェアドライン型の電話機ごとに 14 パケット
  - SCCP プロトコルと Cisco Unified CallManager 5.0：シェアドライン型の電話機ごとに 10 パケット
  - SIP プロトコルと Cisco Unified CallManager 5.0：シェアドライン型の電話機ごとに 6 パケット

  たとえば、Cisco Unified CallManager 4.1 と、同じ回線を共有する 5 台の電話機を使用する場合、トラフィックのシグナリング クラス用のキュー項目数は 70 以上に調整する必要があります。表 3-9 は、支店サイトでのシェアドライン アピアランスの量に基づいた推奨されるキュー項目数を示しています。

表 3-9　支店サイトごとの推奨されるキュー項目数

	SCCP		SIP
	Cisco Unified CallManager 4.x	Cisco Unified CallManager 5.0	Cisco Unified CallManager 5.0
シェアドライン アピアランスの数	キュー項目数（パケット数）	キュー項目数（パケット数）	キュー項目数（パケット数）
5	70	64	64
10	140	100	64
15	210	150	90
20	280	200	120
25	350	250	150

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

MPLS などのレイヤ 3 WAN テクノロジーを使用する場合は、単一のシグナリング キューで複数の支店を処理できます。この場合、処理するすべての支店の合計に対して、調整を行う必要があります。たとえば、Cisco Unified CallManager 4.1 を使用していて、10 箇所の支店に回線を共有する電話機が 5 台ずつある場合、中央サイトの WAN ルータのシグナリング キュー項目数は 700 に調整する必要があります。

分散型コール処理を使用したコール制御トラフィック用のプロビジョニング

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

この配置モデルには、次の考慮事項が適用されます。

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

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

WAN を通過する制御トラフィックは、次のカテゴリのいずれかに属します。

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

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

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

公式 5：仮想タイ ライン数に基づく推奨帯域幅

推奨帯域幅（bps）= 116 ∗（仮想タイ ライン数）

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

無線 LAN インフラストラクチャ

統合されたネットワークの無線 LAN（WLAN）部分に IP テレフォニーを追加する場合は、無線 LAN インフラストラクチャの設計が重要になります。Cisco Unified Wireless IP Phone 7920 などの無線 IP テレフォニー エンドポイントが追加されている場合、音声トラフィックは WLAN 上に移動しているため、そこで既存のデータ トラフィックと合流します。有線 LAN および有線 WAN インフラストラクチャの場合と同様、WLAN に音声を追加するには、基本的な設定と設計に関するベスト プラクティスに従って、可用性の高いネットワークを配置する必要があります。また、WLAN インフラストラクチャを適切に設計するには、ネットワーク全体でエンドツーエンドの音声品質を保証するために、QoS を理解して無線ネットワーク上に配置する必要もあります。次の項では、これらの要件について説明します。

- WLAN の設計と設定（P.3-62）
- WLAN の QoS（P.3-68）

WLAN の設計の詳細については、次の Web サイトで入手可能な『*Cisco Wireless LAN SRND*』のガイドを参照してください。

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

Cisco Wireless IP Phone 7920 の詳細については、次の Web サイトで入手可能な『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

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

WLAN の設計と設定

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

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

- 無線インフラストラクチャに関する考慮事項（P.3-62）
- 無線 AP の設定と設計（P.3-65）
- 無線セキュリティ（P.3-67）

無線インフラストラクチャに関する考慮事項

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

- VLAN（P.3-62）
- ローミング（P.3-63）
- 無線チャネル（P.3-63）
- 無線の干渉（P.3-64）
- WLAN 上のマルチキャスト（P.3-65）

VLAN

有線 LAN インフラストラクチャの場合と同様、無線 LAN に音声を配置する場合は、アクセス レイヤにある 2 つ以上の VLAN を有効にする必要があります。無線 LAN 環境のアクセス レイヤには、アクセス ポイント（AP）と最初のホップのアクセス スイッチが含まれます。AP とアクセス スイッ

チ上では、データ トラフィック用のネイティブ VLAN と、音声トラフィック用の Voice VLAN（Cisco IOS の場合）または Auxiliary VLAN（CatOS の場合）を設定する必要があります。この Voice / Auxiliary VLAN は、ネットワークにある他のすべての有線 Voice VLAN とは分離される必要があります。また、有線 LAN 上の音声エンドポイントの場合と同様、無線音声エンドポイントは、RFC 1918 プライベート サブネット アドレスを使用してアドレス指定される必要があります。無線インフラストラクチャを配置する場合は、WLAN AP の管理用に独立した管理 VLAN を設定することもお勧めします。この管理 VLAN には WLAN アピアランスを設定しないでください。つまり、関連付けられた Service Set Identifier（SSID）を設定することも、WLAN から直接アクセスできるように設定することもしないでください。

ローミング

無線インフラストラクチャでは、無線エンドポイントのローミングについて考慮することも非常に重要です。無線デバイスがレイヤ 2 で移動する場合、デバイスはその IP アドレスとネットワーク設定を保持します。このため、ローミングは、きわめて迅速に（100 ～ 400 ms で）行われる場合があります。ローミングで必要になるのは、Cisco LEAP または Extensible Authentication Protocol（EAP）を使用する場合の再認証と、エンドポイントが移動したことを示すために前回の AP と新しい AP の間で Inter-Access Point Protocol（IAPP）メッセージを受け渡しすることです。レイヤ 2 ローミングは、一般に、エンドユーザに負荷を感じさせません。

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。Cisco Catalyst 6500 シリーズ Wireless LAN Services Module（WLSM）によって、Cisco Wireless IP Phone 7920 は、アクティブ コールを維持しながらレイヤ 3 で移動できます。Cisco Wireless IP Phone 7920 は、静的 WEP または Cisco Centralized Key Management（Cisco CKM）プロトコルを使用して、レイヤ 3 で移動できます。Cisco CKM を使用すると、Cisco Wireless IP Phone 7920 は、WEP 128 または TKIP 暗号化の使用中に完全なレイヤ 3 モビリティを実現できます。シームレスなレイヤ 3 ローミングは、クライアントが同じモビリティ グループ内で移動するときだけに行われます。Cisco WLSM およびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

ワイヤレス LAN で 802.1x 認証を使用している場合は、ローミングのダウンタイムを最小にするため、Cisco CKM をお勧めします。レイヤ 2 またはレイヤ 3 のどちらで移動する場合も、デバイスのダウンタイムが 300 ～ 400 ms から 100 ms 未満に減少します。Cisco CKM は、Access Control Server（ACS）に送信する必要がある認証要求の数を減らすことによって、ACS の負荷も軽減します。

（注） Cisco Catalyst 4000 シリーズ スイッチをディストリビューション レイヤでレイヤ 3 デバイスとして使用する場合は、少なくとも、Supervisor Engine 2+（SUP2+）モジュールまたは Supervisor Engine 3（SUP3）モジュールが必要です。Supervisor Engine 1 または 2（SUP1 または SUP2）モジュールを使用すると、ローミング遅延が発生する場合があります。Cisco Catalyst 2948G、2948G-GE-TX、2980G、2980G-A、および 4912 スイッチも、ローミング遅延を引き起こすことがわかっています。これらのスイッチを無線音声ネットワークで使用することはお勧めできません。

無線チャネル

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

2.4 GHz 802.11b 用のチャネル設定を最適化するには、設定するチャネルの間に 5 チャネル以上の間隔を設定して、チャネル間の干渉やオーバーラップを防止する必要があります。許可されるチャネルが 1 ～ 11 の北米では、チャネル 1、6、および 11 が、AP と無線エンドポイント デバイスに使用

可能な 3 つの非オーバーラップ チャネルです。それに対して、許可されるチャネルが 1 ～ 13 の欧州では、5 チャネルの間隔がある組み合せは複数可能です。日本も許可されるチャネルが 1 ～ 14 なので、5 チャネルの間隔がある組み合せは複数可能です。

AP カバレッジは、同じチャネルで設定された AP 間でオーバーラップが発生しない（または最小になる）ように、配置する必要があります。同じチャネルのオーバーラップは、通常、19 dBm の間隔で発生します。ただし、オーバーラップのないチャネルで適切な AP 配置およびカバレッジを行うには、15% ～ 20% の最低限のオーバーラップが必要です。このオーバーラップ量であれば、無線エンドポイントが AP カバレッジ セルの間を移動するときにローミングが円滑に行われることが保証されます。オーバーラップが 15% ～ 20% 未満の場合、ローミングに時間がかかり、音質が悪くなることがあります。

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

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

無線の干渉

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

考えられる干渉源には、次のものがあります。

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

WLAN 上のマルチキャスト

音声デバイスを含む WLAN 上でマルチキャスト トラフィックを転送することはお勧めできません。その理由は、次のとおりです。

- AP に関連付けられたデバイスが省電力モードになると、マルチキャスト パケットが AP 上でバッファに入れられるため。

  Cisco Unified Wireless IP Phone 7920 などのデバイスが省電力モードになると、AP 上ですべてのマルチキャスト パケットがバッファに入れられます。この状態は、このデバイスが次にアクティブになるまで続きます。このバッファリングによりパケット遅延が発生し、AP に関連付けられたすべてのデバイスが、省電力モードでない場合も含めて影響を受けます。この状況は、Music On Hold やストリーミング ビデオなどのリアルタイム マルチキャスト アプリケーションで重大な問題となる場合があります。

- WLAN 上のマルチキャスト パケットは応答されないため、損失や破損が起きても再送信されません。

  AP と無線エンドポイントのデバイスは、リンク レイヤ上で応答を使用して、信頼性の高い配信を保証します。パケットが受信されない場合や応答されない場合、パケットは再送信されます。この再送信は、WLAN 上のマルチキャスト トラフィックには行われません。無線ネットワークでは有線ネットワークよりもビット エラーの発生頻度が高いため、この再送信が行われない場合は、有線 LAN よりも多くのパケットが損失します。

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

マルチキャスト トラフィックを使用する場合の追加の考慮事項については、P.7-1 の「Music on Hold」を参照してください。

無線 AP の設定と設計

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

AP の選択

無線音声を配置する場合は、次の AP を選択することをお勧めします。

- Aironet 350 シリーズ AP
- Aironet 1100 シリーズ AP
- Aironet 1130 シリーズ AP
- Aironet 1200 シリーズ AP
- Aironet 1240 シリーズ AP
- Aironet 1300 シリーズ AP
- Airespace 1000 シリーズ AP

これらの AP には、Cisco IOS Release 12.3(4) JA 以降が推奨されます。

AP の配置

Cisco アクセス ポイント（AP）を配置するときは、いかなる場合も、単一の AP に 15 ～ 25 を超えるデバイスを関連付けないでください。この数は、使用プロファイルによって異なります。AP 上のデバイスの数は、各デバイスがメディアにアクセスできる期間に影響します。デバイスの数が増加すると、トラフィックの競合も増加します。1 つの AP に 15 ～ 25 を超えるデバイスを関連付けると、AP のパフォーマンスが低下し、関連付けられたデバイスの応答時間が遅くなる可能性があります。

単一の AP に関連付けられるデバイスが 25 を超えないことを保証するメカニズムはありませんが、定期的なサイト調査を行い、ユーザとデバイスのトラフィック パターンを分析することによって、システム管理者はデバイスと AP の割合を管理できます。追加のデバイスおよびユーザを特定の領域でネットワークに追加した場合は、追加のサイト調査を行い、ネットワークにアクセスする必要があるエンドポイントの数に対応するために追加の AP が必要かどうかを判断する必要があります。

AP の設定

無線音声を配置する場合は、特定の AP 設定に関する次の要件に従います。

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

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

- AP と無線音声エンドポイントの伝送パワーを一致させる

  可能であれば、AP と音声エンドポイントの伝送パワーを一致させる必要があります。AP と音声エンドポイントの伝送パワーを一致させると、片方向オーディオ トラフィックの可能性を排除できます。伝送パワーが AP によって異なる場合は、すべての音声エンドポイントの伝送パワーを、伝送パワーが最も高い AP に一致するように設定する必要があります。

（注） Cisco Wireless IP Phone 7920 のファームウェアのバージョン 1.0(8) より、電話機は、Dynamic Transmit Power Control（DTPC）機能を利用して、その伝送パワーを現在の AP の Limit Client Power（mW）に基づいて自動的に調整するようになりました。

- データ レートを 11 Mbps に設定する

  最大 11 Mbps のデータ レートを設定すると、音声デバイスのスループットの最適レベルと、AP ごとのアクティブ コールの最大数が保証されます。

- RF チャネルの選択を手動で設定する（**Search for Least Congested Channel** オプションは使用*しないでください*）

  無線ネットワーク チャネルを制御し、チャネル オーバーラップを排除するには、そのロケーションに基づいて、AP ごとにチャネル数を手動で設定することが重要です。

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

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

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

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

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

  音声ポリシーとデータ ポリシーに各 VLAN のデフォルトの分類を設定することで、音声トラフィックがプライオリティ キューイング処理されることを保証します（詳細については、P.3-69 の「インターフェイス キューイング」を参照）。

無線セキュリティ

無線インフラストラクチャでは、セキュリティについて考慮することも重要です。無線電話機などの無線エンドポイントは、次のセキュリティ メカニズムのいずれかを使用して、無線ネットワークに接続することができます。

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）

  無線クライアントと、Protected Access Credential（PAC）を使用する認証、認可、アカウンティング（AAA）サーバとの間で認証トンネルの確立を最初に要求する標準ベースのセキュリティ プロトコルです。次に、無線エンドポイントはユーザ名とパスワードを使用して、トンネルを介して認証を行い、802.1X 経由でネットワークとの認証を行います。この認証が行われると、無線デバイスとの間のトラフィックは TKIP または WEP で暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。

- Wi-Fi Protected Access（WPA）

  標準ベースのセキュリティ プロトコルは、ネットワークに対して認証するためのユーザ名とパスワードを、無線エンドポイントに要求します。802.1X または事前共有キー（PSK）を使用してこの認証が発生すると、無線デバイスとの間のトラフィックは Temporal Key Integrity Protocol（TKIP）で暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。

- Cisco LEAP

  Cisco LEAP は、ネットワークに対して認証するためのユーザ名とパスワードを、無線エンドポイントに要求します。この認証が行われると、動的な鍵が生成され、無線デバイスとの間で送受信されるトラフィックが暗号化されます。この方法には、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、無線デバイスを認証するためのユーザ データベースにアクセスします。

- スタティック Wired Equivalent Privacy（WEP）

  スタティック WEP では、静的に設定された 40 ビットまたは 128 ビットの文字の鍵を、無線エンドポイントと AP の間で交換する必要があります。鍵が一致すると、無線デバイスはネットワークにアクセスできます。WEP 暗号化アルゴリズムには既知の脆弱性があることに注意してください。この脆弱性に加え、静的な鍵の設定と保守が複雑であることもあって、このセキュリティ メカニズムは、多くの場合に不適切となることがあります。

認証と ACS 配置モデル

Extensible Authentication Protocol（EAP）は、ネットワークおよび Voice VLAN へのアクセスに対して最もセキュアで堅牢なメカニズムを提供するため、無線デバイス認証（特に音声デバイス）に最適な方法です。EAP 準拠の RADIUS サーバが必要となるため、Cisco Secure ACS for Windows Server Version 3.1 以降の使用をお勧めします。

無線認証および暗号化用に EAP-FAST、WPA、または Cisco LEAP を配置する場合は、ネットワーク内の ACS の配置を慎重に検討して、次の ACS 配置モデルのいずれかを選択します。

- 集中型 ACS

  ACS サーバ（複数可）は、ネットワーク内の中央に配置され、ネットワーク内のすべての無線デバイスおよびユーザを認証するために使用されます。

- リモート ACS

  リモート ロケーションが低速リンクまたは輻輳した WAN リンクを介して中央サイトから分離しているネットワークでは、ACS サーバをリモート サイトに配置し、リモート無線デバイスまたはユーザをこのサーバでローカルに認証することができます。その結果、WAN リンクを介して集中型 ACS で認証する場合の遅延がなくなります。

- Cisco AP 上のローカルおよびフォールバック RADIUS サーバ

  リモート ロケーションが低速 WAN リンクを介して中央サイトから分離しているネットワークでは、ローカルの無線デバイスがローカル Cisco IOS AP に対して認証できます。Cisco IOS Release 12.2(11)JA 以降を実行する AP では、外部 ACS を利用しないでローカルにユーザおよびデバイスを認証できます。この機能では、単一の AP で最大 50 ユーザをサポートできます。この機能は、中央またはローカル ACS の代わりに使用することも、WAN または ACS に障害が発生してリモート サイトのユーザがローカル ACS または中央サイトの ACS にアクセスできなくなった場合に使用することもできます。

ACS の配置モデルを選択する場合は、認証サービスを冗長にして、無線デバイスがネットワークへのアクセスを試みるときに ACS が単一障害点にならないようにする必要があります。このため、各 ACS サーバはそのデータベースをセカンダリ サーバに複製する必要があります。さらに、WAN に障害が発生しても引き続きリモートの無線デバイスが認証できることを保証するため、リモート サイトにローカルの ACS サーバまたは AP の RADIUS サーバを配置することをお勧めします。

ACS サーバの配置に加え、ACS サーバに関連するユーザ データベースのロケーションの影響を考慮することも重要です。ACS サーバはユーザ データベースにアクセスして無線デバイスを認証する必要があるため、ユーザ データベースのロケーションは、認証に要する時間に影響を与えます。ユーザ データベースがネットワーク上の Microsoft Active Directory（AD）サーバである場合、ACS は AD サーバに認証要求を送信し、応答を待つ必要があります。ネットワークへの認証を試みる無線音声エンドポイントへの応答時間が最小になることを保証するには、ACS サーバ上でローカルにユーザを定義することをお勧めします。リモート データベースは、応答時間が不明であるため、認証時間に悪影響を与える場合があります。

WLAN の QoS

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

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

無線 QoS には、次の主要な設定領域があります。

- トラフィック分類（P.3-68）
- インターフェイス キューイング（P.3-69）
- 帯域幅のプロビジョニング（P.3-70）

トラフィック分類

有線ネットワーク インフラストラクチャの場合と同様、できるだけネットワークのエッジの近くで適切な無線トラフィックを分類またはマークすることが重要です。トラフィック マーキングは、有線および無線ネットワーク全体でキューイング方式の入力基準となるため、マーキングはできるだけ無線エンドポイントで行われる必要があります。無線ネットワーク デバイスによるマーキングまたは分類は、有線ネットワーク デバイスの場合（表 3-2 を参照）と同じである必要があります。

Cisco Wireless IP Phone 7920 は、有線ネットワークのトラフィック分類ガイドラインに従って、音声メディア トラフィックまたは RTP トラフィックを DSCP 46（または PHB EF）でマークし、音声シグナリング トラフィック（SCCP）を DSCP 24（または PHB CS3）でマークします。このトラフィックをマークしたら、ネットワーク全体でプライオリティ処理およびキューイング、またはベストエフォート型よりも優れた処理およびキューイングを行うことができます。無線音声デバイスはすべて、この方法でトラフィックをマークできる必要があります。無線ネットワーク上の他のトラフィックはすべて、ベストエフォート型としてマークされるか、有線ネットワークのマーキング ガイドラインで規定されているいくつかの中間分類を使用してマークされる必要があります。

インターフェイス キューイング

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

残念ながら、無線ネットワークで使用できるアップストリーム キューイングはほとんどありません。Cisco Wireless IP Phone 7920 などの無線デバイスは、パケットがデバイスを通過するときにアップストリームのキューイングを行えますが、無線ネットワークは共有メディアであるため、無線 LAN 上のすべてのクライアントでキューイングを行うようにするメカニズムは用意されていません。したがって、音声メディア パケットは無線エンドポイントを通過するときにプライオリティ処理される場合がありますが、このパケットは、他の無線デバイスが送信を試みている可能性のある他のすべてのパケットと競合することになります。このため、無線クライアントを AP ごとに 15 ～ 25 以下に抑えるというガイドラインに従うことがきわめて重要になります。このガイドラインの上限を超えると、音声パケットの遅延やジッタが増加する場合があります。

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

この 2 つのキューを設定するには、AP 上に 2 つの QoS ポリシーを作成します。1 つ目のポリシーには **voice** という名前を付け、**Default Classification for all packets on the Vlan** として **Voice <10 ms Latency (6)** サービス クラスを設定します。2 つ目のポリシーには **data** という名前を付け、**Default Classification for all packets on the Vlan** として **Best Effort (0)** サービス クラスを設定します。次に、**data** ポリシーをデータ VLAN の着信および発信無線インターフェイスに割り当て、**voice** ポリシーを Voice VLAN の着信および発信無線インターフェイスに割り当てます。QoS ポリシーを VLAN レベルで適用すると、AP が着信または発信するすべてのパケットを検査して、パケットに適用する必要があるキューイングのタイプを判別することはなくなります。この設定にすると、ダウンストリーム方向のすべての音声メディアおよびシグナリングがプライオリティ キューイング処理されることが保証されます。

帯域幅のプロビジョニング

帯域幅の適切なプロビジョニングも、無線ネットワーキングに対する QoS 要件の 1 つです。帯域幅のプロビジョニングでは、有線ネットワークと無線ネットワーク間の帯域幅や、AP で処理できる同時音声コールの数が対象となります。無線 AP は、一般に、アクセス レイヤ スイッチ ポートへの 100 Mbps リンクを介して有線ネットワークに接続されます。AP 上の入力イーサネット ポートは 100 Mbps のトラフィックを受信できますが、802.11b 無線ネットワークの最大スループットは 11 Mbps です。無線メディアの半二重性と無線ヘッダーのオーバーヘッドを考慮すると、802.11b 無線ネットワークの実質的なスループットは、約 7 Mbps となります。このように有線ネットワークと無線ネットワーク間のスループットは一致しないため、ネットワーク内でトラフィック バーストが発生すると、パケットがドロップする場合があります。

トラフィック バーストによって過剰なトラフィックが AP に送信されることを許可しても、結局は AP でドロップされるため、代わりに、レート制限または規制によってこのトラフィックを無線ネットワークで処理できるレートに抑えることをお勧めします。AP で過剰なトラフィックをドロップさせると、AP での CPU 使用率と輻輳が増加します。代わりに、有線アクセス レイヤ スイッチと無線 AP 間のリンク上でトラフィック レートを 7 Mbps に制限すると、トラフィックがアクセス レイヤ スイッチでドロップされることが保証されるため、AP の負荷がなくなります。AP に送信されるトラフィックのレート制限の詳細については、P.19-37 の「Cisco Unified Wireless IP Phone 7920」の項にある QoS の推奨事項を参照してください。無線ネットワークの配置によっては、実質的なスループットが 7 Mbps を下回ることがあります。特に、単一の AP に関連付けられたデバイスの数が推奨値より多い場合に該当します。

シスコでは、無線音声ネットワークのテストに基づいて、単一の 802.11b 無線 AP で最大 7 つのアクティブ G.711 音声ストリームまたは最大 8 つのアクティブ G.729 音声ストリームをサポートできることを確認しています。

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

これらの制限を超えると、音声品質が低下し、場合によっては音声コールがドロップされます。音声トラフィックの無線帯域幅をプロビジョニングするのに最適なコール アドミッション制御のメカニズムまたは方式はありませんが、Cisco Wireless IP Phone 7920 では、ネットワーク上の AP から受信するチャネル使用率の情報に基づいた、コール アドミッション制御または帯域幅プロビジョニングの簡易バージョンを使用できます。この情報は、QoS Basic Service Set（QBSS）を含むビーコンを介して、AP から電話機に送信できます。QBSS 要素の値が大きいほど、チャネル使用率が高くなり、チャネルと AP が追加の無線音声デバイスに対して十分な帯域幅を提供できる可能性が低くなります。QBSS 要素の値が最大しきい値を超える場合、無線 IP Phone によって試行されるコールはすべて拒否され、「Network Busy」メッセージが示されます。また、無線 IP Phone は、そのローミング アルゴリズムで QBSS 要素を検討し、QBSS 要素が最大しきい値を超えるビーコンを送信する AP には移動しません。

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

QBSS 情報要素が AP から送信されるのは、AP 上で **QoS Element for Wireless Phones** が有効になっている場合のみです（P.3-65 の「無線 AP の設定と設計」を参照）。

CHAPTER 4

ゲートウェイ

ゲートウェイは、IP テレフォニー ネットワークを PSTN（公衆電話交換網）、従来型の PBX、またはキー システムに接続するための複数の方法を提供します。ゲートウェイには、特殊なエントリレベルのスタンドアロン音声ゲートウェイから、機能が豊富なハイエンド統合ルータや Cisco Catalyst ゲートウェイまで、さまざまなものがあります。

この章では、IP テレフォニー ネットワークに適切なプロトコルと機能サポートを提供するために Cisco ゲートウェイを選択する際に、考慮すべき重要な要素について説明します。この章は、次の項で構成されています。

- Cisco ゲートウェイの概要（P.4-2）
- ゲートウェイの選択（P.4-3）
- QSIG サポート（P.4-21）
- FAX とモデムのサポート（P.4-22）
- ビデオ テレフォニー用のゲートウェイ（P.4-34）

Cisco ゲートウェイの概要

Cisco アクセス ゲートウェイにより、Cisco Unified CallManager は IP 以外の通信デバイスと情報を交換できます。Cisco アクセス ゲートウェイには、アナログとデジタルの 2 種類があります。

Cisco アクセス アナログ ゲートウェイ

Cisco アクセス アナログ ゲートウェイには、トランク ゲートウェイとステーション ゲートウェイの 2 つのカテゴリがあります。

- アクセス アナログ ステーション ゲートウェイ

  アナログ ステーション ゲートウェイは、Cisco Unified CallManager を POTS（Plain Old Telephone Service; 一般電話サービス）のアナログ電話機、IVR（Interactive Voice Response; 音声自動応答装置）システム、FAX マシン、およびボイスメール システムに接続します。ステーション ゲートウェイは、FXS（Foreign Exchange Station）ポートを備えています。
- アクセス アナログ トランク ゲートウェイ

  アナログ トランク ゲートウェイは、Cisco Unified CallManager を公衆網セントラル オフィス（CO）または PBX トランクに接続します。トランク ゲートウェイは、公衆網、PBX、またはキー システムへのアクセス用の FXO（Foreign Exchange Office）ポート、および従来型の PBX とのアナログ トランク接続用の E&M（recEive and transMit、または ear and mouth）ポートを備えています。応答と接続解除の監視の問題を最小限に抑えるために、可能な限り、デジタル ゲートウェイを使用してください。アナログ Direct Inward Dialing（DID; ダイヤルイン方式）および Centralized Automatic Message Accounting（CAMA）も、公衆網接続に使用できます。

Cisco アクセス デジタル トランク ゲートウェイ

Cisco アクセス デジタル トランク ゲートウェイは、PRI（一次群速度インターフェイス）、Basic Rate Interface（BRI; 基本速度インターフェイス）、または T1 CAS（チャネル連携信号）などのデジタル トランクを経由して、Cisco Unified CallManager を公衆網または PBX に接続します。デジタル T1 PRI トランクは、所定の従来型ボイスメール システムとの接続にも使用できます。

ゲートウェイの選択

IP テレフォニー ゲートウェイを選択する場合は、次の点を考慮してください。

- コア機能要件（P.4-3）
- ゲートウェイ プロトコル（P.4-3）
- ゲートウェイ プロトコルとコア機能要件（P.4-6）
- サイト固有のゲートウェイ要件（P.4-13）

コア機能要件

IP テレフォニー アプリケーションで使用するゲートウェイは、次のコア機能要件を満たす必要があります。

- DTMF（Dual tone multifrequency）リレー機能

  DTMF リレー機能、特にアウトバンド DTMF は、DTMF ディジットを音声ストリームから切り離し、音声ストリームまたはベアラ トラフィックの一部としてではなく、ゲートウェイ プロトコル（H.323、SCCP、MGCP、または SIP）シグナリング チャネルを通じて、シグナリング標識として送信します。音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失また歪みの可能性があるので、アウトバンド DTMF が必要です。

- 補足サービス サポート

  補足サービスは、一般に、保留、転送、および会議などの基本的なテレフォニー機能です。

- FAX/ モデム サポート

  FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。詳細については、P.4-22 の「FAX とモデムのサポート」を参照してください。

- Cisco Unified CallManager 冗長性サポート

  Cisco Unified Communications は、分散モデルに基づき、高いアベイラビリティを確保しています。Cisco Unified CallManager クラスタには、Cisco Unified CallManager の冗長性が用意されています。ゲートウェイは、プライマリ Cisco Unified CallManager に障害が発生した場合に、セカンダリ Cisco Unified CallManager に「re-home」機能をサポートする必要があります。冗長性は、Cisco Unified CallManager またはネットワークの障害時のコール存続可能性とは異なります。

企業での配置用に選択する IP テレフォニー ゲートウェイがすべて、上記のコア要件を満たしていることを確認するには、ゲートウェイ製品の資料を参照してください。さらに、どの IP テレフォニーの実装についても、各サイト特有の機能要件（たとえば、アナログまたはデジタル アクセス、DID、およびキャパシティ要件）があります（P.4-13 の「サイト固有のゲートウェイ要件」を参照してください）。

ゲートウェイ プロトコル

Cisco Unified CallManager（Release 3.1 およびそれ以降）では、次のゲートウェイ プロトコルがサポートされています。

- H.323
- メディア ゲートウェイ コントロール プロトコル（MGCP）

Cisco Unified CallManager Release 4.0 以降では、トランク側での Session Initiation Protocol（SIP）がサポートされています。Cisco Unified CallManager Release 5.0 の SIP トランクの実装は、より多くの機能をサポートするよう拡張されました。

Cisco Unified IP Phone は、超軽量プロトコルである（SCCP）を使用します。SCCP はマスター / スレーブ モデルを使用しますが、H.323 は、ピアツーピア モデルです。MGCP も、マスター / スレーブ モデルを使用します。

プロトコルの選択は、サイト特有の要件と機器の設置ベースによって決まります。たとえば、リモート サイトである支店の大部分のロケーションには、Cisco 2600XM、2800、3700、または 3800 シリーズのルータが設置されます。これらのルータは、Cisco IOS　Release 12.2.11(T)　および Cisco Unified CallManager Release 3.1 以降で、H.323 と MGCP 0.1 をサポートします。ゲートウェイの設定では、MGCP は設定が単純なので H.323 よりも優先されます。一方、サポートされるインターフェイスの堅牢性により、H.323 が MGCP より優先される場合もあります。

SMDI（Simplified Message Desk Interface）は、ボイスメール システムを PBX または Centrex システムに統合するための標準です。SMDI を介してボイスメール システムに接続し、アナログ FXS またはデジタル T1 PRI を使用するには、SCCP または MGCP プロトコルが必要です。これは、H.323 デバイスは、ポートのグループから、使用される特定の回線を識別しないからです。この目的に H.323 ゲートウェイを使用すると、Cisco Message Interface は、着信コールに使用される実際のポートまたはチャネルと、SMDI 情報とを正常に相関させることができません。

また、使用される Cisco Unified CallManager の配置モデルも、ゲートウェイ プロトコルの選択に影響を与える場合があります（P.2-1 の「IP テレフォニー配置モデル」の章を参照してください）。

表 4-1 では、どのゲートウェイが所定のプロトコルをサポートするかを示しています。これらのプロトコルはそれぞれ、コア ゲートウェイ要件をサポートするために多少異なる方法を使用します。P.4-6 の「ゲートウェイ プロトコルとコア機能要件」では、各プロトコルがこれらの機能要件をどのように満たしているかを説明します。

表 4-1　サポートされるゲートウェイ プロトコルと Cisco Unified Communications ゲートウェイ

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP	SIP
Cisco 3800	あり、Cisco IOS Release 12.3.11T 以降	あり、Cisco IOS Release 12.3.11T 以降	あり、Cisco IOS Release 12.3.11T 以降	あり、SIP トランク
Cisco 2800	あり、Cisco IOS Release 12.3.8T4 以降	あり、Cisco IOS Release 12.3.8T4 以降	あり、Cisco IOS Release 12.3.8T4 以降	あり、SIP トランク
Cisco 3700	あり サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	Cisco IOS Release 12.2.13T の DSP ファーム	あり、SIP トランク
コミュニケーション メディア モジュール（CMM）	あり サポート対象： • T1 CAS FXS • T1/E1 PRI • FXS	あり	なし	あり

表 4-1　サポートされるゲートウェイ プロトコルと Cisco Unified Communications ゲートウェイ（続き）

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP	SIP
Catalyst 6000 WS-X6608-x1 ゲートウェイ モジュール、および FXS モジュール WS-X6624	あり サポート対象： • T1 CAS E&M • T1 CAS FXS • T1/E1 PRI • FXS with WS-6624	なし	なし	なし
VG224	あり、FXS のみ Cisco IOS Release 12.3(T) 以降では、VG224 の会議とトランスコーディングもサポート	あり、FXS のみ	あり、Cisco IOS Release 12.4(2)T 以降	あり、SIP トランク
VG248	なし	なし	あり[1]	なし
Cisco ATA 188	あり、FXS のみ	あり、FXS のみ	あり、FXS のみ	あり、サードパーティ製の SIP 電話機
Cisco AS5350 Cisco AS5400	なし	あり	なし	あり、SIP トランク
Cisco AS5850	なし	あり	なし	あり、SIP トランク
Cisco 5300	なし	あり	なし	あり、SIP トランク
Cisco 3640 および 3660	あり サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	Cisco IOS Release 12.2.13T の DSP ファーム	あり、SIP トランク
Cisco 2600 および 2600XM[2]	あり サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	Cisco IOS Release 12.2.13T の DSP ファーム	あり、SIP トランク
Cisco 1751 および 1760	あり	あり	あり、会議およびトランスコーディング	あり、SIP トランク
VG200[3]	あり サポート対象： • アナログ FXS/FXO • T1 CAS（E&M Wink Start; Delay Dial のみ） • T1/E1 PRI	あり	あり（DSP ファーム）	なし

表 4-1　サポートされるゲートウェイ プロトコルと Cisco Unified Communications ゲートウェイ（続き）

Cisco ゲートウェイ	MGCP 0.1	H.323	SCCP	SIP
Cisco 7200	なし	あり	なし	あり、SIP トランク
Catalyst 4000 WS-X4604-GWY ゲートウェイ モジュール	あり	あり	なし	なし
Cisco ICS7750-MRP	なし	あり	なし	なし
Cisco ICS7750-ASI	なし	あり	なし	なし
DE-30+、DT-24+[4]	あり	なし	なし	なし
Cisco 827-V4[4]	なし	あり、FXS に対してサポート	なし	なし

1. VG248 は、H.323、MGCP、SIP のいずれでもなく、SCCP を使用するので、真のゲートウェイではありません。
2. IP テレフォニー アプリケーションには、Cisco 2800 シリーズ ルータを使用してください。Cisco 2600 ルータのメモリの考慮事項については、次の Web サイトの製品情報をご覧ください。http://www.cisco.com/warp/customer/cc/pd/rt/2600/prodlit/1675_pp.htm
3. VG200 は、Cisco 2800 ルータに置き換えられたので、販売終了になりました。VG200 の既存のモデルは、引き続き IP テレフォニー設置環境でご使用いただけます。
4. これらのモデルは、製造中止になりました。

（注） 配置する前に、Cisco IOS ソフトウェアのリリース ノートを調べて、機能またはインターフェイスのサポートを確認してください。

ゲートウェイ プロトコルとコア機能要件

ここでは、各プロトコル（SCCP、H.323、MGCP、および SIP）が次のゲートウェイ機能要件をどのようにサポートするかについて説明します。

- DTMF リレー（P.4-6）
- 補足サービス（P.4-8）
- Cisco Unified CallManager の冗長性（P.4-11）

DTMF リレー

DTMF（Dual-Tone Multifrequency）は、信号に音声帯域内の特定の周波数ペアを使用するシグナリング方式です。64 kbps の PCM（パルス符号変調）音声チャネルは、これらの信号を容易に伝送できます。しかし、音声圧縮に低ビット レート コーデックを使用する場合、DTMF 信号の損失または歪みの可能性があります。VoIP（Voice over IP）インフラストラクチャを介して DTMF トーンを伝送するアウトバンド シグナリング方式は、コーデックにより誘発されるこれらの症状を簡単に解決します。

SCCP ゲートウェイ

Cisco VG248 などの SCCP ゲートウェイは、伝送制御プロトコル（TCP）ポート 2002 を使用して、DTMF 信号をアウトバンドで伝送します。アウトバンド DTMF は、VG248 用のデフォルトのゲートウェイ設定モードです。

H.323 ゲートウェイ

Cisco 3700 シリーズ製品などの H.323 ゲートウェイは、DTMF 信号をアウトバンドで交換するための拡張 H.245 機能を使用して、Cisco Unified CallManager と情報を交換できます。次の例は、Cisco IOS ゲートウェイ上のアウトバンド DTMF 設定例です。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
CODEC g729ar8
dtmf-relay h245-alphanumeric
preference 0
```

MGCP ゲートウェイ

Cisco IOS ベースの VG224、2600XM、2800、3700、および 3800 プラットフォームは、Cisco Unified CallManager との通信に MGCP を使用します。MGCP プロトコルには、パッケージの概念があります。MGCP ゲートウェイは、始動後、DTMF パッケージをロードします。MGCP ゲートウェイは、制御チャネルを介して、受信した DTMF トーンを表すシンボルを送信します。次に、Cisco Unified CallManager は、これらの信号を解釈し、アウトバンドでシグナリング エンドポイントに DTMF 信号を渡します。DTMF リレーのグローバル設定コマンドは、次のとおりです。

```
mgcp dtmf-relay CODEC all mode out-of-band
```

Cisco Unified CallManager MGCP ゲートウェイ設定インターフェイスで、追加の設定パラメータを入力する必要があります。

Catalyst 6000、DE-30+、および DT-24+ はすべて、Cisco Unified CallManager Release 3.1 以降で MGCP をサポートします。デフォルトで DTMF リレーは使用可能であり、追加の設定は必要ありません。

SIP ゲートウェイ

Cisco IOS ベースの VG224、2600XM、2800、3700、3800 プラットフォームは、Cisco Unified CallManager との通信に SIP を使用できます。これらのプラットフォームはさまざまな方式の DTMF をサポートしていますが、Cisco Unified CallManager との通信に使用できるのは次の 2 つの方式だけです。

- Named Telephony Events（NTE）、または RFC 2833
- Unsolicited SIP Notify（UN）

次の例は、NTE 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay rtp-nte
```

次の例は、UN 用の設定を示しています。

```
dial-peer voice 100 voip
destination-pattern 555….
session target ipv4:10.1.1.1
session protocol sipv2
dtmf-relay sip-notify
```

DTMF 方式の選択の詳細については、P.6-1 の「メディア リソース」の章を参照してください。

補足サービス

補足サービスは、保留、転送、および会議などのユーザ機能を提供します。これらのサービスは、音声通信の確立の基本的な要件であると見なされます。IP テレフォニー ネットワークでの使用について評価される各ゲートウェイは、ソフトウェアの MTP（メディア ターミネーション ポイント）を使用しなくても、独自に補足サービスをサポートする必要があります。

SCCP ゲートウェイ

Cisco VG224、VG248、および ATA 188 ゲートウェイは、補足サービスを完全にサポートしています。SCCP ゲートウェイは、ゲートウェイと Cisco Unified CallManager 間のシグナリング チャネル、および SCCP を使用して、コール制御パラメータを交換します。

H.323 ゲートウェイ

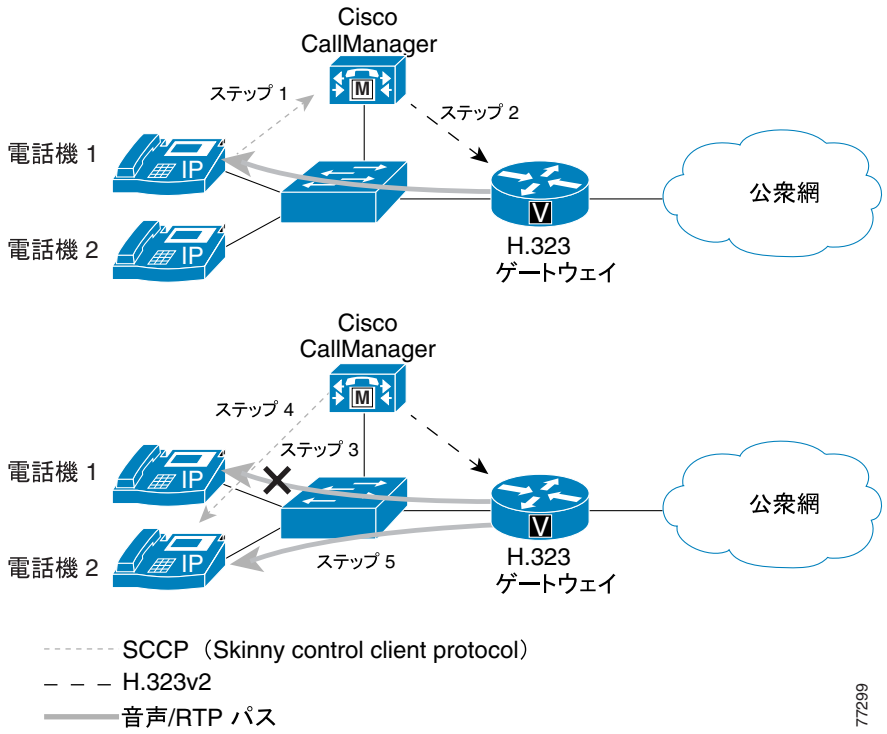
H.323v2 は、Open/Close LogicalChannel 機能と emptyCapabilitySet 機能を実行します。Cisco IOS Release 12.0(7)T および Cisco Unified CallManager Release 3.0 以降から始まった、H.323 ゲートウェイによる H.323v2 の使用により、MTP が補足サービスを提供する必要がなくなりました。Cisco Unified CallManager Release 3.1 以降では、トランスコーダが動的に割り当てられるのは、G.711 専用デバイスへのアクセスを提供すると同時に、WAN を介した G.729 ストリームを保持するために、コール中に必要な場合だけです。H.323v2 に対するフル サポートは、Cisco IOS Release 12.1.1T で利用可能です。

Cisco Unified CallManager を H.323 プロキシとして使用して、Cisco IOS ゲートウェイと IP Phone 間で H.323v2 コールがセットアップされた後は、その IP Phone は、ベアラ接続の変更を要求できます。RTP（Real-Time Transport Protocol）ストリームは、Cisco IOS ゲートウェイから IP Phone に直接接続されるので、サポートされる音声コーデックをネゴシエートできます。

図 4-1 と次の手順では、2 台の IP Phone 間のコール転送を示しています。

1. 電話機 1 が Cisco IOS ゲートウェイから電話機 2 にコールを転送しようとする場合、電話機 1 は、SCCP を使用して Cisco Unified CallManager に転送要求を出します。
2. Cisco Unified CallManager は、この要求を H.323v2 CloseLogicalChannel 要求に変換して、Cisco IOS ゲートウェイに送信して、適切な SessionID を求めます。
3. Cisco IOS ゲートウェイは、電話機 1 との RTP チャネルをクローズします。
4. Cisco Unified CallManager は、SCCP を使用して、Cisco IOS ゲートウェイとの RTP 接続をセットアップする要求を、電話機 2 に出します。同時に、Cisco Unified CallManager は、新しい宛先パラメータを指定して（ただし、同じ SessionID を使用）、Cisco IOS ゲートウェイに OpenLogicalChannel 要求を出します。
5. Cisco IOS ゲートウェイがこの要求を確認した後、RTP 音声ベアラ チャネルが、電話機 2 と Cisco IOS ゲートウェイとの間で確立されます。

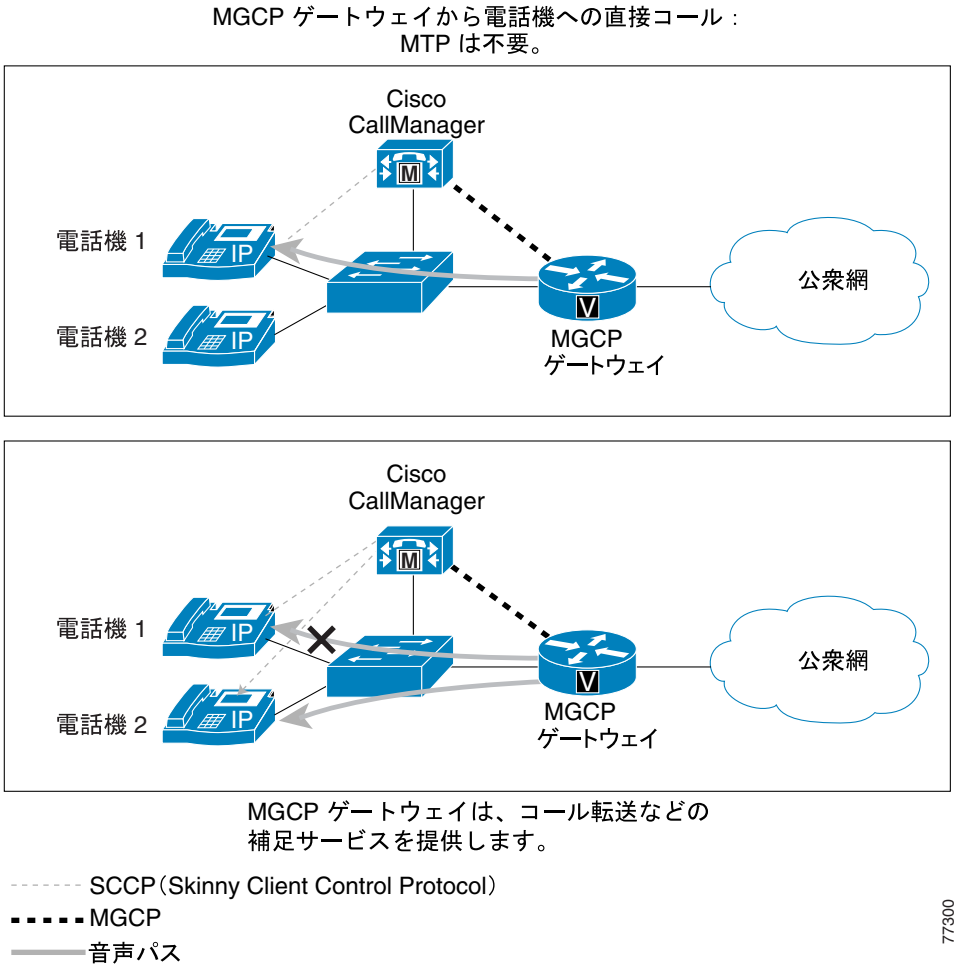
図 4-1　H.323 ゲートウェイの補足サービス サポート



MGCP ゲートウェイ

MGCP ゲートウェイは、MGCP プロトコルを使用して、保留、転送、および会議機能を完全にサポートします。MGCP プロトコルは、すべてのセッション機能を制御する、Cisco Unified CallManager とのマスター / スレーブ プロトコルであるので、Cisco Unified CallManager は、MGCP ゲートウェイの音声接続を容易に操作できます。IP テレフォニー エンドポイント（たとえば、IP Phone）が、セッションの変更（たとえば、コールを別のエンドポイントに転送する）を必要とする場合、そのエンドポイントは、セッションの変更を SCCP を使用して Cisco Unified CallManager に通知します。次に、Cisco Unified CallManager は、Session ID に関連した現在の RTP ストリームを終了し、新しいエンドポイント情報を使用して新しいメディア セッションを開始することを、MGCP UDP（ユーザ データグラム プロトコル）制御接続を使用して、MGCP ゲートウェイに通知します。図 4-2 では、プロトコルが MGCP ゲートウェイ、エンドポイント、および Cisco Unified CallManager 間で交換される様子を示しています。

図 4-2　MGCP ゲートウェイの補足サービス サポート



SIP ゲートウェイ

Cisco IOS SIP ゲートウェイへの Cisco Unified CallManager SIP トランク インターフェイスは、保留、ブラインド転送、在席転送などの補足サービスをサポートしています。補足サービスのサポートは、INVITE や REFER などの SIP 方式によって実現されます。詳細については、次のマニュアルを参照してください。

- *Cisco Unified CallManager 5.0 System Guide*。次のサイトにあります。

  http://www.cisco.com

- *Cisco IOS SIP Configuration Guide*。次のサイトにあります。

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/sip_c/sipc1_c/index.htm

Cisco Unified CallManager の冗長性

IP テレフォニー アーキテクチャの必須部分は、高価な専有の従来型の PBX システムの代わりに、低コストの分散型 PC ベース システムを提供することです。この分散型設計は、クラスタ化された Cisco Unified CallManager の堅固なフォールト トレラント アーキテクチャに適しています。最も単純な形式（2 システムのクラスタ）であっても、セカンダリ Cisco Unified CallManager は、最初にプライマリ Cisco Unified CallManager によって管理されていたすべてのゲートウェイの制御権を引き受ける必要があります。

SCCP ゲートウェイ

ブート後、Cisco VG224、VG248、および ATA 188 ゲートウェイには、Cisco Unified CallManager サーバ情報が提供されます。これらのゲートウェイが初期設定されるときに、Cisco Unified CallManager のリストがゲートウェイにダウンロードされます。このリストでは、プライマリ Cisco Unified CallManager とセカンダリ Cisco Unified CallManager に優先順位が付けられています。プライマリ Cisco Unified CallManager が通信不能になった場合、ゲートウェイはセカンダリ Cisco Unified CallManager に登録されます。

H.323 ゲートウェイ

Cisco H.323 ゲートウェイは、Cisco IOS Release 12.1(2)T における **dial-peer** コマンドと **voice class** コマンドの複数の拡張機能を使用して、冗長 Cisco Unified CallManager をサポートします。新しいコマンド **H.225 tcp timeout <seconds>** が追加されました。このコマンドは、H.323 ゲートウェイが、H.323 コール セットアップ用の H.225 制御接続の確立に要する時間をトラッキングします。H.323 ゲートウェイがプライマリ Cisco Unified CallManager との H.225 接続を確立できない場合、別の **dial-peer** ステートメントで指定されるセカンダリ Cisco Unified CallManager との接続を試行します。H.323 ゲートウェイは、次に高い **preference** 設定を指定する **dial-peer** ステートメントに移ります。次のコマンドを使用すると、H.323 ゲートウェイに対して Cisco Unified CallManager の冗長性を設定できます。

```
dial-peer voice 101 voip
  destination-pattern 1111
  session target ipv4:10.1.1.101
  preference 0
  voice class h323 1
dial-peer voice 102 voip
  destination-pattern 1111
  session target ipv4:10.1.1.102
  preference 1
  voice class h323 1
voice class h323 1
  h225 tcp timeout <1-30 sec>
```

MGCP ゲートウェイ

MGCP ゲートウェイには、プライマリ Cisco Unified CallManager との通信が失われた場合に、セカンダリ Cisco Unified CallManager にフェールオーバーする機能もあります。フェールオーバーが起きても、アクティブ コールは保持されます。

MGCP ゲートウェイのコンフィギュレーション ファイル内で、プライマリ Cisco Unified CallManager は、**call-agent <hostname>** コマンドを使用して指定され、セカンダリ Cisco Unified CallManager のリストは、**ccm-manager redundant-host** コマンドを使用して追加されます。プライマリ Cisco Unified CallManager とのキープアライブは、MGCP アプリケーション レベルのキープアライブ メカニズムを介して行われます。このメカニズムでは、MGCP ゲートウェイは、空の MGCP notify（NTFY）メッセージを Cisco Unified CallManager に送信し、確認応答を待ちます。バックアップ Cisco Unified CallManager とのキープアライブは、TCP キープアライブ メカニズムを介して行われます。

プライマリ Cisco Unified CallManager が後で使用可能になると、MGCP ゲートウェイは、元の Cisco Unified CallManager に「re-home」（つまり復帰）できます。この復帰は、ただちに行われることもあれば、設定可能な時間が経過した後、または接続されているすべてのセッションが解除された後に行われることもあります。これは、次のグローバル設定コマンドを使用して使用可能になります。

```
ccm-manager redundant-host <hostname1 | ipaddress1 > <hostname2 | ipaddress2>
[no] call-manager redundancy switchback [immediate|graceful|delay <delay_time>]
```

SIP ゲートウェイ

Cisco IOS SIP ゲートウェイでの冗長性は、H.323 と同様の方法で実現できます。SIP ゲートウェイがプライマリ Cisco Unified CallManager との接続を確立できない場合、高い優先順位を持ち、別の dial-peer ステートメントで指定されるセカンダリ Cisco Unified CallManager との接続を試行します。

デフォルトでは、Cisco IOS SIP ゲートウェイは dial-peer で設定された Cisco Unified CallManager の IP アドレスに SIP INVITE 要求を 6 回送信します。SIP ゲートウェイは、その Cisco Unified CallManager から応答を受信しなかった場合、他の dial-peer で設定された、優先順位の高い Cisco Unified CallManager との接続を試行します。

Cisco IOS SIP ゲートウェイは、INVITE に対する SIP 100 応答を 500 ms 待ちます。デフォルトでは、Cisco IOS SIP ゲートウェイがバックアップ Cisco Unified CallManager に到達するまでに最大 3 秒かかります。SIP INVITE の再試行回数は、**sip-ua** 設定で **retry invite** <*number*> コマンドを使用して変更できます。また、Cisco IOS SIP ゲートウェイが SIP INVITE 要求に対する SIP 100 応答を待つ期間は、**sip-ua** 設定で **timers trying** <*time*> コマンドを使用して変更できます。

バックアップ Cisco Unified CallManager へのフェールオーバーを高速化する別の方法としては、**dial-peer** 文での **monitor probe icmp-ping** コマンドの設定があります。Cisco Unified CallManager が Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）エコー メッセージ（ping）に応答しなかった場合、そのダイヤルピアはシャットダウンされます。このコマンドが役に立つのは、Cisco Unified CallManager が到達不能のときだけです。ICMP エコーメッセージは、10 秒ごとに送信されます。

次のコマンドを使用すると、Cisco IOS SIP ゲートウェイに対して Cisco Unified CallManager の冗長性を設定できます。

```
sip-ua
 retry invite <number>
 timers trying <time>

dial-peer voice 101 voip
 destination-pattern 2...
 session target ipv4:10.1.1.101
 preference 0
 monitor probe icmp-ping
 session protocol sipv2


dial-peer voice 102 voip
 destination-pattern 2...
 session target ipv4:10.1.1.102
 preference 1
 monitor probe icmp-ping
 session protocol sipv2
```

サイト固有のゲートウェイ要件

IP テレフォニーの実装にはそれぞれ、サイト固有の要件があります。次の質問は、IP テレフォニー ゲートウェイの選択に役立ちます。

- 公衆網（または PBX）アクセスは、アナログですか、デジタルですか。
- 公衆網または PBX には、どのタイプのアナログ（FXO、FXS、E&M、DID、CAMA）インターフェイス、またはデジタル（T1、E1、CAS、CCS）インターフェイスが必要ですか。
- 公衆網アクセスがデジタルである場合、どのタイプのシグナリングが必要ですか（T1　CAS、Q.931 PRI、E1 CAS、または R2）。
- PBX は、現在どのタイプのシグナリングを使用していますか。
  - FXO または FXS: ループ スタートまたはグラウンド スタート
  - E&M: ウィンク スタート、遅延スタート、または即時スタート
  - E&M: タイプ I、II、III、IV、または V
  - T1: CAS、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、または Proprietary D チャネル（CCS）シグナリング
  - E1: CAS、R2、Q.931 PRI（ユーザ側またはネットワーク側）、QSIG、DPNSS、Proprietary D チャネル（CCS）シグナリング
- PBX は、現在どのタイプのフレーム同期（SF、ESF、または G.704）と回線エンコーディング（B8ZS、AMI、CRC-4、または HDB3）を使用していますか。
- PBX に、専有シグナリングを渡す必要がありますか。必要な場合、そのシグナリングはどのタイムスロットで渡されますか。それは HDLC フレームですか。
- ゲートウェイにどれくらいのキャパシティが必要ですか。つまり、チャネルがいくつ必要ですか（一般に、音声チャネルが 12 本以上必要な場合は、デジタルの方が、アナログ ソリューションより費用対効果が高くなります）。
- ダイヤルイン方式（DID）が必要ですか。必要な場合は、アナログか、デジタルかを指定してください。（日本ではアナログ DID 未対応）
- 発呼回線 ID（CLID）が必要ですか。
- 発信者名が必要ですか。
- どのタイプの FAX およびモデム サポートが必要ですか。
- どのタイプの音声圧縮が必要ですか。
- どのタイプの補足サービスが必要ですか。
- PBX はクロッキングをサポートしますか。または PBX は、Cisco ゲートウェイがクロッキングをサポートすることを期待しますか。
- 必要なすべてのゲートウェイ、ルータ、およびスイッチを収容するラック スペースがありますか。

（注） ダイヤルイン方式（DID）とは、オペレータが介在しなくても、外部コールを直接、端末回線に着信できるようにする PBX（構内交換機）またはセントレック（Centrex）機能のことです。

（注） 発呼回線 ID（CLI、CLID、または ANI）とは、着呼側に対して発信番号を表示する、デジタル電話ネットワークで利用可能なサービスを指します。セントラル オフィス機器は、発信者の電話番号を識別し、発信者についての情報をコール自体と一緒に送信できるようにします。CLID は、ANI（Automatic Number Identification; 自動番号識別）と同義です。

Cisco Unified Communications ゲートウェイは、大部分の主要 PBX ベンダー製品と相互運用でき、EIA/TIA-464B に準拠しています。

可能な選択肢を絞り込むには、サイト固有およびコアのゲートウェイ要件から始めるのが適しています。必要な機能を指定した後、該当する設定ごとに、企業における規模と複雑さが異なる単一サイトの配置であるか、マルチサイトによる配置であるかに関係なく、ゲートウェイの選択を行うことができます。

次の表では、さまざまな Cisco ゲートウェイ モデルによってサポートされる機能とインターフェイス タイプをまとめています。

（注） 次の表では、Cisco IOS および Cisco Unified CallManager のリリース番号は、リストされている機能を特定のゲートウェイ プラットフォーム上でサポートできるようになったリリースを指しています。ハードウェア プラットフォームごとの推奨ソフトウェア リリースの推奨事項については、次の Web サイトの資料を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

Cisco アナログ ゲートウェイ

表 4-2 では、H.323 または SIP（Session Initiation Protocol）を使用する Cisco アナログ ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-3 では、メディア ゲートウェイ コントロール プロトコル（MGCP）を使用する Cisco アナログ ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。

表 4-2　サポートされるアナログ H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**FXS**	**FXO**	**E&M**	**FXO、バッテリ リバーサル**	**アナログ DID**	**CAMA 911**
3800 シリーズ	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり
3700 シリーズ	あり	あり	あり	あり	あり	あり
コミュニケーション メディア モジュール（CMM）24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
6608 および 6624	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG224	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	あり	なし	なし	なし	なし	なし
3600 シリーズ	あり	あり	あり	あり	あり	12.2.11T
2600 シリーズ	あり	あり	あり	あり	あり	12.2.11T
1751 および 1760	あり	あり	あり	あり	あり	あり
VG200	あり	あり	あり	なし	あり	なし
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
ICS 7750	あり	あり	あり	あり	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	なし	なし	なし	なし
827-4V[1]	あり	なし	なし	なし	なし	なし

1. このモデルは、製造中止になりました。

表 4-3　サポートされるアナログ MGCP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**FXS**	**FXO**	**E&M**	**FXO、バッテリ リバーサル**	**アナログ DID**	**CAMA 911**
3800 シリーズ	あり	あり	なし	あり	なし	なし
2800 シリーズ	あり	あり	なし	あり	なし	なし
3700 シリーズ	あり	あり	なし	あり	なし	なし
コミュニケーション メディア モジュール（CMM）24FXS	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
6608 および 6624	あり	なし	なし	なし	なし	なし
VG224	あり	なし	なし	なし	なし	なし
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	あり	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
3600 シリーズ	あり	あり	なし	あり	なし	なし
2600 シリーズ	あり	あり	なし	あり	なし	なし
1751 および 1760	あり	あり	なし	あり	なし	なし
VG200	あり	あり	なし	あり	なし	なし
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
ICS 7750	あり	あり	なし	なし	なし	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	なし	なし	なし	なし
827-4V[1]	なし	なし	適用対象外	適用対象外	適用対象外	適用対象外

1. このモデルは、製造中止になりました。

Cisco デジタル ゲートウェイ

表 4-4 ～表 4-7 では、H.323 または SIP を使用する Cisco デジタル ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。表 4-8 では、メディア ゲートウェイ コントロール プロトコル（MGCP）を使用する Cisco デジタル ゲートウェイに対してサポートされているインターフェイス タイプをリストしています。

表 4-4　BRI、T1 CAS、T1 FGB、T1 FGD、および T1 QSIG に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ							
Cisco ゲートウェイ	BRI（TE、ユーザ側）	BRI（NT、ネットワーク側）	BRI QSIG（Net3）	BRI 電話	T1 CAS（robbed ビット）	T1 FGB	T1 FGD	T1 QSIG
3800 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
2800 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
3700 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	適用対象外	適用対象外	適用対象外	あり	なし	なし	あり
6608 および 6624	適用対象外	適用対象外	適用対象外	適用対象外	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし	なし	なし
3600 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
2600 シリーズ	あり	あり	あり	なし	あり	なし	あり	あり
1751 および 1760	なし	あり	あり	なし	あり	なし	なし	あり
VG200	あり	あり	なし	なし	あり	なし	あり	なし
7x00 ファミリー	適用対象外	適用対象外	適用対象外	適用対象外	あり	なし	あり	あり
ICS 7750	あり	あり	なし	なし	あり	なし	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	なし	あり	なし	あり	なし	あり	あり
827-4V[1]	なし	なし	なし	なし	なし	なし	なし	なし

1. このモデルは、製造中止になりました。

表 4-5　T1 PRI SL-1、4ESS、および 5ESS に対してサポートされるデジタル H.323 および SIP 機能

Cisco ゲートウェイ	インターフェイス タイプ					
	T1 PRI（ユーザ、DMS-100）	T1 PRI（ネットワーク、SL-1）	T1 PRI（ユーザ、4ESS）	T1 PRI（ネットワーク、4ESS）	T1 PRI（ユーザ、5ESS）	T1 PRI（ネットワーク、5ESS）
3800 シリーズ	あり	将来的にサポート	あり	あり	あり	あり
2800 シリーズ	あり	将来的にサポート	あり	あり	あり	あり
3700 シリーズ	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	あり	あり	あり	あり
6608 および 6624	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし
3600 シリーズ	あり	将来的にサポート	あり	あり	あり	あり
2600 シリーズ	あり	将来的にサポート	あり	あり	あり	あり
1751 および 1760	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
VG200	あり	なし	あり	なし	あり	なし
7x00 ファミリー	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
ICS 7750	あり	なし	あり	なし	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	将来的にサポート	あり	将来的にサポート	あり	将来的にサポート
827-4V[1]	なし	なし	なし	なし	なし	なし

1. このモデルは、製造中止になりました。

表 4-6　T1 PRI NI2、NFAS、および Network Specific Facilities（NSF）サービスに対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**T1 PRI（ユーザ、NI2）**	**T1 PRI（ネットワーク、NI2）**	**T1 PRI NFAS（ユーザ、DMS-100）**	**T1 PRI NFAS（ユーザ、4ESS）**	**T1 PRI NFAS（ユーザ、5ESS）**	**T1 PRI（Megacom または SDN、4ESS）**
3800 シリーズ	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり
3700 シリーズ	あり	あり	あり	あり	あり	あり
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	あり	あり	あり	将来的にサポート	将来的にサポート	なし
6608 および 6624	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし
3600 シリーズ	あり	あり	あり	あり	あり	あり
2600 シリーズ	あり	あり	あり	あり	あり	あり
1751 および 1760	あり	あり	なし	なし	なし	なし
VG200	あり	あり	なし	なし	なし	なし
7x00 ファミリー	あり	あり	なし	なし	なし	なし
ICS 7750	あり	あり	あり	あり	あり	なし
Catalyst 4000 Access Gateway Module（AGM）	あり	あり	将来的にサポート	将来的にサポート	将来的にサポート	将来的にサポート
827-4V[1]	なし	なし	なし	なし	なし	なし

1. このモデルは、製造中止になりました。

表 4-7　E1 および J1 に対してサポートされるデジタル H.323 および SIP 機能

	インターフェイス タイプ						
Cisco ゲートウェイ	**E1 CAS**	**E1 MELCAS**	**E1 R2**	**E1 PRI（ユーザ側、Net5）**	**E1 PRI（ネットワーク側、Net5）**	**E1 QSIG**	**J1**
3800 シリーズ	あり	あり	あり	あり	あり	あり	あり
2800 シリーズ	あり	あり	あり	あり	あり	あり	あり
3700 シリーズ	あり	あり	あり	あり	あり	あり	あり
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	なし	なし	あり	あり	あり	あり	適用対象外
6608 および 6624	なし	なし	なし	なし	なし	なし	なし
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	なし	なし	なし	なし	なし	なし	なし
Analog Telephone Adapter（ATA）	なし	なし	なし	なし	なし	なし	なし
3600 シリーズ	あり	あり	あり	あり	あり	あり	あり
2600 シリーズ	あり	あり	あり	あり	あり	あり	あり
1751 および 1760	なし	なし	あり	あり	あり	あり	なし
VG200	なし	あり	あり	あり	あり	なし	あり
7x00 ファミリー	あり	なし	あり	あり	あり	あり	なし
ICS 7750	なし	なし	あり	あり	あり	なし	なし
Catalyst 4000 Access Gateway Module（AGM）	なし	なし	あり	あり	あり	あり	なし
827-4V[1]	なし	なし	なし	なし	なし	なし	なし

1. このモデルは、製造中止になりました。

表 4-8　サポートされるデジタル MGCP 機能

	インターフェイス タイプ					
Cisco ゲートウェイ	**BRI**[1]	**T1 CAS（E&M）**	**T1 PRI**	**T1 QSIG**	**E1 PRI**	**E1 QSIG**
3800 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
2800 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
3700 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
コミュニケーション メディア モジュール（CMM）24FXS	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
CMM-6T1/E1	適用対象外	あり	あり	あり	あり	あり
6608	適用対象外	あり	あり	あり	あり	あり
6624	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG224	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
VG248	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
Analog Telephone Adapter（ATA）	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外
3600 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
2600 シリーズ	12.4(2)T	あり[2]	あり[2]	あり[2]	あり[2]	あり[2]
1751 および 1760	12.3(14)T	あり	あり	あり	あり	あり
VG200	なし	あり	あり	あり	あり	あり
7x00 ファミリー	適用対象外	なし	なし	なし	なし	なし
ICS 7750	12.3.7T	あり	あり	あり	あり	あり
Catalyst 4000 Access Gateway Module（AGM）	なし	あり	あり	あり	あり	あり
827-4V[3]	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外	適用対象外

1. Cisco IOS Release 12.4(2)T は、BRI MGCP を NM-HDV2、NM-HD-XX、オンボード H-WIC スロットの各ハードウェアでサポートします。BRI MGCP は、NM-1V/2V ハードウェアで旧リリースの Cisco IOS によってもサポートされています。
2. AIM-VOICE-30 モジュールは、MGCP のサポートに Cisco IOS Release 12.2.13T を必要とします。プロトコルタイプ NTT は、MGCP BRI 未対応です。
3. このモデルは、製造中止になりました。

QSIG サポート

QSIG は、企業ネットワーク内で PBX 機器を柔軟に接続するために設計された、1 組の国際標準です。その他の機能の 1 つとして、QSIG には、さまざまなベンダー製の PBX 機器を相互接続するためのオープンな標準ベースの方法が用意されています。

ECMA QSIG は、PBX-to-PBX モードの H.323 ゲートウェイでサポートされています。H.323 ゲートウェイは、QSIG 情報要素に対する QSIG 機能の完全な透過性を備えています。基本的なコールのセットアップと終了は、表 4-9 に示されているように、H.323 QSIG ゲートウェイを使用してサポートされます。

表 4-9　H.323 ゲートウェイにおける QSIG サポート

プラットフォーム	メディア	必要な Cisco IOS ソフトウェア対応リリース
Cisco 3800	BRI および T1/E1 QSIG	12.3.11T
Cisco 2800 シリーズ	BRI および T1/E1 QSIG	12.3.8T4
Cisco 3700	T1/E1 QSIG	12.2.8T
Cisco AS5350 Cisco AS5400	T1/E1	12.2.2T
Cisco 5300	T1/E1	12.0.7T
Cisco 2600 および 3600 シリーズ	BRI および T1/E1 QSIG	12.1.2T
Cisco 1751 および 1760	BRI T1/E1 QSIG	12.2(8)YH 12.2(4)YB
Cisco 7200	T1/E1 QSIG	12.1.2T

Cisco IOS ゲートウェイにおける QSIG のサポートの詳細は、次の Web サイトを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121t/121t2/dt_qsig.htm#xtocid116542

Cisco Unified CallManager Release 3.3 より前のリリースでは、PBX が H.323 を介して QSIG を使用するゲートウェイに接続されている場合、PBX 上の電話機と、Cisco Unified CallManager に接続されている IP Phone との間でコールが行われるときにサポートされているのは、基本的な PRI 機能だけです。CLID（発呼回線 ID）と DID（ダイヤルイン方式）番号だけが含まれるこの基本機能は、Cisco Unified CallManager によってではなく、QSIG プロトコルを終端するゲートウェイによってサポートされています。

Cisco Unified CallManager が QSIG 機能をサポートするには、QSIG を Cisco Unified CallManager に直接バックホール（back-haul）する必要があります。このサポートは、Catalyst 6608、2600XM シリーズ、および 3640/60 シリーズなどの MGCP ゲートウェイと連携して、Cisco Unified CallManager Release 3.3 およびそれ以降で実装されています。

FAX とモデムのサポート

ここでは、Cisco Unified CallManager と Cisco 音声ゲートウェイで使用可能な FAX とモデムのサポートについて説明します。まず、Cisco 音声ゲートウェイ上での FAX とモデムのサポートの概要を説明した後、サポートされるプラットフォームとコンフィギュレーション ファイル例をリストします。

FAX パススルーと Cisco FAX リレーに対するゲートウェイ サポート

FAX over IP により、従来のアナログ FAX マシンと IP テレフォニー ネットワークとの相互運用性が可能になります。FAX イメージは、アナログ信号から変換され、パケット ネットワークを介してデジタル データとして伝送されます。

FAX データの元の形式は、デジタルです。しかし、従来の公衆網を経由して送信するために、データは変調され、アナログに変換されます。FAX over IP は、このアナログ変換のプロセスを逆転させて、パケット ネットワーク上でデジタル データを送信した後、受信側の FAX マシン用にそのデジタル データをアナログに再変換します。

大部分の Cisco 音声ゲートウェイは、現在、IP ネットワークを介して FAX トラフィックを送信する、次の 2 通りの方法をサポートします。

- Cisco FAX リレー：FAX リレー モードでは、ゲートウェイが T.30 または T.38 FAX 信号を終端します。
- FAX パススルー：FAX パススルー モードでは、ゲートウェイは、FAX コールを音声コールと区別しません。

FAX トラフィックの送信には、Cisco FAX リレー モードをお勧めします。しかし、特定のゲートウェイが Cisco FAX リレーをサポートしない場合、そのゲートウェイは FAX パススルーをサポートします。

ベスト プラクティス

Cisco 音声ゲートウェイで FAX サポートを最大限に実装するには、次の推奨事項とガイドラインが役立ちます。

- QoS を使用する場合は、できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失
  - 遅延
  - 遅延変動（ジッタ）

  Cisco Unified Communications ネットワークにおける QoS の実装についての詳細は、次の Web サイトで入手可能な『*Cisco Network Infrastructure Enterprise Quality of Service Design*』のガイドを参照してください。

  http://www.cisco.com/go/srnd
- FAX コールの完全性を確保するには、次のヒントが役立ちます。
  - コール アドミッション制御（CAC）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
  - モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。
- 最良のパフォーマンスを確保するために、起点と終端の両方のゲートウェイで、Cisco FAX リレーを有効にしていることを確認してください。2 つの Cisco IOS ゲートウェイの転送方法が異なる場合、ゲートウェイはネゴシエートして Cisco FAX リレーを使用します。

  Cisco FAX リレーをサポートしていない IOS 以外のゲートウェイは、Cisco Digital Access DT-24/DE-30+ だけです。このゲートウェイを Cisco IOS ゲートウェイに接続する場合は、FAX パススルー モードの使用を両方のゲートウェイに設定する必要があります。

- ネットワーク上の恒常的なパケット遅延が 1 秒を超えないこと、および遅延変動（ジッタ）が 240 ミリ秒を超えないことを確認してください。
- 不良パケットの着信頻度が高いネットワークで、パフォーマンスを改善するには、FAX マシンでエラー訂正モード（ECM）を無効にしてください。
- 大部分の FAX マシンは、現在の速度をスロー ダウンすることなく、0.4% ～ 0.6% の範囲内のパケット ドロップを受け入れるようです。しかし、0.8% ～ 1% の範囲内のパケット ドロップがあるネットワークでは、ECM を無効にする必要があります。
- 複数の FAX マシンで ECM を無効にするのを検討する前に、ゲートウェイ自体で ECM を無効にすることができます。しかし、パケット ドロップが発生する場合、FAX のイメージ品質が低下する恐れがあります。したがって、ECM を無効にするときには、長いコール所要時間やコールのドロップを検討する前に、イメージ品質を損なってもよいかどうかを十分に検討してください。また、パケットがドロップする原因を突き止めて、解決するために、ネットワークを監視し、評価することも必要です。

モデム パススルーに対するゲートウェイ サポート

一般に、音声ゲートウェイを使用して、IP ネットワーク上のモデム セッションをサポートするには、次の 2 通りのメカニズムがあります。

- モデム パススルー
- モデム リレー

現在、モデム リレーとモデム パススルーは、どちらも Cisco 音声ゲートウェイでサポートされています。

モデム パススルーとは、パルス符号変調（PCM）符号化パケットと G.711 コーデックを使用して、パケット ネットワークを通じてモデム信号を転送することです。モデム パススルーでは、ゲートウェイがモデム信号と音声信号を区別し、適切なアクションを取ることができなければなりません。ゲートウェイは、モデム信号を検出すると、次のサービスを無効にします。

- エコー キャンセレーション（EC）
- 音声アクティビティ検出（VAD）

モデム パススルー モードでは、ゲートウェイは、モデム コールを音声コールと区別しません。2 台のモデム間の通信は、「音声」コールを介してインバンドにそのまま伝送されます。モデム トラフィックは、QoS 対応の IP インフラストラクチャを介して透過的に伝送され、IP ネットワーク内でデータが復調されることはありません。

モデム コールは「音声」コールを介してインバンドに伝送されるという点で、モデムのアップスピード機能は、パススルーに似ています。違いは、アップスピード機能が使用されるときに、ゲートウェイがある程度まで、モデム コールを認識する点です。リレー メカニズムは使用されませんが、ゲートウェイは、モデム トーンを認識し、「音声」コーデックを G.711（アップスピード部分）に自動的に変更し、コールの期間中 VAD とエコー キャンセレーション（EC）を無効にします。

現在、このアップスピード機能は、Cisco IOS Release 12.1.3T による Cisco AS5300 以外の Cisco IOS プラットフォームではサポートされていません。Cisco 2600XM、3700、VG224、および Catalyst 4000 Access Gateway Module（AGM）プラットフォームの場合、モデムのアップスピード機能は、将来の Cisco IOS リリースでサポートされる予定です。これらのプラットフォームの場合、モデムのアップスピード機能が使用可能になるまで、ダイヤルピアで **no vad** を設定できます。

モデム アップスピード機能は、Catalyst 6000 ゲートウェイ モジュールでもサポートされています。

ベスト プラクティス

IP インフラストラクチャを介して転送されるモデム トラフィックの最適なパフォーマンスを確保するには、次の推奨ベスト プラクティスを守ってください。

- IP ネットワークで QoS（Quality of Service）が使用可能になっていること、および LAN、MAN、および WAN 環境で、QoS を提供するためのすべての推奨事項に従っていることを確認します。できる限り、次のパラメータが最小になる方法を採用してください。
  - パケット損失：FAX とモデムのトラフィックには、本質的に損失のない転送が必要です。パケットが 1 つでも損失すると、再送信が行われます。
  - 遅延
  - 遅延変動（ジッタ）

  詳細は、次の Web サイトで入手可能な『*Cisco Network Infrastructure Enterprise Quality of Service Design*』のガイドを参照してください。

  http://www.cisco.com/go/srnd
- コール アドミッション制御（CAC）を使用して、コールが規定の合計帯域幅限界を超えると、拒否されるようにします。
- モデムを使用するすべてのコールに、G.711 を使用します。ゲートウェイの 1 つがモデム リレーをサポートしていない場合、モデム パススルーがネゴシエートされます（G.711 のみ）。モデムが使用される場合、すべてのコールに G.711 を使用することが最善の方法です。
- IP ネットワークにモデムを接続して、IP ネットワークの問題のトラブルシューティングや診断をしないでください。この場合、IP インフラストラクチャを構成するデバイスのトラブルシューティングに使用されるモデムは、一般電話サービス（POTS）に接続する必要があります。
- 可能な場合、単一のシグナリング プロトコルとゲートウェイ ファミリーを使用して、相互運用性の問題を最小限にします。
- モデムと FAX のすべての専用ポートで、コール ウェイティングを使用不可にします。

V.90 サポート

現在、Cisco 機器は V.34 モデムのみをサポートします。V.90 モデムは既存のハードウェアで機能し、V.34 よりも高速ですが、V.90 の完全なサポートは保証できません。

サポートされるプラットフォームと機能

FAX とモデムの機能をサポートしている Cisco プラットフォームは、次のとおりです。

アナログ ゲートウェイ

Cisco IOS ゲートウェイ：

- 2600XM および 2691（FXS）
- 2800（FXS）
- 3725 および 3745（FXS）
- 3800（FXS）
- VG200（FXS）
- VG224
- 1751 および 1760
- コミュニケーション メディア モジュール（CMM）FXS カード

IOS 以外のゲートウェイ：

- VG248
- ATA 188

- 6624

デジタル ゲートウェイ

Cisco IOS ゲートウェイ：

- 2600XM および 2691
- 2800
- 3725 および 3745
- 3800
- VG200
- VG224
- 1751 および 1760
- 7200 および 7500
- AS5300、5350、5400、および 5850
- コミュニケーション メディア モジュール（CMM）

IOS 以外のゲートウェイ：

- 6608

（注） FAX とモデムのサポート テストは、Cisco IOS ゲートウェイ上の Cisco IOS Release 12.3(1)、および Cisco VG248 Analog Phone Gateway の Release 1.2.1 を使用して、上記のプラットフォーム上で実行されました。

プラットフォーム プロトコルのサポート

企業ソリューションで現在使用されている一般的なコール制御プロトコルには、H.323、Session Initiation Protocol（SIP）、メディア ゲートウェイ コントロール プロトコル（MGCP）、および Skinny Client Control Protocol（SCCP）があります。すべての Cisco 音声プラットフォームが、これらのプロトコル、または FAX とモデム機能をすべてサポートしているわけではないので、相互運用性の問題が発生します。また、Cisco 2600XM や Cisco 3700 シリーズなどの Cisco IOS ゲートウェイを、VG248 などの IOS 以外のゲートウェイと組み合せる場合は、さらに相互運用性の問題が発生します。ここでは、FAX、モデム、およびプロトコルの機能の相互運用性をサポートしているゲートウェイの組み合せをリストしています。

高いレベルで、Cisco IOS Release 12.3(1)（Cisco 6608 のロード 47 と Cisco 6624 のロード 41）、および VG248 の Release 1.2.1 は、Cisco FAX リレー、モデム パススルー、および音声機能の相互運用性をサポートします。Cisco IOS Release 12.2(11)T1 より前には、Cisco IOS と IOS 以外の音声プラットフォーム間では、音声と Cisco FAX リレーのみがサポートされていました。これは、パススルー Named Service Event（NSE）方式の非互換性により、モデム パススルーが相互運用できなかったからです。

ネットワークにおける一般的なプロトコルの組み合せの一部には、MGCP と H.323、SCCP と H.323、および SCCP と MGCP があります。一般的な音声ゲートウェイには、Cisco VG224、VG248、2600XM、2800、3700、3800、5300、および Catalyst 6000 が含まれます。

表 4-10 では、FAX とモデムの相互運用性を現在サポートしている、プロトコルの組み合せをリストしています。

表 4-10　FAX とモデムの機能がサポートされるコール制御プロトコルの各種組み合せ

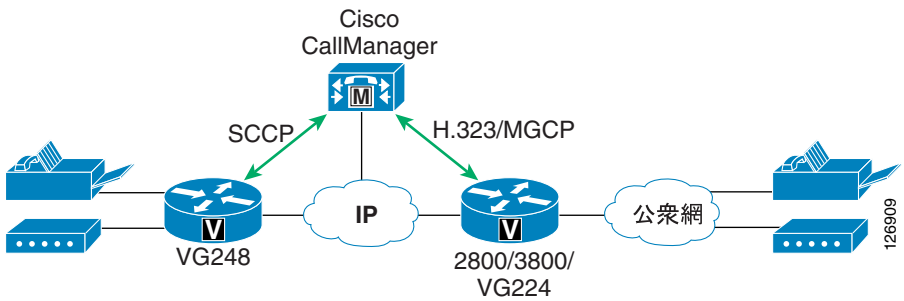
プロトコルの組み合せ	モデム リレー	モデム パススルー	T.38 FAX リレー	Cisco FAX リレー	FAX パススルー
MGCP を使用する Cisco Unified CallManager と H.323 または SIP を使用する Cisco Unified CallManager との組み合せ	あり	あり	なし	あり	あり
MGCP を使用する Cisco Unified CallManager と MGCP を使用する Cisco Unified CallManager との組み合せ	あり	あり	なし	あり	あり
SCCP と、H.323 または SIP を使用する Cisco Unified CallManager との組み合せ	あり	あり	なし	あり	あり
SCCP と MGCP を使用する Cisco Unified CallManager との組み合せ	あり	あり	なし	あり	あり
H.323 を使用する Cisco Unified CallManager と、H.323 または SIP との組み合せ	あり	あり	あり	あり	あり
SIP を使用する Cisco Unified CallManager と H.323 または SIP との組み合せ	あり	あり	あり	あり	あり

(注)　Cisco ATA 188、VG248、および Catalyst 6000 プラットフォームは現在、T.38 FAX リレーをサポートしていません。これらのプラットフォームが Cisco AS5350 または AS5400 ゲートウェイに接続される場合、FAX アプリケーションに対して FAX パススルーのみがサポートされます。

ゲートウェイの組み合せと機能の相互運用性

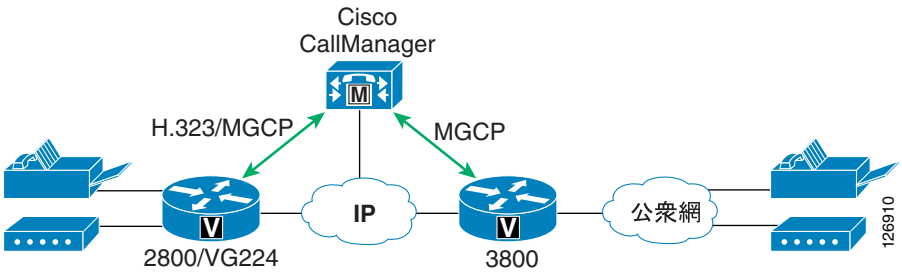
FAX とモデムの相互運用性について最も多い質問は、図 4-3 に示されているような、Cisco IOS ゲートウェイ（たとえば、Cisco 2800 や 3800）と IOS 以外のゲートウェイ（たとえば、Cisco VG248）との組み合せに関するものです。

図 4-3　Cisco IOS と IOS 以外のゲートウェイを組み合せる構成



FAX とモデムの相互運用性について次に多い質問は、図 4-4 に示されているような、Cisco IOS ゲートウェイのみを使用する構成に関するものです。

図 4-4　Cisco IOS ゲートウェイのみを使用する構成



どちらのシナリオの回答も、基本的に同じです。6608 上の Cisco IOS ロード 47、および VG248 上の Release 1.2.1 より前では、音声と Cisco FAX リレーのみがサポートされ、FAX パススルーとモデム パススルーは、NSE の非互換性によりサポートされません。6608 上の Cisco IOS ロード 47 以降、6624 上のロード 41 以降、および VG248 上の Release 1.2.1 は、この 3 つのプラットフォームはすべて、コール制御プロトコルに関係なく、音声、Cisco FAX リレー、およびモデム パススルー用に、Cisco IOS ゲートウェイと相互運用できます。NSE パススルー方式は、シグナリング パスではなく、ベアラ パスで動作するので、コール制御プロトコルとは関係しません。

類似ゲートウェイ間の機能サポート

表 4-11 では、同じ一般的なタイプのゲートウェイ間（たとえば、Cisco VG248 と 6608 間、2600XM と 3700 間、または 2600XM と AS5300 間）でサポートされる FAX とモデムの機能をリストします。両方のプラットフォームが所定の機能をサポートする限り、プラットフォームは相互運用します。

表 4-11　同じタイプのゲートウェイ上での FAX とモデム機能のサポート

ゲートウェイ タイプ	FAX パススルー	Cisco FAX リレー	T.38 FAX リレー	モデム パススルー	モデム リレー
Cisco IOS ゲートウェイ	サポートする	サポートする（5350 と 5400 を除く）	サポートする	サポートする	サポートする（NM-HDV のみ）
IOS 以外のゲートウェイ	サポートする	サポートする（ATA 188 を除く）	適用対象外	サポートする（ATA 188 を除く）	適用対象外

ゲートウェイ設定例

ここでは、FAX とモデムをサポートするためのゲートウェイ設定例を示します。

Cisco IOS ゲートウェイの設定

H.323

```
!
! Cisco fax relay is ON by default
!(except for 5350/5400, where Cisco fax relay is not supported)
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
!
```

MGCP

```
!
ccm-manager mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

Cisco VG248 の設定

```
-----------------------------------------------------
|               Cisco VG248 (VGC10d8002407)          |
----- -----------------------------------------------
     | Advanced settings                             |
     |-----------------------------------------------|
     | Allow last good configuration (enabled)       |
     | SRST policy                   (disabled)      |
     | SRST provider                 ()              |
     | Call preservation             (enabled: no timeout) |
     | Media receive timeout         (disabled)      |
     | Busy out off hook ports       (disabled)      |
     | DTMF tone dur ------------------------  100ms)      |
     | Echo cancelli| Passthrough signalling |e: use DSP)  |
     | Passthrough s|------------------------|)          |
     | Hook flash ti| legacy                 | default>)   |
     | Hook flash re| IOS mode               |             |
     | Fax relay max ------------------------  14400 bps)  |
     | Fax relay playout delay       (default: 300)  |
      -----------------------------------------------
        ---------------------------------------------

-----------------------------------------------------
|               Cisco VG248 (VGC10d8002407)          |
----- -----------------------------------------------
     | Advanced settings                             |
     |-----------------------------------------------|
     | Allow last good configuration (enabled)       |
     | SRST policy                   (disabled)      |
     | SRST provider                 ()              |
     | Call preservation             (enabled: no timeout) |
     | Media receive timeout         (disabled)      |
     | Busy out off hook ports       (disabled)      |
     | DTMF tone duration            (default: 100ms)      |
     | Echo cancelling policy        (alternate: use DSP)  |
     | Passthrough signalling        (IOS mode)      |
     | Hook flash timer              (<country default>)   |
     | Hook flash reject period      (none)          |
     | Fax relay maximum speed       (default: 14400 bps)  |
     | Fax relay playout delay       (default: 300)  |
      -----------------------------------------------
        ---------------------------------------------
```

Cisco IOS ゲートウェイ用の Cisco Unified CallManager 設定

Cisco IOS ゲートウェイ（たとえば、Cisco 6608 や 6624）用に Cisco Unified CallManager を設定するには、Cisco CallManager で次の手順を実行します。

ステップ 1　Cisco Unified CallManager Administration で、**Device** > **Gateway** の順に選択して、**Find/List Gateways** ウィンドウを表示します。

ステップ 2　変更するゲートウェイを検索するか（すでに存在する場合）、または **Add a New Gateway** をクリックして新しいゲートウェイを Cisco Unified CallManager データベースに追加します。

ステップ 3　適切なタイプのゲートウェイ（たとえば、Cisco Catalyst 6000）を選択した後、**FAX Relay Enable** をクリックして Cisco FAX リレーを使用可能にします。

ステップ 4　**NSE Type** ドロップダウン リスト ボックスを使用して、モデム パススルー用に **IOS Gateways** を選択します。

ステップ 5　**Update** をクリックして変更内容を保存します。

ステップ 6　ゲートウェイをリセットして変更内容を適用します。

この設定は、Cisco VG248、6608、6624、および IOS ゲートウェイ間での、音声、Cisco FAX リレー、およびモデム パススルーをサポートします。ただし、Cisco FAX リレーをサポートしない Cisco AS5350 および AS5400 ゲートウェイを除きます。また、この設定は、パススルー モードの V.34 モデム接続もサポートします。V.90 モデム接続は保証されていませんが、ネットワーク ジッタの量とクロック同期によっては可能です。

FAX とモデム パススルー用のクロック ソーシング

FAX とモデム パススルーを正常に機能させるには、クロック信号が重要な役割を果たします。ゲートウェイのクロックは、Stratum クロッキングが提供される公衆網クロックと同期させる必要があります。このクロック同期がないと、FAX および（特に）モデムのパススルーは機能しません。クロックを正しく同期させるには、T1 コントローラで次の設定を入力してください（この例では、T1 コントローラは、公衆網に接続している音声ゲートウェイです）。

```
!
controller T1 0
 framing esf
 linecode b8zs
 clock source line
 channel-group 1 timeslots 1-24 speed 64
 !
```

また、公衆網に接続している他のすべてのインターフェイスでも、この設定を入力してください。

T.38 FAX リレー

T.38 FAX リレーは、Cisco ATA 188、VG248、6608、および 6624 ゲートウェイではサポートされていませんが、Cisco 2800 および 3800 シリーズ ルータなど、大部分の高性能 Cisco IOS 音声プラットフォームではサポートされています。H.323 または SIP モードで動作する場合、これらのプラットフォームは MGCP をサポートしません。

T.38 FAX リレーは、次のいずれかの方法で設定できます。

- Named Service Event（NSE）を使用して制御されるゲートウェイ（P.4-31）
- H.245 または SDP（Session Description Protocol）による機能交換を使用して制御されるゲートウェイ（P.4-31）
- H.323 Annex D を使用したコール エージェント制御の T.38（P.4-33）

Named Service Event（NSE）を使用して制御されるゲートウェイ

この設定では、次の Cisco IOS ゲートウェイ設定例に示されているように、ダイヤルピア上の静的 T.38 設定を使用します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
 fax protocol t38
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

H.245 または SDP（Session Description Protocol）による機能交換を使用して制御されるゲートウェイ

この T.38 FAX リレー設定方法には、次の特性が適用されます。

- T.38 機能はゲートウェイ間で交換されます。FAX トーンの検出後に T.38 FAX リレーに切り替わることを起点側のゲートウェイに知らせるために、Named Service Event（NSE）メッセージが、RTP ストリーム上で終端側のゲートウェイから送信されます。この NSE メッセージは RTP ストリーム上で送信されるので、コール制御信号に対しては透過されます。
- Cisco Unified CallManager は、MGCP ではこの機能交換をサポートできません。したがって、T.38 機能が交換されない場合であっても、設定コマンドを使用して強制的に T.38 FAX リレーに切り替える必要があります。
- 選択可能なフォールバック方法は、次の 3 通りです。
  - Cisco FAX リレー（デフォルト）
  - FAX パススルー
  - なし

次に、このタイプの設定例を示します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to Cisco fax relay when
! T.38 fax negotiation fails. This is the default case.
 fax protocol t38 fallback cisco
!
dial-peer voice 1001 voip
 destination-pattern 2T
 session target ipv4:10.10.10.2
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay and fall back to fax passthrough when
! T.38 fax negotiation fails.
fax protocol t38 nse fallback pass-through
!
dial-peer voice 1002 voip
 destination-pattern 3T
 session target ipv4:10.10.10.3
 modem passthrough mode nse codec g711ulaw
!
! This CLI is needed when talking to MGCP endpoint where CA/GK
! doesn't support T.38 fax relay such as CCM.
 fax protocol t38 nse force fallback none
!
!
```

MGCP

```
!
ccm-manage mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
mgcp modem passthrough voip mode nse
no mgcp fax t38 inhibit
!
! This CLI is needed when CA doesn't support T.38 fax relay
mgcp fax t38 gateway force
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
!
```

Cisco VG248 および 6608 または 6624 を使用するトポロジでは、次の Cisco IOS コマンドを使用してください。

```
fax protocol t38 [nse [force]] fallback [cisco | none]
modem passthrough nse codec {g711ulaw|g711alaw}
```

これらの 2 つのコマンドにより、Cisco IOS ゲートウェイは、T.38 FAX リレーとモデム パススルーを実行するために他の Cisco IOS ゲートウェイと相互運用するだけでなく、Cisco FAX リレーとモデム パススルーを実行するために VG248 とも相互運用できるようになります。

H.323 Annex D を使用したコール エージェント制御の T.38

この T.38 FAX リレー設定方法には、次の特性が適用されます。

- コール制御エージェント（たとえば、Cisco Unified CallManager）が T.38 FAX リレーを制御し、ゲートウェイはパッシブ モードで動作します。
- ゲートウェイ間で NSE メッセージは送信されません。
- このタイプの設定では、T.38 FAX リレーは、コール制御プロトコルに対して透過的ではありません。コール エージェントは、H.323 と SIP 間のプロトコル変換を実行します。
- この方法により、T.38 FAX リレーは、Cisco IOS Release 12.3(1) で設定できます。Cisco BTS 10200 Softswitch もこの方法をサポートします。
- Cisco Voice Media Streaming Application は T.38 をサポートしませんが、Cisco IOS メディア ターミネーション ポイント（MTP）は T.38 をサポートします。したがって、メディア リソース グループ リスト（MRGL）の中で Cisco IOS MTP に正しい優先順位付けが行われるようにしてください。

次に、このタイプの設定例を示します。

H.323

```
!
dial-peer voice 1000 voip
 destination-pattern 1T
 session target ipv4:10.10.10.1
 modem passthrough mode nse codec g711ulaw
!
! To enable T.38 fax relay.
 fax protocol t38
!
!
```

MGCP

```
!
ccm-manager mgcp
mgcp
mgcp call-agent 10.10.10.1 service-type mgcp version 0.1
!
! T.38 fax relay is ON by default. HOWEVER, Unified CM doesn't
! support CA controlled mode. This is the configuration for
! talking to BTS.
!
dial-peer voice 100 pots
 application mgcpapp
 port 1/0/0
!
```

ビデオ テレフォニー用のゲートウェイ

シスコでは、音声ゲートウェイ機能を、スタンドアロン デバイス、Cisco IOS ルータに組み込むモジュール、Cisco Catalyst イーサネット スイッチに組み込むライン カードなど、さまざまな形で提供しています。これらのゲートウェイは、複数の VoIP プロトコル（H.323、MGCP、SIP、SCCP など）、複数のポート インターフェイス タイプ（FXS、FXO、E&M、T1/E1-CAS、T1/E1-PRI、ISDN BRI など）、および無数の最新 VoIP 機能をサポートしています。また、これらのゲートウェイでは、管理用およびトラブルシューティング用のインターフェイス セットを豊富に使用できます。ただし、Cisco 音声ゲートウェイは、H.320 プロトコル スイートまたは H.26x ファミリのビデオ コーデックをサポートしていないので、ビデオ コールに使用することはできません。このため、シスコでは、別のファミリのビデオ対応ゲートウェイを IP/VC 3500 シリーズのポートフォリオで提供しています。

IP/VC ゲートウェイはビデオ コール用として優れていますが、Cisco 音声ゲートウェイが提供するすべての機能をサポートしているわけではありません。IP/VC ゲートウェイには、次の特性があります。

- H.323 と H.320 のみをサポートします。
- スタンドアロン デバイスです。Cisco IOS ルータまたは Cisco Catalyst スイッチに統合することはできません。
- T1/E1-PRI、ISDN BRI、V.35 の各インターフェイス タイプのみをサポートします。
- G.711、G.728、および G.722 のみをサポートし、G.729 オーディオをサポートしません。
- H.245 Empty Capabilities Set（ECS）をサポートします。
- Cisco 音声ゲートウェイに固有の、多数の管理機能とトラブルシューティング機能をサポートしません。

このように製品間の違いがあるため、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、Cisco 音声ゲートウェイの代わりとしては推奨できません。IP テレフォニーのユーザが通信環境にビデオを追加するには、両方のタイプのゲートウェイを購入して、すべての音声コールに Cisco 音声ゲートウェイを使用し、Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイをビデオ コールのみに使用する必要があります。また、導入する Cisco IOS ゲートウェイのモデルに応じて、公衆網サービス プロバイダーから音声回線とビデオ回線を別々に調達しなければならない場合もあります。たとえば、セントラル オフィス（CO）からの T1-PRI 回線を 1 つだけ設け、その回線を音声コールとビデオ コールの両方に共有することはできません。以前の世代の H.320 ビデオ会議では、そのような回線が多くの場合、図 4-5 に示すように共有されていました。IP ビデオ テレフォニーを使用する場合は、図 4-6 に示すように、音声ゲートウェイとビデオ ゲートウェイを別々に置く必要があるため、公衆網回線を共有できなくなりました。

図 4-5　音声と H.320 ビデオ会議に公衆網回線を共有する従来型の PBX

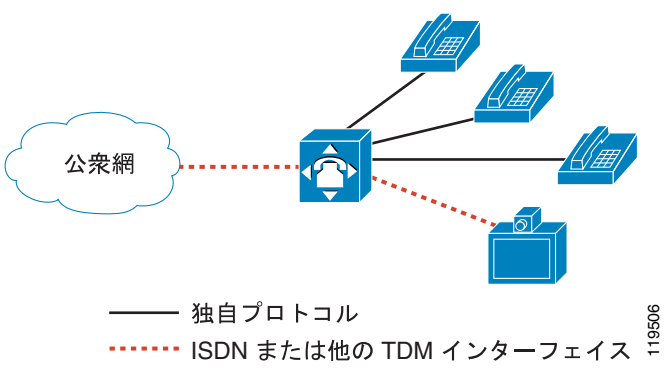
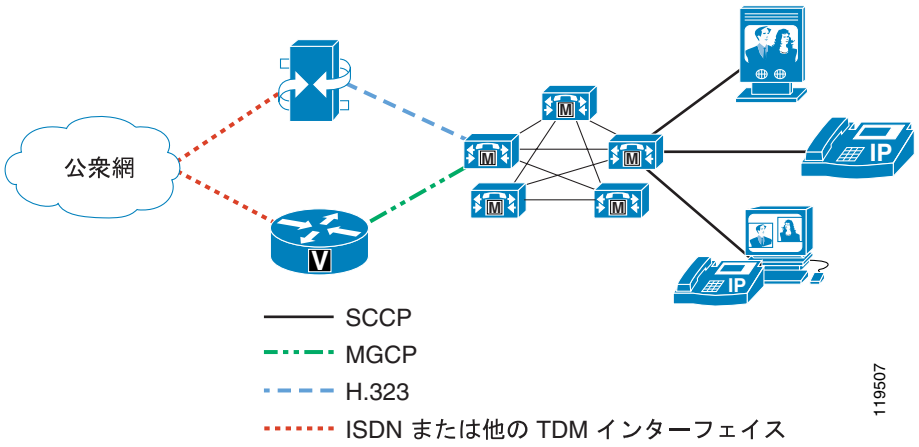


図 4-6　音声と IP ビデオ テレフォニーに別々の公衆網回線を使用する Cisco Unified CallManager システム



音声ゲートウェイとビデオ ゲートウェイを別々にする場合は、ルート プランも着信コールと発信コールの両方について、別々にする必要があります。着信コールの場合、Direct Inward Dial（DID; ダイヤルイン）内線を 1 つしか持たないユーザが音声コールとビデオ コールの両方を受信することはできません。通常、各ユーザは、あらかじめ音声コール用の DID を持っています。そのシナリオにビデオを導入する場合は、何か別の方法でユーザにダイヤルする必要があります。たとえば、第 2 の DID 番号を使用する方法や、ビデオ ゲートウェイのメイン番号にダイヤルし、音声自動応答装置（IVR）から促されてユーザのビデオ内線に入るなどの方法があります。発信コールの場合は、単一の公衆網アクセス コードを音声コールとビデオ コールの両方に使用することができません。通常、ユーザはすでに音声用の既知のアクセス コード（多くの米国企業における 9 など）を持っていますが、そのシナリオにビデオを導入した場合、ビデオ コールを発信するユーザは何か別のアクセス コードをダイヤルする必要があります。

2 つのタイプのゲートウェイを導入するための、もう 1 つの考慮事項は、それらのゲートウェイの配置です。通常、企業は多数の公衆網ゲートウェイ リソースを中央サイト（複数の場合もある）に集約し、それぞれの支店も、いくつかのローカル ゲートウェイ リソースを持っています。たとえば、Cisco Catalyst 6500 ゲートウェイを中央サイトに配置し、そのゲートウェイに複数の T1/E1 回線を接続する一方で、各支店に Cisco Integrated Services Router（ISR）と、ローカル CO へのアナログまたはデジタルのトランクが配備されている場合があります。このシナリオにビデオを導入するユーザは、ビデオに必要な公衆網回線の数と、ビデオ ゲートウェイの配置場所も決定する必要があります。たとえば、少数の IP/VC 3500 シリーズ ゲートウェイのみを中央サイトに配置するのか、それとも各支店にもゲートウェイを配置するのか、といったことです。

最後に、トール バイパスを設けるためには IP ネットワーク内でコールをどのようにリモート ゲートウェイへルーティングするのか、および IP ネットワークが使用不能になったり、コールを完了できるだけの帯域幅がない場合に、公衆網上でコールをどのように再ルーティングするのかを考慮してください。具体的には、ビデオ コール用の自動代替ルーティング（AAR）を起動するのか、といったことです。

公衆網からの着信コールのルーティング

公衆網からの着信コールをルーティングするには、次のいずれかの方法を使用します。

- Cisco Unified CallManager クラスタ内にある各ビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。この方法では、外部の（公衆網）発信者はビデオを有効にするために、正しい番号をダイヤルする必要があります。
- ビデオ コールの場合は、外部の発信者にビデオ ゲートウェイのメイン番号をダイヤルしてもらいます。Cisco Unified Videoconferencing ゲートウェイは統合 IVR を提供し、発信者に相手側の内線番号の入力を求めます。次に、Cisco Unified CallManager は、それがビデオ コールであることを認識し、宛先デバイスを呼び出します。この方法では、発信者はそれぞれの着信側ごとに 2 つの異なる DID 番号を覚える必要はありませんが、着信ビデオ コールをダイヤルするという余分な手順が増えます。

（注） 外部のビデオ エンドポイントは、IVR プロンプトに着信側の内線番号を入力するために、DTMF をサポートしている必要があります。

次の例は、2 番目の方法を示しています。

ユーザの Cisco Unified IP Phone 7960 は、Cisco Unified Video Advantage を実行している PC に接続されています。IP Phone の内線番号は 51212 で、完全修飾 DID 番号は 1-408-555-1212 です。DID 番号をダイヤルするだけで、音声専用コールの公衆網からそのユーザに到達できます。CO は、Cisco 音声ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その DID 番号にコールを送信します。ゲートウェイでコールが受信されると、Cisco Unified CallManager はゲートウェイが音声専用であることを認識し、そのコール用に 1 つの音声チャネルのみのネゴシエーションを行います。逆に、公衆網からビデオ コールのためにそのユーザに到達するには、ビデオ ゲートウェイのメイン番号をダイヤルした後、ユーザの内線番号を入力する必要があります。たとえば、1-408-555-1000 をダイヤルするとします。CO は、Cisco Unified Videoconferencing 3500 シリーズ ビデオ ゲートウェイに接続した T1-PRI 回線（複数の場合もある）を通じて、その番号にコールを送信します。ゲートウェイでコールが受信されると、IVR プロンプトが発信元に、到達すべき相手の内線番号の入力を求めます。発信者が DTMF トーンで内線番号を入力すると、Cisco Unified CallManager はゲートウェイにビデオ機能があることを認識し、そのコール用に音声とビデオの両方のチャネルをネゴシエートします。

ゲートウェイの番号操作

Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、公衆網から受信したコールの番号を操作できません。Q.931 Called Party Number フィールドで渡されたものと正確に同じ数の番号を受け取り、それらすべてを Cisco Unified CallManager に送信します。したがって、Cisco Unified CallManager は番号を操作して、宛先デバイスの電話番号（DN）と照合する必要があります。たとえば、CO スイッチからゲートウェイへの回線が 10 桁を渡すように設定されていて、着信側の内線番号が 5 桁しかない場合、Cisco Unified CallManager は、一致する DN を検索する前に、先頭の 5 桁を削除する必要があります。この番号操作は、次のいずれかの方法で実装できます。

- IP/VC ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランクの、Significant Digits フィールドを設定します。

  この方法では、Cisco Unified CallManager に、着信番号の下位 N 桁だけに注目するよう指示できます。たとえば、Significant Digits を 5 に設定すると、Cisco Unified CallManager は着信番号の最後の 5 桁以外を無視します。これは最も簡単な方法ですが、そのゲートウェイから受信したすべてのコールに影響を及ぼします。したがって、可変長の内線番号がある場合、この方法は推奨できません。
- 変換パターンを設定し、それを IP/VC ゲートウェイからの着信コールを伝達する H.323 ゲートウェイ デバイスまたは H.225 ゲートキーパー制御トランクのコーリング サーチ スペースに格納します。

この方法では、Cisco Unified CallManager は受信した完全な桁数でコールを照合し、着信番号を修正してから、得られた変更後の番号に対して番号分析を続行できます。この方法は前の方法に比べてわずかながら複雑ですが、柔軟性があり、コールの照合と修正をきめ細かく行うことができます。

公衆網への発信コールのルーティング

発信コールを公衆網へルーティングするには、次のいずれかの方法を使用します。

- 音声コールとビデオ コールに異なるアクセス コード（異なるルート パターン）を割り当てます。たとえば、ユーザが 9 の後にコール先の公衆網電話番号をダイヤルすると、それがコールを音声ゲートウェイに送るルート パターンと一致します。同様に、数字の 8 を、ビデオ ゲートウェイにコールを渡すルート パターンとして使用することもできます。
- Cisco Unified CallManager クラスタ内にある各ビデオ対応デバイスごとに、少なくとも 2 つの異なる電話番号を割り当て、1 つの回線を音声用、もう 1 つをビデオ用とします。その後、2 つの回線に異なるコーリング サーチ スペースを指定します。ユーザが第 1 の回線上でアクセス コード（たとえば 9）をダイヤルすると音声ゲートウェイにつながり、同じアクセス コードを第 2 の回線上でダイヤルするとビデオ ゲートウェイにつながります。この方法では、ユーザが 2 つの異なるアクセス コードを覚える必要がありませんが、コールの発信時に電話機で正しい回線を押す必要があります。

ゲートウェイ サービス プレフィックス

Cisco Unified Videoconferencing ゲートウェイは、発信コールの速度を定義するためにサービス プレフィックスを使用します。ゲートウェイでサービス プレフィックスを設定するときは、次のいずれかの速度を選択する必要があります。

- Voice-only
- 128 Kbps
- 256 Kbps
- 384 Kbps
- 768 Kbps
- Auto（動的に決定され、128 kbps ～ 768 kbps の範囲の任意のコール速度をサポート）

（注） 上記の各速度は、64 kbps の倍数を表します。56 kbps のダイヤリング用として、サービス プレフィックスの設定ページには、各チャネルを 56 kbps に制限するチェックボックスがあります。したがって、制限モードを有効にした 128 kbps サービスは 112 kbps サービスになり、制限モードを有効にした 384 kbps サービスは 336 kbps になり、その他も同様です。

IP エンドポイントから公衆網へ向かうコールは、ゲートウェイがそのコールにどのサービスを使用するかを決定できるように、着信番号の先頭にサービス プレフィックスを含んでいる必要があります。オプションとして、番号の先頭にサービス プレフィックスを含んでいないコールに使用する、デフォルト プレフィックスを設定できます。この方法は、非常に複雑になる可能性があります。ユーザは、求めるコール速度を得るためにダイヤルすべきプレフィックスを覚えておく必要があるからです。また、管理者は、Cisco Unified CallManager で複数の（速度ごとに 1 つずつ）ルート パターンを設定する必要があります。ただし、Auto 速度を使用するとその手間を最小にできます。コールの大多数が 1 チャネルあたり 64 kbps（たとえば、128 kbps、384 kbps、512 kbps、768 kbps など）を使用して行われる場合には、Auto サービスを使用できます。その場合、1 チャネルあたり 56 kbps（たとえば、112 kbps、336 kbps など）のコールを行うまれなケースに備えて、1 つだけ別のサービスを作成すれば済みます。

ゲートウェイは、# をダイヤル末尾の文字として認識するので、サービス プレフィックスの中に必ず # 文字を使用することをお勧めします。この文字をサービス プレフィックスに入れておくと、ゲートウェイのメイン番号をダイヤルして IVR に接続してからオフネット番号にダイヤルするといった料金詐欺にゲートウェイが使用されることを防止できます。# は、サービス プレフィックスの先頭（推奨）と末尾どちらでもかまいません。たとえば、ビデオ コールで公衆網に到達するためのアクセス コードが 8 であれば、サービス プレフィックスを #8 または 8# として設定することをお勧めします。あるいは、上記のように 2 つのサービス プレフィックスを使用する場合は、Auto の 64 kbps サービスに #80 を使用し、Auto の 56 kbps サービスに #81 を使用するという方法もあります。

サービス プレフィックスを使用することの欠点は、IP/VC ゲートウェイにコールを送信するときに、Cisco Unified CallManager で着信番号の前にサービス プレフィックスを付加する必要があることです。ユーザに # をダイヤルさせるのはあまり使いやすくないので、ダイヤルされた番号の前に Cisco Unified CallManager が # を付加するように設定することをお勧めします。たとえば、公衆網にビデオ コールをダイヤルするアクセス コードが 8 の場合、Cisco Unified CallManager でルート パターンを 8.@ として設定し、ルート パターン設定の中で、そのルート パターンがダイヤルされたときは必ず前に #8 を付加するように、着信番号変換規則を設定します。あるいは、上記のようにサービス プレフィックスを 2 つ使用する場合は、80.@ を Auto 64 kbps サービス（着信番号の前に # を付ける）に使用し、81.@ を Auto 56 kbps サービス（着信番号の前に # を付ける）に使用するという方法もあります。

自動代替ルーティング（AAR）

IP ネットワークにコールを処理できるだけの帯域幅がない場合、Cisco Unified CallManager はコール アドミッション制御メカニズムを使用して、コールの処理方法を決定します。P.15-1 の「IP ビデオ テレフォニー」の説明のように、Cisco Unified CallManager は設定に従って、次のいずれかの処理を実行します。

- コールに失敗し、発信側に対してビジー トーンを再生し、発信側の画面に Bandwidth Unavailable メッセージを表示します。
- ビデオ コールを音声専用コールとして再試行します。
- 自動代替ルーティング（AAR）を使用し、公衆網ゲートウェイなどの代替パス上でコールを再ルーティングします。

最初の 2 つのオプションについては、P.15-1 の「IP ビデオ テレフォニー」の章に説明があります。ここでは、AAR オプションについて説明します。

音声コールまたはビデオ コールに AAR を使用できるようにするには、発信側デバイスと着信側デバイスを AAR グループのメンバーとして設定し、着信側デバイスに外部電話番号マスクを設定する必要があります。外部電話番号マスクによって、ユーザの内線用の完全修飾 E.164 アドレスが指定されます。また、AAR グループによって、コールが公衆網上で正しくルーティングされるために、着信側デバイスの外部電話番号マスクの前に付加すべき数字が示されます。

たとえば、ユーザ A が San Jose AAR グループに属し、ユーザ B が San Francisco AAR グループに属しているとします。ユーザ B の内線番号は 51212 で、外部電話番号マスクは 6505551212 です。AAR グループは、San Jose と San Francisco の AAR グループ間のコールに対して、番号の前に 91 を付加するよう設定されています。この場合、ユーザ A が 51212 をダイヤルし、2 つのサイト間の IP WAN 上にそのコールを処理できるだけの帯域幅がない場合、Cisco Unified CallManager はユーザ B の外部電話番号マスクである 6505551212 を選択し、その前に 91 を付加して 916505551212 への新規コールを生成し、ユーザ A 用の AAR コーリング サーチ スペースを使用します。

ビデオ コールにも同じロジックが適用されますが、プロセスに 1 つだけ手順が追加されます。ビデオ対応デバイスに対して、Retry Video Call as Audio というフィールドが存在します。P.15-1 の「IP ビデオ テレフォニー」の章で説明するように、このオプションを有効（オン）にした場合、

Cisco Unified CallManager は AAR を実行しないで、同じコール（つまり、51212 へのコール）を音声専用コールとして再試行します。このオプションを無効（オフ）にした場合、Cisco Unified CallManager は AAR を実行します。Cisco Unified CallManager のデフォルトでは、すべてのビデオ対応デバイスで Retry Video Call as Audio オプションが有効（オン）になります。したがって、ビデオ コールで AAR を使用できるようにするには、Retry Video Call as Audio オプションを無効（オフ）にする必要があります。また、ロケーション間でリソース予約プロトコル（RSVP）に基づいたコール アドミッション制御ポリシーが使用されている場合は、RSVP ポリシーを音声ストリームとビデオ ストリームの両方について Mandatory に設定する必要があります。

さらに、Cisco Unified CallManager は、着信側デバイスだけを見て Retry Video Call as Audio オプションが有効か無効かを判断します。したがって、上記のシナリオで AAR プロセスが実行されるためには、ユーザ B の電話機で Retry Video Call as Audio オプションが無効にされている必要があります。

最後に、デバイスは 1 つの AAR グループだけに所属できます。AAR グループによって、どの数字を前に付加するかが決定されるため、再ルーティングされたコールにどのゲートウェイが使用されるかにも影響があります。前項で述べたように、公衆網への発信コール ルーティングの設定に何を選択したかに応じて、AAR によって再ルーティングされるビデオ コールは、ビデオ ゲートウェイでなく音声ゲートウェイに送られる可能性もあります。したがって、AAR グループと AAR コーリング サーチ スペースの構築は入念に行い、必ず正しい数字が付加され、AAR に正しいコーリング サーチ スペースが使用されるようにしてください。

こうした考慮事項により、大規模な企業環境での AAR の設定がかなり複雑になる可能性がありますが、エンドポイントのタイプが 2 つのどちらかに限定されている場合（IP Phone が音声専用コール用で、Tandberg T-1000 などのシステムがビデオ コール専用など）には AAR の実装が容易です。エンドポイントが音声とビデオの両方のコールに対応している場合（Cisco Unified Video Advantage または Cisco IP Video Phone 7985G など）は、AAR の設定が非常に複雑になることがあります。したがって、音声とビデオのエンドポイントが混在する大企業では、ユーザごとに AAR の重要性をよく考え、専用のビデオ会議室や経営幹部用ビデオ システムなど、一部のビデオ デバイスだけに AAR を使用してください。表 4-12 に、さまざまなデバイス タイプで AAR を使用するのが適切なシナリオのリストを示します。

表 4-12　デバイス タイプ別の AAR 使用条件

デバイス タイプ	デバイスを使用したコールの宛先	AAR の必要性	備考
IP Phone	他の IP Phone およびビデオ対応デバイス	あり	ビデオ対応デバイスにコールするときでも、発信元デバイスが音声専用なので、コールを音声ゲートウェイにルーティングするように AAR を設定できます。
Cisco Unified Video Advantage の搭載された IP Phone、または Cisco IP Video Phone 7985G	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。
Sony 社製または Tandberg 社製の SCCP エンドポイント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。

表 4-12　デバイス タイプ別の AAR 使用条件（続き）

デバイス タイプ	デバイスを使用したコールの宛先	AAR の必要性	備考
H.323 または SIP クライアント	他のビデオ対応デバイスのみ	あり	デバイスは必ずビデオ コールに使用されるので、AAR グループを設定できます。
	IP Phone およびその他のビデオ対応デバイス	なし	音声専用コールではビデオ コールと異なるルーティングを行うように AAR グループを設定するのは困難です。

最低料金選択機能

Least-Cost Routing（LCR; 最低料金選択機能）と Tail-End Hop-Off（TEHO; テールエンド ホップオフ）は、VoIP ネットワークでは非常によく知られており、ビデオ コールにも利用できます。一般的にどちらの用語も、長距離電話番号へのコールが IP ネットワークを通じて宛先に最も近いゲートウェイにルーティングされ、通話料金が安くなるような、コール ルーティング規則の設定方法を指しています。Cisco Unified CallManager Release 4.1 の場合、LCR は基本的に TEHO と同じ意味です。Cisco Unified CallManager は、次に示すような豊富な番号分析機能と番号操作機能を使用して、この機能をサポートします。

- パーティションとコーリング サーチ スペース
- トランスレーション パターン
- ルート パターンとルート フィルタ
- ルート リストとルート グループ

LCR をビデオ コール用に設定するのは、音声コールの場合よりも少し複雑で、その理由は次のとおりです。

- この章ですでに述べたように、ビデオ コールには独自の専用ゲートウェイが必要です。
- ビデオ コールには、音声コールをはるかに上回る帯域幅が必要です。

専用ゲートウェイに関しては、LCR をビデオ コールに使用するかどうかを決めるための基礎となるロジックは、P.4-38 の「自動代替ルーティング（AAR）」の項で説明したロジックとほとんど同じです。音声とビデオ用にさまざまなタイプのゲートウェイが必要になるため、LCR で音声コールを 1 つのゲートウェイに送り、ビデオ コールを別のゲートウェイに送るために必要なすべてのパーティション、コーリング サーチ スペース、変換パターン、ルート パターン、ルート フィルタ、ルート リスト、およびルート グループを設定するのは、かなり複雑な作業になる可能性があります。

帯域幅の要件に関しては、LCR を使用するかどうかは、特定のロケーションとの間を結ぶビデオ コールの LCR をサポートできるだけの帯域幅が、使用している IP ネットワークにあるかどうかで決まります。現在の帯域幅が十分でない場合は、IP ネットワークをアップグレードしてビデオ コール用の空きを作ったり、ローカル ゲートウェイを導入して公衆網上でコールをルーティングしたりするためのコストと、ビデオ コールの利点を比較する必要があります。たとえば、ある中央サイトに 1.544 Mbps の T1 フレーム リレー回線を介して支店が接続されているとします。その支店内には、20 人のビデオ機能を持つユーザがいます。1.544 Mbps の T1 回線は、最大でほぼ 4 つの 384 kbps ビデオ コールを処理できます。この場合、中央サイトまでビデオ コールをルーティングして、通話料金を節約することに意味があるかどうかが問題です。サポートするコールの数に応じて、1.544 Mbps の T1 回線をもっと高速のものにアップグレードしなければならない場合もあります。ビデオには、そうしたアップグレードに要する毎月の追加料金に見合うだけの重要性があるのでしょうか。もしないのなら、その支店に IP/VC ビデオ ゲートウェイを導入すると、LCR に煩わされずに済みます。しかし、各支店へのローカル IP/VC ゲートウェイの配置も安価には行えないため、最終的には、ビデオから公衆網へのコールがビジネスにとってどれほど重要であるかを判断しなければなりません。ビデオが重要でないなら、帯域幅をアップグレードしたりビデオ ゲートウェイを購入

したりするよりも、Retry Video Call as Audio 機能を使用し、使用可能な帯域幅を超過した場合にビデオ コールを音声専用コールとして再ルーティングした方がよいこともあります。コールが音声専用までダウングレードされると、LCR を実行するためのローカル ゲートウェイ リソースと帯域幅は、もっと手ごろな価格で設定しやすいものになります。

ISDN B チャネル バインディング、ロールオーバー、およびビジーアウト

H.320 ビデオは、複数の ISDN チャネルをまとめて使用しすることで、フルモーション ビデオの受け渡しに必要な速度を実現します。このボンディング メカニズムの問題の 1 つは、着信 ISDN ビデオ コールを受信した時点でゲートウェイにはそのコールに必要なチャネル数がわからず、コールを受け入れて発信元デバイスから必要な追加チャネル数を指示されて、初めてそれがわかることです。その要求を満たせるだけの B チャネルがないと、コールは切断されます。したがって、そのような状況が発生する可能性を最小にするよう、慎重なトラフィック エンジニアリングが必要です。基本的に、次に着信する可能性があるコールを処理できる、十分な B チャネルを常に使用可能にしておく必要があります。

この B チャネルの問題は、次の 2 つのケースで発生します。

- 公衆網から IP ネットワークへの着信コール
- IP ネットワークから公衆網への発信コール

着信コール

着信コールについて、次のシナリオを考えてみます。

> ある会社に Cisco 3526 IP/VC ゲートウェイがあり、それが ISDN PRI 回線でセントラル オフィス（CO）のスイッチに接続されています。この場合、ISDN PRI 回線は 23 の B チャネルを提供します。ビデオ コールが公衆網から 384 kbps で受信されます。このコールは 6 つの B チャネルを使用するので、残りの空きは 17 になります。最初のコールがまだアクティブな間に、第 2 と第 3 の 384 kbps のコールがその回線上で受信されます。それぞれのコールが 6 チャネルを使用するので、残りの空きは 5 チャネルになります。第 4 の 384 kbps のコールが受信されると、ゲートウェイはそのコールに応答しますが、十分な B チャネルの空きがないこと（残りチャネルは 5 つだけだが、コールに必要なチャネルは 6 つ）を認識し、接続を解除します（「16: Normal Call Clearing」を理由とした Q.931 RELEASE COMPLETE を送信）。第 4 のコールを試みた発信側は、コールの失敗の原因がわからず、番号を繰り返しリダイヤルしてコールを発信しようとします。

Cisco Unified Videoconferencing ゲートウェイでは、こうした問題が起きる可能性を最小にするために、ゲートウェイが一定の使用率しきい値（総帯域幅に対するパーセンテージとして設定）に到達したときに、ゲートウェイから CO へ残りの B チャネル（この例では 5 チャネル）をビジーアウトする要求を送信するように設定できます。

さらに、トランク グループ内で CO から複数の ISDN 回線をプロビジョニングできます。最初の回線がビジーアウトしきい値に到達した時点で、コールはグループ内の次の PRI へロールオーバーされます。Cisco 3540 IP/VC ゲートウェイは 2 つの ISDN PRI 接続を提供し、両方のポートにまたがったボンディング チャネルをサポートします。たとえば、ポート 1 の空きが 5 チャネルしかなく、ポート 2 がアイドル状態であるため、23 チャネルが使用可能であるとします。この場合、ポート 1 から 5 チャネル、ポート 2 から 1 チャネルを使用してボンディングすることにより、第 4 の 384 kbps のコールに成功できます。これにより、コントローラ 2 上に残る空きは 22 チャネルとなり、ある時点で着信コールが再びビジーアウトしきい値に到達します。その時点で、ポート 2 上の残りのチャネルはビジーアウトされ、それ以後のすべての着信コールは原因コード「Network Congestion」で拒否されます。Cisco Unified Videoconferencing ゲートウェイでは、異なるゲートウェイにまたがってチャネルを結合したり、同じ Cisco 3544 シャーシ内にあるさまざまな Cisco 3540 ゲートウェイ モデルにまたがってチャネルを結合したりすることができないため、ボンディングできる最大ポート

数は 2 つです。CO スイッチは、トランク グループ内の第 3 または第 4 の PRI にコールをロールオーバできます（ほとんどの CO が最大 6 回線のトランク グループをサポートしています）が、たとえば、PRI 番号 1 と PRI 番号 2 の間でチャネルをボンディングできても、PRI 番号 1 と PRI 番号 3 の間でボンディングすることはできません。

上記のビジーアウト ロジックは、すべてのコールが同じ速度で行われることを前提としています。たとえば、あるポート上で 384 kbps の 2 つのコールがアクティブなときに、128 kbps のコールが着信したとします。このコールは 2 チャネルしか使用しないため、3 つのコールに合計 14 チャネル（6+6+2 = 14）が使用され、回線上に 9 チャネルの空きが残ります。ところが、ビジーアウトしきい値が（すべてのコールが 384 kbps で行われると想定して）18 チャネルに設定されていると、このビジーアウトしきい値でまだ使用可能なチャネルは 4 つだけになります。この時点で別の 384 kbps のコールが着信すると、そのコールは、残りの 4 チャネルではコールのサポートに不十分なため、失敗します。また、18 チャネルというビジーアウトしきい値にまだ達していない（14 チャネルしか使用されていない）ので、回線はビジーアウトされず、コールは次の回線にロールオーバーされません。この状態は、既存のコールの 1 つが切断されるまで続きます。このような状況を避けるため、すべてのコールを単一のコール速度に標準化できるようにすることが重要です。

発信コール

発信コールでも着信コールと同じ状況が起きる可能性がありますが、ビジーアウトの発生の仕方は異なります。Cisco 3500 シリーズの IP/VC ゲートウェイは、Resource Availability Indicator および Resource Availability Confirm（RAI/RAC）というメッセージをサポートしています。RAI/RAC メッセージは H.225 RAS 仕様で定義されており、ゲートウェイが満杯でコールをそれ以上ゲートキーパーにルーティングできないことを、ゲートウェイからゲートキーパーに伝えるために使用されます。ゲートウェイはビジーアウトしきい値に達すると、ステータスが True の RAI メッセージをゲートキーパーに送信します。True は「これ以上のコールの送信不可」を意味し、False は「送信可」を意味します。ゲートウェイは、ビジーアウトしきい値を下回るとすぐに RAI=False を送信します。発信コールのビジーアウトしきい値は着信コールのビジーアウトしきい値とは別のもので、それぞれ別々に設定できるので、着信コールを次の空き回線にロール オーバしても発信コールは引き続き受け入れられ、その逆も同様です。たとえば、RAI しきい値を 12 チャネルに設定し、ISDN ビジーアウトしきい値を 18 チャネルに設定できます。その場合、384 kbps の 2 つのコールがアクティブのとき、発信コールは次の空きゲートウェイにロール オーバされますが、3 番目の 384 kbps の着信コールは引き続き受け入れられます。同じように効率的に発信コールのビジーアウト フェールオーバーを実現する方法として、RAI/RAC 方式ではなく、次項で述べるように Cisco Unified CallManager のルート グループとルート リストの構造を使用する方法があります。

Cisco Unified CallManager でのゲートウェイの設定

Cisco Unified CallManager では、次のいずれかの方法で IP/VC ゲートウェイを設定できます。

- H.323 ゲートウェイとして設定し、Cisco Unified CallManager でコールをそのゲートウェイに直接ルーティングします。
- ゲートキーパーへの H.225 ゲートキーパー制御トランクを設定し、ゲートキーパーを通じてそのゲートウェイにコールをルーティングします。

ゲートウェイが 1 つだけであれば、多くの場合、トランクを介してゲートウェイに到達するよりも、Cisco Unified CallManager で直接設定した方が簡単です。ロード バランシングと冗長性を得るために複数のゲートウェイを使用している場合は、それらのゲートウェイをすべて Cisco Unified CallManager で設定し、ルート グループとルート リストの中に配置する方法があります。または、ゲートキーパーへの H.225 トランクを設定してゲートウェイ間の RAI/RAC を使用し、コールの送信先となるゲートウェイをゲートキーパーが Cisco Unified CallManager に指示するように設定する方法があります。

公衆網から Cisco Unified CallManager への着信コールの場合、各 Cisco Unified Videoconferencing ゲートウェイを 1 つのゲートキーパーに登録する方法と、それらのゲートウェイを、すべての着信コール要求の送り先とする最大 3 台の Cisco Unified CallManager サーバの IP アドレスを使用して設定する方法があります。この方法は、ピアツーピア モードと呼ばれます。どちらの方法でも最終的な目標は、各ゲートウェイが受信したすべての着信コールを Cisco Unified CallManager に送り、Cisco Unified CallManager がコールのルーティング方法を決定できるようにすることです。コールをゲートウェイから Cisco Unified CallManager にルーティングするようゲートキーパーを設定する方法の詳細については、P.15-24 の「ゲートキーパー」を参照してください。

コール シグナリング ポート番号

デフォルトでは、Cisco Unified Videoconferencing ゲートウェイはウェルノウン ポート 1720 ではなく、TCP ポート 2720 を監視します。しかし、同じくデフォルトで、Cisco Unified CallManager は H.323 コールをポート 1720 に送信します。Cisco Unified CallManager の H.323 ゲートウェイ デバイスの設定では、ゲートウェイが監視するポートや、Cisco Unified CallManager の送信先ポートを変更できます。いずれの方法でも、ゲートウェイへの発信コールが成功するためには、両側で一致している必要があります。

着信方向では、Cisco Unified Videoconferencing ゲートウェイは、ピアツーピア モードで動作するように設定された場合、コールをポート 1720 で Cisco Unified CallManager に送信します。ゲートキーパーに登録するように設定された場合、Cisco Unified CallManager は、ランダムに生成されたポート番号をすべてのゲートキーパー制御トランクに使用します。この方法では、Cisco Unified CallManager が同じゲートキーパーに対して複数のトランクを持つことができます。このポート番号は、Cisco Unified CallManager からゲートキーパーへの Registration Request（RRQ）に含まれているため、ゲートウェイから Cisco Unified CallManager への着信 H.225 セットアップ メッセージは、このポート番号に送られます。ただし、ゲートウェイが Cisco Unified CallManager で H.323 ゲートウェイ デバイスとして直接設定されている場合、Cisco Unified CallManager はコールが H.225 トランクの TCP ポートに着信したことを無視し、発信元 IP アドレスをデータベースに設定されている H.323 ゲートウェイ デバイスと照合します。一致するデバイスが見つからない場合、Cisco Unified CallManager はそのコールがトランクに着信したかのように扱います。

発信方向に関しては、Cisco Unified CallManager がゲートキーパー制御 H.225 トランクを使用してゲートウェイに到達している場合は、ゲートキーパーが Cisco Unified CallManager に、どの TCP ポートを使用してゲートウェイに到達すべきかを知らせます。ゲートウェイが Cisco Unified CallManager で H.323 ゲートウェイ デバイスとして設定されている場合（ピアツーピア モード）、Cisco Unified CallManager は、ポート 2720（デフォルト）か 1720（ゲートウェイで監視ポートが変更された場合）にコールを送るように設定されている必要があります。

コール シグナリング タイマー

H.320 ボンディングに固有の遅延のため、ビデオ コールは音声コールよりも接続に時間がかかる場合があります。Cisco Unified CallManager のいくつかのタイマーは、デフォルトで音声コールをできるだけ高速に処理するように調整されているため、それが原因でビデオ コールが失敗する場合があります。したがって、H.320 ゲートウェイ コールをサポートするには、次のタイマーをデフォルト値から変更する必要があります。

- H.245TCSTimeout
- Media Exchange Interface Capability Timer
- Media Exchange Timer

これらの各タイマーを、Cisco Unified CallManager Administration の Service Parameters で 25 まで増やすことをお勧めします。このパラメータは、クラスタ全体のサービス パラメータなので、既存の H.323 Cisco 音声ゲートウェイへの音声コールも含めて、あらゆるタイプの H.323 デバイスへのコールに影響を与えることに注意してください。

音声ゲートウェイ ベアラ機能

H.323 コールは、どのタイプのコールを行うかを示すために、H.225/Q.931 Bearer Capabilities Information Element（bearer-caps）を使用します。音声専用コールでは、bearer-caps が「speech」または「3.1 KHz Audio」に設定され、ビデオ コールでは bearer-caps が「Unrestricted Digital Information」に設定されます。Cisco 音声ゲートウェイ、一部のレガシー PBX、および大部分のセルラー電話会社は、Unrestricted Digital Information の bearer-caps をサポートしていません。したがって、音声ゲートウェイへのコールを Cisco Unified CallManager がビデオ コールとして試みた場合、コールが失敗することがあります。

Cisco Unified CallManager は、次の要因に基づいて、どの bearer-caps を設定するかを決定します。

- 発信側デバイスまたは着信側デバイス（あるいはその両方）がビデオ対応かどうか
- それらのデバイス間のコールにビデオを許可するように Cisco CallManager のリージョンが設定されているかどうか

たとえば、ビデオ対応デバイス（関連付けられた VT Advantage クライアントを持つ Cisco Unified IP Phone など）が Cisco 音声ゲートウェイと同じリージョン内で設定されているネットワークを考えてみます。ユーザが外線にアクセスするために 9 をダイヤルすると、Cisco Unified CallManager は、発信側デバイスがビデオ対応であって、リージョンが 384 kbps のビデオ帯域幅を許可するように設定されていることを確認します。Cisco Unified CallManager は、そのコールに対して bearer-caps を Unrestricted Digital Information に設定します。ところが、コールが Cisco 音声ゲートウェイへのコールなので、ゲートウェイはそのコールを原因コード「Incompatible Destination」で拒否します。この問題は、H.323 音声ゲートウェイを使用し、Cisco Unified Video Advantage に関連付けられた IP Phone のあるすべてのネットワークで発生します。ユーザにとっては、Cisco Unified Video Advantage をインストールするまで、すべてが順調に機能しているように見えますが、Cisco Unified Video Advantage を実行している PC を IP Phone に接続するとすぐに、公衆網へのコールが失敗します。

この状況になるのは、H.323 音声ゲートウェイへのコールだけです。Cisco 音声ゲートウェイが Cisco Unified CallManager との通信に MGCP を使用している場合、この問題は発生しません。それは、Cisco Unified CallManager の MGCP プロトコル スタック上ではビデオがサポートされておらず、しかも、MGCP モードでは、Cisco Unified CallManager が公衆網への D チャネル シグナリングを完全に制御するためです。同様に、Cisco 音声ゲートウェイが Cisco Unified CallManager との通信に SIP を使用している場合も、この問題は発生しません。その理由は、Cisco Unified CallManager の SIP プロトコル スタック上でビデオがサポートされていないためです。たとえサポートされていたとしても、ゲートウェイは、Cisco Unified CallManager の発信 SDP（Session Description Protocol）アドバタイズメントで渡されたビデオ機能を無視するだけです。

このような状況を防止するには、次の例に示すように、**voice-port** 設定モードで **bearer-caps** コマンドを使用することにより、すべての Cisco H.323 音声ゲートウェイに bearer-caps を設定します。

```
gateway#configure terminal
gateway(config)#voice-port 1/0:23
gateway(config-voiceport)#bearer-caps speech
```

CHAPTER 5

Cisco Unified CallManager トランク

Cisco Unified CallManager Release 4.0 では、Session Initiation Protocol（SIP）トランクがサポートされるようになりました。Release 4.0 より前の Cisco Unified CallManager は、H.323 トランクのみをサポートしていました。この章では、Cisco Unified CallManager Release 5.0 に関する設計の考慮事項について説明します。ただし、説明の多くは Cisco Unified CallManager Release 4.1、4.0、および 3.3 にも該当します。

現在、H.323 トランクは、他の Cisco Unified CallManager クラスタや、ゲートウェイなどの他の H.323 デバイスに対する接続性を提供します。H.323 トランクは、Cisco Unified CallManager がクラスタ内通信用にサポートするオーディオおよびビデオ コーデックのほとんどをサポートします。ただし、ワイドバンド オーディオ、ワイドバンド ビデオ、および H.264 ビデオについてはサポートしません。

H.323 トランクは、Empty Capabilities Set（ECS）を使用して、保留 / 保留解除や転送などの補足コール サービスを提供します。この方法は、メディア ストリーム（またはチャネル）を停止または終了し、同一または別のエンドポイント アドレスに対してメディア ストリームを開始または起動するための標準の H.245 メカニズムです。この方法を使用すると、Cisco Unified CallManager は、コールをアクティブにしたままでも、メディア ストリームの送信元および宛先を迅速に制御することができます。

たとえば、H.323 トランクを使用した 2 つのクラスタ（A と B）間のコールについて考えます。クラスタ A のユーザがクラスタ B のユーザを保留にした場合、2 人のユーザ間のメディア ストリームは終了し、クラスタ B のユーザはクラスタ A の Music On Hold（MoH）サーバに接続されます。MoH サーバは、ユーザにメディア（音楽ファイル）を送信するよう指示されます。クラスタ A のユーザがコールを保留解除すると、MoH ストリームが終了し、2 人のユーザ間で双方向メディア ストリームが再開されます（Cisco Unified CallManager は、補足コール サービス用に H.450 をサポートしていません）。このケースでは、MoH は ECS 動作の一例です。H.323 トランクはマルチキャスト MoH をサポートしないため、H.323 トランクの Media Resource Group List（MRGL; メディア リソース グループ リスト）には、ユニキャスト MoH リソースだけを含める必要があります（詳細については、P.7-1 の「Music on Hold」を参照してください）。

H.323 トランク上のコールに使用される帯域幅を制御するには、Cisco Unified CallManager で設定され、各トランクに割り当てられる、*リージョン*を使用します。リージョンは、そのリージョンの音声コーデック タイプとビデオ帯域幅を指定することで、コールに割り当てられる帯域幅の量を制限します。そのリージョンと別のリージョン間のコールは、指定された帯域幅の制限を超えることはできません。H.323 トランク上でコールを発信するデバイスが、より限定的なリージョン内にある場合や、ビデオなどの特定のコーデックをサポートしない場合、そのデバイスはそのコールに使用可能なコーデックのサブセットになっています。

H.323 トランク上のすべての DTMF（Dual Tone MultiFrequency）シグナリングは、H.245 を使用してアウトバンドで提供されます。

SIP トランクは、ゲートウェイ、プロキシ、ボイスメール システム、および他の Cisco Unified CallManager クラスタなど、他の SIP デバイスへの接続性を提供します。Cisco Unified CallManager 5.0 では、SIP トランクの主な拡張機能が導入され、Cisco Unified CallManager 4.1 および 4.0 での制限（たとえば、単一コーデックのサポート、ビデオ サポートの欠如、RFC 2833 DTMF サポートに必須のメディア ターミネーション ポイント（MTP）など）が解消されました。

Cisco Unified CallManager 5.0 でのそれ以外の SIP トランクに対する主な拡張機能としては、REFER、ヘッダー置換、Subscribe/Notify、Message Waiting Indication（MWI; メッセージ待機インジケータ）、MTP の削除、ビデオ サポート、着信ポート番号 1 つあたり複数の SIP トランク、SIP リダイレクション 3XX、Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）、ダイジェスト認証、コール保持、および T.38 FAX リレーのサポートがあります。SIP トランクの新規拡張機能の全リストについては、次の Web サイトで入手可能な Cisco Unified CallManager 5.0 の製品マニュアルを参照してください。

http://www.cisco.com

クラスタ間トランキングに使用した場合、SIP トランクは Secure Real-Time Transport Protocol（SRTP）や、Annex M1 を使用した QSIG Tunneling をサポートしません。

H.323 トランク

Cisco Unified CallManager では、次の主要なタイプの H.323 トランクを設定できます。

- クラスタ間トランク（非ゲートキーパー制御）（P.5-3）
- クラスタ間トランク（ゲートキーパー制御）（P.5-3）
- H.225 トランク（ゲートキーパー制御）（P.5-4）

クラスタ間トランク（非ゲートキーパー制御）

このトランクは、最も単純なもので、単一のマルチクラスタ キャンパスまたは分散型コール処理配置で他の Cisco Unified CallManager クラスタに接続するために使用されます。このトランクは、コール アドミッション制御にゲートキーパーを使用しません。ただし、帯域幅制御が必要な場合は、Cisco Unified CallManager で設定されたロケーションを使用できます。

このタイプのトランクを定義する場合、同一の宛先クラスタに最大 3 つのリモート Cisco Unified CallManager サーバを定義できます。トランクは、定義されているすべてのサーバに自動的にロードバランスされます。リモート クラスタでは、対応するクラスタ間トランク（非ゲートキーパー制御）を設定することが重要です。このトランクには、最初のクラスタでリモート Cisco Unified CallManager サーバとして定義されているサーバと同じサーバを含む Cisco Unified CallManager グループを割り当てます。同様の設定は、クラスタ間トランクによって接続された各 Cisco Unified CallManager クラスタでも必要です。

たとえば、クラスタ 1 にクラスタ 2 へのトランクがあり、クラスタ 2 にクラスタ 1 へのトランクがある場合は、次の設定が必要になります。

- クラスタ 1
  - サーバ B、C、および D を、クラスタ 2 へのトランクに関連付けられたデバイス プールで定義されている Cisco Unified CallManager グループのメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 2 のリモート サーバ D、E、および F を設定します。
- クラスタ 2
  - サーバ D、E、および F を、クラスタ 1 へのトランクに関連付けられたデバイス プールで定義されている Cisco Unified CallManager グループのメンバーとして設定します。
  - 非ゲートキーパー制御トランクに、クラスタ 1 のリモート サーバ B、C、および D を設定します。

クラスタ間トランク（ゲートキーパー制御）

クラスタ数が多くなる場合は、クラスタ間非ゲートキーパー制御トランクの代わりに、クラスタ間ゲートキーパー制御トランクを使用する必要があります。ゲートキーパー制御トランクを使用する主な利点は、クラスタとフェールオーバー時間を全体的に管理できることです。非ゲートキーパー制御トランクでは、一般に、トランクのフル メッシュを設定する必要があります。ただし、この作業は、クラスタ数が増加すると管理負担になる場合があります。また、クラスタ内のサブスクライバ サーバが到達不能になった場合は、5 秒（デフォルト）でコールの試行がタイムアウトします。クラスタ全体が到達不能になった場合、コール障害または公衆網を介した再ルーティングのどちらかが発生するまでの試行回数は、トランク用に定義されたリモート サーバの数と、ルート リストまたはルート グループ内のトランクの数によって異なります。リモート サーバと非ゲートキーパー制御トランクの数が多いと、コール遅延が過剰になることがあります。

ゲートキーパー制御トランクを使用する場合は、ゲートキーパーに登録されている他のすべてのクラスタとゲートキーパーを介して通信できるトランクを 1 つだけ設定します。クラスタまたはサブスクライバが到達不能になった場合、ゲートキーパーは自動的に、コールをクラスタ内の別のサブ

スクライバに送信するか、または他のサブスクライバが存在しなければコールを拒否します。その結果、ほとんど遅延させることなく、公衆網を介して（必要な場合）コールを再ルーティングすることができます。単一の Cisco ゲートキーパーを使用すると、100 のクラスタすべてが、それぞれ 1 つのトランクを、相互にコールできるすべてのクラスタに登録できます。非ゲートキーパー制御トランクを使用する場合、この同じトポロジでは、各クラスタに 99 のトランクを設定する必要があります。クラスタ間ゲートキーパー制御トランクは、他の Cisco Unified CallManager と通信する場合にのみ使用する必要があります。これは、このトランクを他の H.323 デバイスで使用すると、補足サービスに問題が発生することがあるためです。また、Release 3.2 より前の Cisco Unified CallManager との下位互換性を確保する場合は、クラスタ間ゲートキーパー制御トランクを使用する必要があります。

H.225 トランク（ゲートキーパー制御）

H.225 ゲートキーパー制御トランクは、本質的にはクラスタ間ゲートキーパー制御トランクと同じですが、Cisco Unified CallManager クラスタ Release 3.2 以降のほか、ゲートウェイ、会議システム、およびクライアントなどの他の H.323 デバイスと連携動作する機能を持つ点が異なります。この機能は、コールごとに検出メカニズムを通じて実現されます（この検出プロセスの詳細については、P.5-10 の「Cisco Unified CallManager における H.323 の動作」を参照してください）。このタイプのトランクは、すべての Cisco Unified CallManager クラスタが Release 3.2 以降の場合に推奨される H.323 トランクです。

ゲートキーパー トランクの冗長性、復元性、およびロード バランシング

冗長性は、設計の要件に応じて、複数の方法で実現できます。最も簡単に実現するには、ゲートキーパー制御トランクを設定し、そのトランクに割り当てられたデバイス プールに関連付けられている Cisco Unified CallManager グループに、最大 3 つのサブスクライバを割り当てます。この設定により、すべてのサーバが、同じテクノロジー プレフィックスと共に、同じゾーン内の同じゲートキーパーに登録されます。ただし、h323_id に使用される H.323 トランクの名前には、「*_n*」というサフィックスが付加されます。ここで、*n* はクラスタ内のノード番号です。この ID は自動的に生成され、変更することはできません。単一のトランクを設定しても、ゲートキーパーは、複数のトランク、つまり Cisco Unified CallManager グループ内のサブスクライバごとに 1 つのトランクを登録します。

追加の冗長性要件がある場合は、別のゲートキーパー制御トランクに、Cisco Unified CallManager グループにある別の名前と別のサブスクライバを設定できますが、それ以外のパラメータはすべて最初のトランクと同じになります。この 2 つ目のトランクによって、追加のサブスクライバがゲートキーパーに登録されます。

標準のサブスクライバ ペアを構成する 2 つのサーバから Cisco Unified CallManager グループを構成し、このグループを含むデバイス プールを割り当てることをお勧めします（サブスクライバの冗長性の詳細については、P.8-7 の「コール処理サブスクライバ」を参照してください）。クラスタ全体で完全な冗長性を実現するには、4 つの異なるデバイス プールを使用する 4 つのトランクが必要になります。結果的に、8 つのサブスクライバがゲートキーパーに登録されます（3 つのトランクとより大きな Cisco Unified CallManager グループを使用しても同じ結果となります）。

登録時、Cisco Unified CallManager とゲートキーパー間では複数のパラメータが受け渡しされます。Cisco Unified CallManager は、トランクごとに、ゲートキーパーの Registration Admission Status（RAS）メッセージ用に、一時的なユーザ データグラム プロトコル（UDP）ポートを使用します。このポートは、通常であれば、UDP 1719 です。ただし、Cisco Unified CallManager は、特定の RAS メッセージの宛先であるトランクを判別できる必要があります。したがって、Cisco Unified CallManager は一定範囲の UDP ポートを使用して、動的に割り当てます。

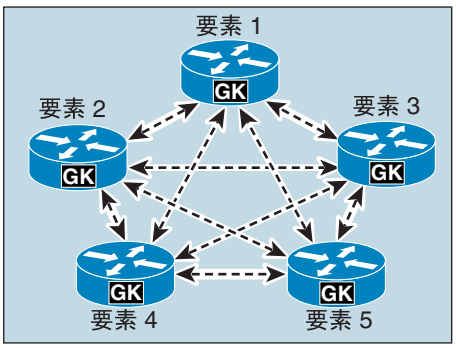
登録プロセス時、トランクは、その Cisco Unified CallManager グループにある他のサブスクライバに関する次の情報を登録します。

- H.225 コール シグナリング ポート
- h323_id
- CanMapAlias サポート
- テクノロジー プレフィックス
- H.225 コール シグナリング アドレス

推奨されるクラスタ化ゲートキーパーが使用されている場合、ゲートキーパーは、代替ゲートキーパー アドレスのリストを返します。このリストは、プライマリ ゲートキーパーで障害が発生した場合や使用可能なリソースが不足した場合に使用されることがあります。

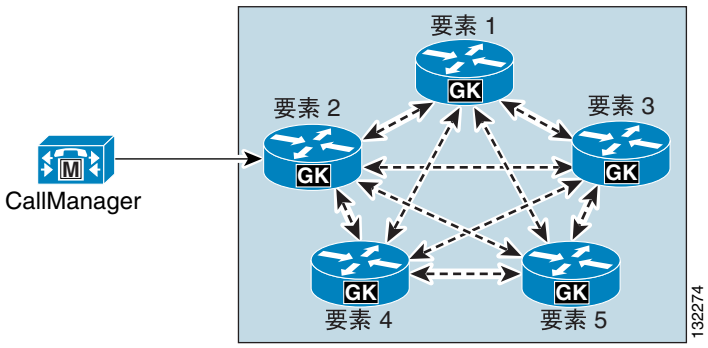
図 5-1 は、Gatekeeper Update Protocol（GUP）を使用して通信する、ゲートキーパーのクラスタを示しています（ゲートキーパーの詳細については、P.8-1 の「コール処理」の章を参照してください）。

図 5-1　ゲートキーパー クラスタ



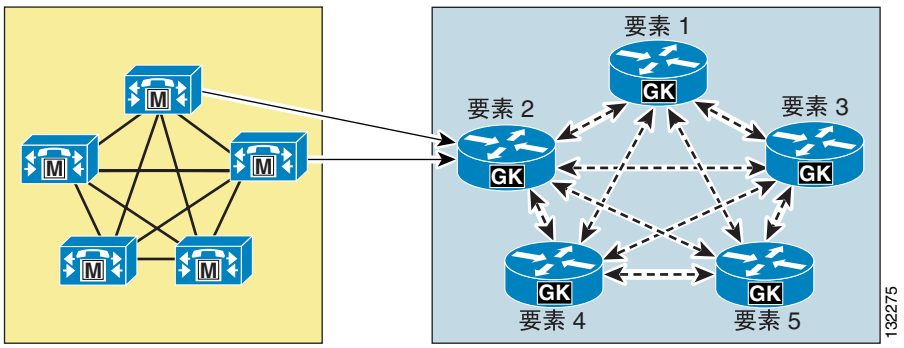
H.323 トランクの Cisco Unified CallManager グループにサブスクライバが 1 つだけ含まれている場合、Cisco Unified CallManager の設定済みゲートキーパーとゲートキーパー クラスタの間の接続は 1 つのみになります（図 5-2 を参照）。

図 5-2　単一の Cisco Unified CallManager サブスクライバを使用する H.323 トランク



トランクに関連付けられた Cisco Unified CallManager グループに複数のサブスクライバが含まれている場合、Cisco Unified CallManager クラスタとゲートキーパー クラスタ間には追加の接続が確立されます（図 5-3 を参照）。

図 5-3　複数の Cisco Unified CallManager サブスクライバを使用する H.323 トランク



このアプローチによってサブスクライバ障害やゲートキーパー障害に対する冗長性が確保されるのは、登録完了後です。これは、トランクの登録時に代替ゲートキーパーの通信が行われるためです。ただし、このアプローチでは、設定済みのゲートキーパーが初期登録時やリセット後に使用不能である場合には、冗長性が確保されません。これは、代替ゲートキーパーのリストがダイナミックであり、データベースに格納されないためです。冗長性のレベルを上げたりロード バランシングを追加したりするには、ゲートキーパー クラスタにある追加のゲートキーパーを Cisco Unified CallManager で設定します。たとえば、元のトランクが要素 2 に登録されている場合は、追加のゲートキーパーを要素 4 として設定できます（図 5-4 を参照）。

図 5-4　ロード バランシングと追加の冗長性のために設定された追加のゲートキーパー

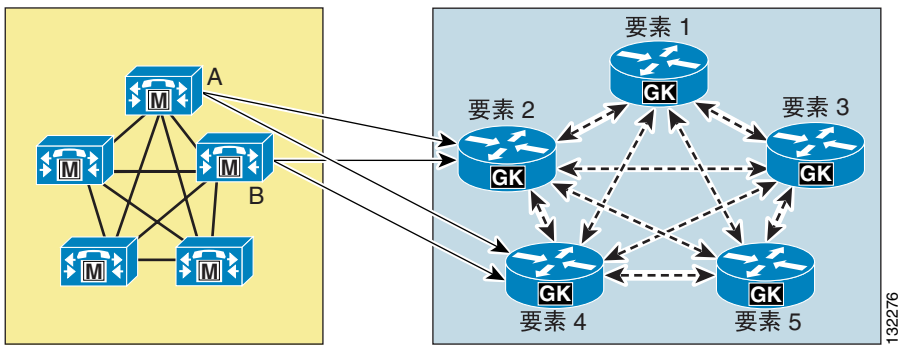


図 5-4 の例の場合、Cisco Unified CallManager の設定には次のコンポーネントが含まれます。

- 要素 2 と要素 4 の 2 つのゲートキーパー
- サブスクライバ サーバ A および B を含む Cisco Unified CallManager グループに対して定義された 2 つの H.323 トランク

このアプローチを使用すると、初期設定時に要素 2 または要素 4 が到達不能であっても（つまり、起動中またはトランクのリセット中でも）、引き続き Cisco Unified CallManager クラスタが登録できるようになります。

Cisco Unified CallManager クラスタに着信するコールのロード バランシングは、デフォルトで自動的に行われます。これは、ゲートキーパーが、ゾーン内の登録済みサブスクライバのいずれかをランダムに選択するためです。この動作が期待と異なる場合は、ゲートキーパーで **gw-priority** 設定コマンドを使用して、このデフォルト動作を変更することができます（例 5-1 を参照）。

例 5-1　gw-priority コマンドを使用してコールを特定のトランクに送信する

```
gatekeeper
 zone local SJC cisco.com 10.0.1.10
 zone prefix SJC 1408....... gw-priority 10 sjc-trunk_2
 zone prefix SJC 1408....... gw-priority 9 sjc-trunk_3
 zone prefix SJC 1408....... gw-default-priority 0
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
 endpoint ttl 60
```

例 5-1 では、H.323 トランクは Cisco Unified CallManager で sjc-trunk として設定されています。また、Cisco Unified CallManager サブスクライバが、クラスタ内のサブスクライバのノード番号を示すために、「_2」と「_3」のサフィックスを自動的に付加します。したがって、この例では、最初の選択肢としてノード 2 を使用します。このノードは、このトランクの CallManager グループにおいて最もプライオリティの高い Cisco Unified CallManager となる必要があります。このケースでは、ノード 3 は 2 番目の選択肢となります。

gw-default-priority 0 を使用するかどうかは任意です。この例で使用したのは、このゾーンで登録するよう不用意に設定される可能性のある他のトランクが一切使用されないようにするためです。

Cisco Unified CallManager クラスタからの発信コールは、次のいずれかの方法でロードバランスできます。

- ルート グループにある単一の H.323 トランクは、常に、Cisco Unified CallManager グループで使用可能な最もプライオリティの高いサブスクライバを使用します。プライオリティの低いサブスクライバが使用されるのは、プライオリティの高いサブスクライバが使用不能になった場合のみです。
- 循環ルート グループにある複数の H.323 トランクは、グループ内のすべての H.323 トランクに均等にコール負荷を分散します。

次の例は、さまざまなシナリオでロード バランシングを設定する方法を示しています。

すべてのコールをクラスタ内の単一のサブスクライバから発信する場合：

- ルート グループ内に単一の H.323 トランクを設定します。

コールをクラスタ内の 4 つのプライマリ サブスクライバに分散する場合：

- 4 つの Cisco Unified CallManager グループに対して 4 つの H.323 トランクを定義し、すべてのトランクを循環ルート グループに含めます。
- Cisco Unified CallManager 冗長性グループは、次のように定義されます。
  - サブスクライバ A、サブスクライバ B
  - サブスクライバ C、サブスクライバ D
  - サブスクライバ E、サブスクライバ F
  - サブスクライバ G、サブスクライバ H

  サブスクライバ A、C、E、および G はすべてプライマリで、サブスクライバ B、D、F、および H はバックアップです。

コールをクラスタ内の 8 つのサブスクライバに分散する場合：

- 8 つの異なる Cisco Unified CallManager グループに対して 8 つの H.323 トランクを定義し、各グループにサブスクライバを 1 つだけ含め、すべてのトランクを循環ルート グループに含めます。
- Cisco Unified CallManager 冗長性グループは、次のように定義されます。
  - サブスクライバ A
  - サブスクライバ B
  - サブスクライバ C
  - サブスクライバ D
  - サブスクライバ E
  - サブスクライバ F
  - サブスクライバ G
  - サブスクライバ H

メディア ターミネーション ポイントを使用する H.323 トランク

メディア ターミネーション ポイント（MTP）は、一般に、H.323 トランクの通常動作には必要ありません。ただし、通信相手となるデバイスが、H.323 Version 1 である場合や、補足サービス用に Empty Capabilities Set（ECS）をサポートしていない場合には必要です。

MTP が必要かどうかをテストするには、次の簡単な手順を使用します。

1. 電話機から H.323 トランクを介して他のデバイスにコールを発信します。このコールは通常どおりに発信する必要があります。
2. コールを保留にしてから、保留解除します。コールがドロップする場合は、Cisco Unified CallManager と他のデバイス間の相互運用性を保証するために MTP を使用することをお勧めします。

MTP は、H.323 トランク上でコールを発信する他のデバイスからのメディア ストリームを終端させる場合や、同じ音声ペイロードでメディア ストリームを再発信する場合に非常に役立ちます。ただし、そのような場合、IP アドレスは MTP のアドレスに変更されます。この事実に留意して、次のシナリオで MTP を使用します。

- 企業内の電話機、ゲートウェイ、および他のデバイスがすべて RFC 1918 プライベート アドレスを使用する場合は、すべての音声およびビデオ デバイスにネットワーク アドレス変換（NAT）を使用しなくても、引き続きパブリック ネットワーク上の他のシステムに接続できます。パブリック ネットワークと通信する Cisco Unified CallManager サブスクライバがパブリック IP アドレスを使用している場合、シグナリングはルーティングされます。また、すべての MTP もパブリック アドレスを使用している場合、RFC 1918 アドレスを持つデバイスからのメディアは MTP で終端され、再度発信されます。ただし、今度は、パブリック ネットワーク上でルーティング可能なパブリック アドレスが割り当てられます。このアプローチを使用すると、RFC 1918 アドレスを持つ何万台ものデバイスが、パブリック ネットワークと通信できるようになります。この同じ方法を使用すると、企業ネットワークにあるデバイスが他の企業またはサービス プロバイダーと通信するときに、そのデバイスの実際の IP アドレスを隠すことができます。
- 信頼性境界を設定すると、ファイアウォールを通過させることや、アクセス コントロール リスト（ACL）を使用したアクセスを許可することができます。通常、メディアがファイアウォールを通過できるようにするには、アプリケーション レイヤ ゲートウェイ（ALG）またはフィックスアップを使用して、動的にメディア ストリームにアクセス許可を与えるか、または、ファイアウォールを越えて通信する必要のある音声デバイスすべてで使用するための広範囲のアドレスおよびポートを割り当てます。H.323 トランクを使用し、ファイルまたは ACL を通過するすべてのコールには、MTP から発信されるメディアが割り当てられます。このメディアでは、単一の IP アドレスまたは狭い範囲の IP アドレスを使用できます。

これらの方法を両方使用する場合、**MTP Required** チェックボックスをオンにすると、デフォルトで、H.323 トランク上のコールが許可されます。このことは、MTP リソースが使用不能の場合や、使い果たされた場合でも同様です。このデフォルト動作により、コールの音声パスが使用不能になる場合があります。この動作を変更するには、H.323 セクションにある Cisco CallManager サービス パラメータ **Fail Call if MTP allocation fails** を **True** に設定します。

Cisco Unified CallManager における H.323 の動作

この項では、H.323 プロトコルを Cisco Unified CallManager で使用および実装する方法、および特定の機能が所定どおりに動作する仕組みとその理由について説明します。

理解する上で最も重要な点は、どのサブスクライバがコール シグナリング デーモンを実行するかということです。このデーモンは、H.323 コールを発信および受信する部分的なコードです。これは、通常、H.225 デーモン（H.225D）と呼ばれます。H.225 は、H.323 プロトコルの一部で、主にコール制御を担当します。H.245 は、H.323 のもう 1 つの主要コンポーネントで、コールのメディア制御を担当します。

特定の H.323 デバイスに対する Cisco Unified CallManager グループのリストに含まれているサブスクライバによって、デーモンを実行するサブスクライバと実行時期が決定されます。この点は非常に重要です。これは、不適切なサブスクライバに送信されたコールは、別の H.225D によって拒否または処理される場合があるためです。たとえば、この状況が発生するのは、Cisco IOS H.323 ゲートウェイに、Cisco Unified CallManager クラスタ内のサブスクライバ C にコールを送信するダイヤルピアが設定されているものの、そのゲートウェイの Cisco Unified CallManager グループのリストにはサブスクライバ A および B しか含まれていない場合です。そのような場合、コールは失敗するか、またはデーモンがサブスクライバ上に設定されていれば H.323 トランク デーモンによって処理されます。

次のシナリオは、H.225D がサブスクライバ上に作成される仕組みとその時期について説明しています。

- H.323 クライアント

  H.225D は、H.323 クライアントに関連付けられた Cisco Unified CallManager グループで使用可能な、最もプライオリティの高いサブスクライバ上だけでアクティブになります。

  H.323 クライアントがゲートキーパー制御の場合、RasAggregator デバイスは、ゲートキーパー制御の H.323 クライアントに関連付けられた Cisco Unified CallManager グループで使用可能な、最もプライオリティの高いサブスクライバから登録されます。

  RasAggregator は、次の 2 つの特殊機能を提供するためにゲートキーパー ゾーンで登録される特殊なデバイスです。

  - H.323 クライアントが DHCP を使用している場合は、DNS を使用している Cisco Unified CallManager でそのクライアントを使用できません。ただし、クライアントが Dynamic DNS をサポートしている場合は除きます。RasAggregator を使用すると、Cisco Unified CallManager は、コールを発信するたびに、ゲートキーパーに登録されている特定の H.323 クライアントの IP アドレスを取得できます。ゲートキーパー登録は、H.323 クライアントの E.164 アドレスを含む標準の RAS ARQ メッセージを使用して行われます。ゲートキーパーは、E.164 アドレスを解決し、IP アドレスを ACF メッセージで Cisco Unified CallManager に返します。
  - また、RasAggregator を使用すると、H.323 クライアントによるコールはすべて Cisco Unified CallManager を経由するようになり、クライアント自身の間では直接やり取りされないことが保証されます。これにより、ダイヤリング規則とコーデック制限が適用されることが保証されます。

- H.323 ゲートウェイ

  H.225D は、H.323 ゲートウェイに関連付けられた Cisco Unified CallManager グループにあるすべてのサブスクライバ上でアクティブになります。

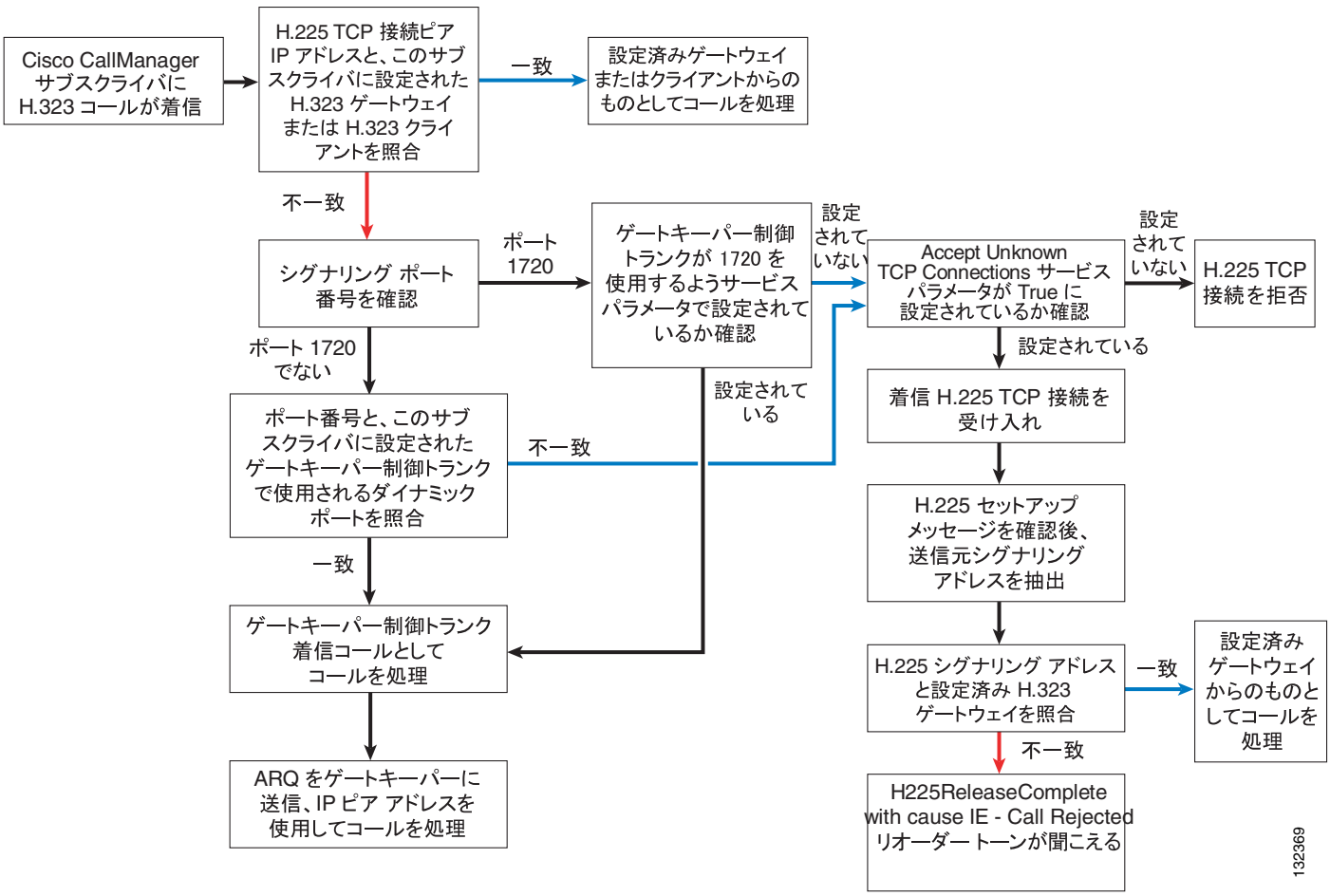
- H.323 トランク

  H.225D は、H.323 トランクに関連付けられた Cisco Unified CallManager グループにあるすべてのサブスクライバ上でアクティブになります。

  RAS デーモンは、関連付けられている Cisco Unified CallManager グループにあるすべてのサブスクライバから、トランクをゲートキーパーに登録します。

Cisco Unified CallManager クラスタ内のサブスクライバに H.323 コールが着信すると、コールを受け入れるかまたは拒否するか、受け入れる場合はどの H.225D がコールを受信するかなど、さまざまな決定が下されます。図 5-5 は、このプロセスの仕組みを示しています。

図 5-5　H.323 コールの受け入れまたは拒否を判別するプロセス



Cisco Unified CallManager の H.323 プロトコルには、次の追加機能が含まれています。

- Protocol Auto Detect

  この機能では、コールごとに、発信側デバイスが Cisco Unified CallManager Release 3.2 以降を使用しているかどうかを判別できます。コールを受信するたびに、Cisco Unified CallManager は H.225 User-to-User Information Element（UUIE）を検索します。この UUIE は、もう一方の側が別の Cisco Unified CallManager であるかどうかを示します。UUIE が見つかった場合、Cisco CallManager は常に Intercluster Trunk Protocol を使用します。UUIE が見つからない場合は、設定済みのプロトコルをそのデバイスに対して使用します。この機能を使用すると、H.225 ゲートキーパー制御トランクは、コールごとに Intercluster Trunk Protocol と H.225 を切り替えることができます。これにより、Cisco Unified CallManager クラスタと他の H.323 デバイスを組み合せてゲートキーパーを使用することができます。Intercluster Trunk Protocol は、H.225 と類似していますが、特定の機能を Cisco Unified CallManager クラスタ間で正しく動作させる仕組みが異なります。

- Tunneled Q.SIG または H.323 Annex M1

  Cisco Unified CallManager 4.1(3) のリリースから、この機能はすべての H.323 トランク上で有効にできるようになりました。これにより、特定の H.323 Annex M1 機能を、Cisco Unified CallManager クラスタと、同じく H.323 Annex M1 をサポートする他の確認済みシステムとの間に実装することができます。これらの機能には、次のものがあります。

  — パス交換

  — メッセージ待機インジケータ（MWI）

  — コールバック

- 代替エンドポイント

  この機能をサポートするゲートキーパー、たとえば Cisco Multimedia Conference Manager（MCM）Gatekeeper などに登録する場合、Cisco Unified CallManager はゲートキーパーに対し、H.323 トランクへのコールの代替宛先を通知できます。この代替エンドポイントまたは代替宛先は、この H.323 トランクが呼び出されたときに、ゲートキーパーによって発信側デバイスに送信されます。代替エンドポイントは、ゲートキーパーに登録されている H.323 トランクに関連付けられた Cisco Unified CallManager グループのリストに含まれている他のサブスクライバです。

- 代替ゲートキーパー

  この機能をサポートするゲートキーパーに H.323 トランクが登録される場合（たとえば、Cisco ゲートキーパー クラスタ）、Cisco Unified CallManager には、このゲートキーパーが失敗した場合や独自のリソースを使い果たした場合に、登録、コール アドミッション要求、および他の RAS 機能を処理できる他のゲートキーパーに関する情報が動的に通知されます。

- CanMapAlias

  H.323 トランクは、ゲートキーパーに Admission Request（ARQ; 許可要求）を送信すると、Admission Confirmation message（ACF; アドミッション確認）で異なる E.164 番号を受信する場合があります。このことは、元の着信番号をこの新しい番号で置き換える必要があることを示しています。この機能では、Gatekeeper Transaction Message Protocol（GKTMP）を使用して Cisco ゲートキーパーと通信するルート サーバが必要になります。

  （注） CanMapAlias は、着信番号に関してのみサポートされます。

- 帯域幅要求

  H.323 トランクは、ゲートキーパーの帯域幅情報をアップデートし、特定のコールに割り当てられた帯域幅の要求量が変更されたことを示すことができます。この機能は、デフォルトでは無効になっています。この機能を制御するには、H.323 セクションにある Cisco CallManager サービス パラメータ **BRQ Enabled** を **True** に設定します。この機能は、H.323 トランク上でビデオを使用するときに特に重要です。これは、元の帯域幅要求が許容最大限の量を要求するためです。この機能を有効にすると、コール アドミッション制御が、コールのセットアップ中にネゴシエートされた実際の帯域幅を使用することが保証されます。

SIP トランク

Cisco Unified CallManager 4.*x* では、DTMF サポートのためにすべての SIP トランクが MTP を割り当てる必要があります。Cisco Unified CallManager 5.0 では、MTP チェックボックスが不要になり、MTP Required フラグはデフォルトでオフになります。この制限が解消されたことで、全体的なパフォーマンスが向上し、開放された MTP リソースを他のアプリケーションで使用できるようになりました。エンドポイントが RFC 2833 またはアウトオブバンド DTMF 方式の使用をエンドツーエンドでネゴシエートできる場合、DTMF イベントに MTP が割り当てられることがなくなりました。エンドポイント間で共通の DTMF 方式をネゴシエートできない場合、Cisco Unified CallManager 5.0 は動的に MTP を挿入します。

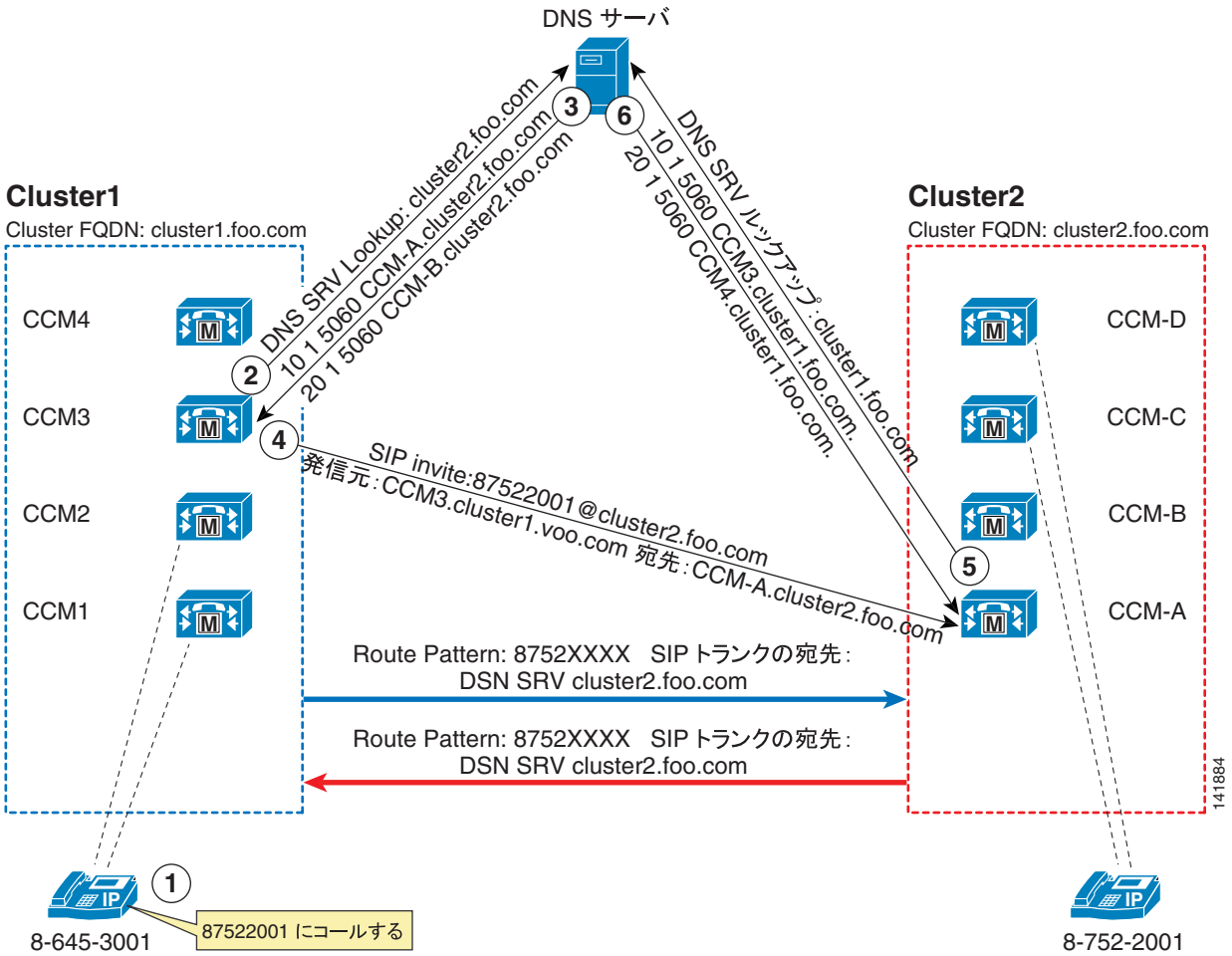
すべての SIP トランク コールに MTP が割り当てられないようにするために、Cisco Unified CallManager 5.0 には遅延メディアのサポート（SDP なしの INVITE）が含まれています。SIP アプリケーションの中には、遅延メディアをサポートしていないものがあります。そのような場合は、SIP Trunk 設定ページで MTP を事前に割り当てておくことにより、SIP トランクを初期メディアとして設定する必要があります。MTP の詳細については、P.6-1 の「メディア リソース」の章を参照してください。

SIP トランクを使用したクラスタ間トランク

クラスタ間トランキングに SIP トランクを使用する主な利点の 1 つは、コール存続可能性です。ただし、H.323 トランクと比較した場合、SIP トランクは Secure Real-Time Transport Protocol（SRTP）や、Annex M1 を使用した QSIG Tunneling をサポートしません。

Cisco Unified CallManager Release 3.3 以降の H.323 トランクとは異なり、SIP トランクは単一の IP アドレスまたは DNS Server（SRV）レコードだけを指すことができます。DNS SRV 機能のないクラスタ間 SIP トランクにフェールオーバーおよびロード バランシングを提供するためには、複数の SIP トランクを設定します。さらに、その SIP トランクは、ルート グループおよびルート リストのメンバーになる必要があります。また、重要な点として、Cisco Unified CallManager が受け入れるコールが、設定済み SIP トランクのいずれかの宛先アドレスと IP アドレスが一致する SIP デバイスからのコールだけであることにも注意してください。さらに、SIP メッセージの着信ポート番号は、その SIP トランク用に設定されたポート番号と一致している必要があります。その結果、コールが着信する可能性のある、あらゆる遠端 SIP デバイスのすべての IP アドレスと一致するように、できるだけ多くの SIP トランクに宛先アドレスを設定するようにしてください。この方式は、複数の Cisco Unified CallManager クラスタがある場合には適さないため、その場合は DNS SRV で SIP トランクを使用することをお勧めします。図 5-6 は、DNS SRV を使用したクラスタ間 SIP トランク コールのコール フローを示しています。

図 5-6　DNS SRV を使用したクラスタ間 SIP トランクのコール フロー



注：DNS A ルックアップは、このコール フローから削除されています。

図 5-6 は、このコール フローにおける次の手順を示しています。

1. Cluster1 内の IP Phone が 87522001 にコールします。
2. コールはルート パターン 8752XXXX と一致し、このパターンは cluster2.foo.com の DNS SRV を使用した SIP トランクを指しています。Cluster1 の CCM3 は、このコールを処理するノードです。その SIP トランクはこのノードに登録されているためです。CCM3 は、cluster2.foo.com の DNS SRV ルックアップを送信します。
3. DNS サーバは、CCM-A.cluster2.foo.com と CCM-B.cluster2.foo.com の 2 つのレコードで応答します。CCM-A.cluster2.foo.com の方がプライオリティが高いので、コールはその Cisco Unified CallManager に対して試みられます。SIP Invite が送信される前に、CCM-A.cluster2.foo.com に関して別の DNS ルックアップが行われます。
4. CCM3 は、SIP Invite を 87522001@cluster2.foo.com に送信します。宛先アドレスは CCM-A の IP アドレスに設定されます。
5. Cisco Unified CallManager は、このコールをローカル コールとして解釈します。Uniform Resource Identifier（URI; ユニフォーム リソース識別子）のホスト部分が Cluster FQDN エンタープライズ パラメータと一致しているためです。Cluster2 には、CCM3 の宛先が設定された SIP トランクがありません。したがって、DNS SRV を使用して SIP トランクに設定されたすべてのドメインに対して、DNS SRV ルックアップを行います。その場合、例では cluster1.foo.com の DNS SRV の宛先を持つ単一のトランクが示されています。
6. DNS サーバは 2 つのエントリを返し、そのうちの 1 つが Invite の発信元 IP アドレスと一致します。クラスタはコールを受け入れ、内線 87522001 にコールをルーティングします。

CHAPTER 6

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（メディア ターミネーション ポイント）にストリームを渡す機能、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）、エコー キャンセレーション、シグナリング、TDM 回線からの音声ストリームの終端（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。

この章を使用して、以下で説明するメディア リソースが配置に必要かどうかを判断してください。また、必要なリソースがソフトウェアベースの機能で提供できるか、リソースを実装するために Digital Signal Processor（DSP; デジタル シグナル プロセッサ）をプロビジョニングする必要があるかを判断してください。リソースについては個別の項で説明しますが、上位機能を実装するために、同じ基本リソース（DSP と Cisco IP Voice Media Streaming Application）が共有されることがあります。

この章では、次の機能を中心に説明します。

- 音声インターフェイス（P.6-2）
- オーディオ会議（P.6-8）
- トランスコーディング（P.6-11）
- メディア ターミネーション ポイント（MTP）（P.6-14）
- Annunciator（P.6-20）
- Cisco RSVP Agent（P.6-22）
- Cisco IP Voice Media Streaming Application（P.6-22）

次の機能の詳細については、それぞれの項を参照してください。

- Music on Hold（P.7-1）
- Cisco Unified CallManager の RSVP 対応ロケーション（P.9-18）

ハードウェアおよびソフトウェアの依存関係の詳細については、P.6-23 の「ハードウェアおよびソフトウェアのキャパシティ」の項を参照してください。

Cisco Unified CallManager のメディア リソースは、メディア リソース グループおよびメディア リソース グループ リストを使用して制御できます。リソースのプールを作成すると、使用する特定のハードウェアまたはソフトウェアを制御できます。プールを使用して、物理的な場所に基づいてリソースをグループ化することをお勧めします。さまざまなコール処理モデルに基づく設計ガイドラインについては、P.6-25 の「一般的な設計ガイドライン」の項を参照してください。

音声インターフェイス

音声インターフェイスは、時分割多重（TDM）インターフェイス上のレッグと VoIP（Voice over IP）接続上のレッグの 2 つのコール レッグを持つコールに適用されます。TDM レッグは、コーディング/デコーディングとストリームのパケット化を実行するハードウェアで終端する必要があります。この終端機能は、同じハードウェア モジュール、ブレード、またはプラットフォーム上にあるデジタル シグナル プロセッサ（DSP）リソースによって実行されます。Cisco TDM ゲートウェイ上の DSP ハードウェアはすべて、音声ストリームを終端できます。また、特定のハードウェアは、会議やトランスコーディングなどの他のメディア リソース機能を実行することもできます（P.6-8 の「オーディオ会議」および P.6-11 の「トランスコーディング」を参照）。

表 6-2 ～表 6-6 は、各ハードウェア プラットフォームでサポートできるコールの数を示しています。この数は、ハードウェア上の DSP チップセットのタイプと DSP の個数によって決まります。ハードウェアには、アップグレードおよび変更ができない固定 DSP リソース、またはアップグレード可能なモジュラ DSP リソースのどちらかが搭載されています。表 6-2 ～表 6-6 は、モジュラ（アップグレード可能な）ハードウェアに関する、ハードウェア モジュールごとの DSP の最大数も示しています。

サポートされるコールの数は、コールに使用されるコーデックの計算の複雑度や、DSP に設定された複雑度モードによって異なります。Cisco IOS を使用すると、ハードウェア モジュールの複雑度モードを設定できます。ハードウェア プラットフォームの中には、中複雑度と高複雑度の 2 つの複雑度モードを持つものがありますが、中複雑度と高複雑度のほかにフレックス モードを持つものもあります。

中複雑度モードと高複雑度モード

モジュールでサポートできるコール数を確認するには、表 6-2 ～表 6-6 でモジュールを見つけ、モジュールに搭載できる DSP の個数と、必要なコーデック タイプを確認します。たとえば、フレックス モードに設定された 3 つの C2510 DSP を持つ NM-HD-2VE モジュールは、DSP ごとに 8 つの G.729 コールをサポートできます。合計すると、フレックス モードと G.729 コーデックを使用して 24 コールをサポートできます。フレックス モードで G.711 コーデックを使用する場合は、同じハードウェアで 48 コールをサポートできます。

表 6-1 に示されているように、コーデックが中複雑度モードでサポートされている場合、そのコーデックは高複雑度モードでもサポートされます。ただし、サポートされるコール数は減少します。

各 DSP は、中複雑度モード、高複雑度モード、またはフレックス モード（C5510 のみ）のいずれかとして個別に設定できます。DSP は、コールのコーデックに関する実際の複雑度に関係なく、設定されている複雑度に応じてすべてのコールを処理します。着信コールの実際の複雑度と同じかそれ以上の複雑度が設定されたリソースが使用可能になっている必要があります。そうでない場合、コールは失敗します。たとえば、コールに高複雑度コーデックが必要な場合、DSP リソースが中複雑度モードに設定されていると、コールは失敗します。ただし、高複雑度モードに設定された DSP に対して中複雑度コールが試行された場合、コールは成功し、Cisco IOS は高複雑度モードのリソースを割り当てます。

サポートされているコールの最大数を確認するには、目的のハードウェアを含む表 6-2 ～表 6-6 で該当する行を見つけます。表 6-1 で、中複雑度と高複雑度の列を調べて、目的のコーデックを処理できる複雑度モードを確認します。次に、目的の複雑度モードの列で、DSP ごとにサポートされているコールの最大数を確認します。

フレックス モード

フレックス モードは、C5510 チップセットを使用するハードウェア プラットフォーム上のみで使用可能で、このモードでは、設定時にコーデックの複雑度を指定する必要がありません。フレックス モードの DSP は、処理能力が足りる限り、サポートされているすべてのコーデック タイプのコールを受け入れます。各コールのオーバーヘッドは、Millions of Instructions Per Second（MIPS）単位の処理能力を計算することで動的にトラッキングされます。Cisco IOS は、受信されたコールごとに MIPS の計算を実行し、新しいコールが開始されるたびにそのバジェットから MIPS クレジットを差し引きます。表 6-1 の Flex Mode 列に示されているように、1 つのコールによって消費される MIPS 数は、コールのコーデックによって異なります。着信コールに必要な MIPS 以上の MIPS クレジットが残っている限り、DSP は新しいコールを許可します。表 6-1 の Flex Mode 列は、サポートされているコーデックをコールごとの MIPS 数別に分類し（コールごとに 15、30、または 40 MIPS）、各種ハードウェアに使用可能な MIPS バジェットを示しています。

フレックス モードは、同じハードウェアで複数のコーデックのコールをサポートする必要がある場合に便利です。これは、フレックス モードでは、DSP が中複雑度または高複雑度として設定されている場合よりも多くのコールをサポートできるためです。ただし、フレックス モードではリソースのオーバーサブスクリプションが許可されています。オーバーサブスクリプションになると、すべてのリソースが使用された場合にコール障害が発生するリスクが生じます。フレックス モードを使用すると、物理 TDM インターフェイスを使用する場合よりも DSP リソースの数を削減できます。

たとえば、各 DSP のバジェットは 240 MIPS となり、バジェットの合計は NM-HD-2VE モジュールごとに 720 MIPS となります。NM-HDV2 モジュールの場合、DSP ごとのバジェットは同じく 240 MIPS ですが、使用可能な MIPS の合計数については、選択項目や PVDM の数によって異なるため、表 6-2 で確認してください。

中複雑度モードまたは高複雑度モードと比べると、フレックス モードには、DSP ごとに最も多くの G.711 コールをサポートできるという利点があります。中複雑度モードでは、DSP は 8 つの G.711 コールをサポートできますが、フレックス モードでは 16 の G.711 コールをサポートします。

音声インターフェイスの DSP リソース

表 6-2 ～表 6-6 は、DSP チップセット別に分類されており、DSP サポートに関する情報を、プラットフォーム、DSP 密度、および DSP ごとにサポートされる音声インターフェイス（またはコール）の数別に示しています。表 6-1 は、ハードウェア モジュールでサポートされるコーデックを複雑度モードごとに示しています。

表 6-1　サポートされるコーデック（複雑度モード別）

中複雑度	高複雑度	フレックス モード
G.711（a-law、mu-law）	G.711（a-law、mu-law）	*コールごとに 15 MIPS の場合：* • G.711（a-law、mu-law） • FAX/ モデム パススルー • クリア チャネル *コールごとに 30 MIPS の場合：* • G.726（32K、24K、16K） • GSM-FR • FAX リレー • G.729 • G.729（a、b、ab） *コールごとに 40 MIPS の場合：* • G.728 • G.723.1（32K、24K、16K） • G.723.1a（5.3K、6.3K） • GSM-EFR • モデム リレー
FAX/ モデム パススルー	FAX/ モデム パススルー	
クリア チャネル	クリア チャネル	
G.726（32K、24K、16K）	G.726（32K、24K、16K）	
GSM-FR	GSM-FR	
FAX リレー	FAX リレー	
G.729（a、ab）	G.729	
	G.729（a、b、ab）	
	G.728	
	G.723.1（32K、24K、16K）	
	G.723.1a（5.3K、6.3K）	
	GSM-EFR	
	モデム リレー	

C5510 チップセットをベースとするハードウェアは、中複雑度モードと高複雑度モードのほか、フレックス モードをサポートします（表 6-2 を参照）。

表 6-2　C5510 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはシャーシ	DSP 構成	DSP およびモジュールごとの音声インターフェイス（コール）の最大数		
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 6 コール）	フレックス モード[1]（DSP ごとに 240 MIPS）
VG-224	4 DSP で固定	適用対象外	プラットフォームごとに 24 コール サポートされるコーデック： • G.711（a-law、mu-law） • G.729a	適用対象外
NM-HD-1V[2]	1 DSP で固定	NM ごとに 4 コール	NM ごとに 4 コール	NM ごとに 240 MIPS
NM-HD-2V	1 DSP で固定	NM ごとに 8 コール	NM ごとに 6 コール	NM ごとに 240 MIPS
NM-HD-2VE	3 DSP で固定	NM ごとに 24 コール	NM ごとに 18 コール	NM ごとに 720 MIPS
NM-HDV2 NM-HDV2-2T1/E1 NM-HDV2-1T1/E1	次の DSP を 1 ～ 4 つ： PVDM2-8[3]（½ DSP） PVDM2-16（1 DSP） PVDM2-32（2 DSP） PVDM2-48（3 DSP） PVDM2-64（4 DSP）	PVDM ごとのコール数： 4 8 16 24 32	PVDM ごとのコール数： 3 6 12 18 24	PVDM ごとの MIPS： 240 480 720 960

表 6-2　C5510 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース（続き）

ハードウェア モジュールまたはシャーシ	DSP 構成	DSP およびモジュールごとの音声インターフェイス（コール）の最大数		
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 6 コール）	フレックス モード[1]（DSP ごとに 240 MIPS）
2801 2811	次の DSP を 1 ～ 2 つ： PVDM2-8[3]（½ DSP）	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS： 120
	PVDM2-16（1 DSP）	4	3	240
	PVDM2-32（2 DSP）	8	6	480
	PVDM2-48（3 DSP）	16	12	720
	PVDM2-64（4 DSP）	24	18	960
		32	24	
2821 2851	次の DSP を 1 ～ 3 つ： PVDM2-8[3]（½ DSP）	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS： 120
	PVDM2-16（1 DSP）	4	3	240
	PVDM2-32（2 DSP）	8	6	480
	PVDM2-48（3 DSP）	16	12	720
	PVDM2-64（4 DSP）	24	18	960
		32	24	
3825 3845	次の DSP を 1 ～ 4 つ： PVDM2-8[3]（½ DSP）	PVDM ごとのコール数：	PVDM ごとのコール数：	PVDM ごとの MIPS： 120
	PVDM2-16（1 DSP）	4	3	240
	PVDM2-32（2 DSP）	8	6	480
	PVDM2-48（3 DSP）	16	12	720
	PVDM2-64（4 DSP）	24	18	960
		32	24	

1. フレックス モードでは、サポートされるコールの最大数は、コールごとに使用される MIPS 数によって異なります（表 6-1 を参照）。
2. NM-HD-1V モジュールを使用する場合、音声インターフェイス（コール）の数は、モジュール上の物理ポートの数によって制限されます。
3. PVDM2-8 のキャパシティは C5510 の半分です。

C5421 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定されている場合があります。表 6-3 は、DSP ごとのコール密度を、表 6-1 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-3　C5421 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 8 コール）	高複雑度（DSP ごとに 8 コール）
NM-HDA-4FXS	2 DSP で固定	NM ごとに 16 コール	NM ごとに 8 コール
	または		
	1 つの DSP-HDA-16（4 DSP）で固定	NM ごとに 16 コール	NM ごとに 16 コール
AIM-VOICE-30 AIM-ATM-VOICE-30	4 DSP で固定	AIM ごとに 30 または 60 コール	AIM ごとに 16 または 30 コール

C549 チップセットをベースとするハードウェアでは、DSP が中複雑度または高複雑度として設定されている場合があります。表 6-4 は、DSP ごとのコール密度を、表 6-1 は、複雑度モードごとにサポートされるコーデックを示しています。

表 6-4　C549 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール	DSP 構成	DSP およびモジュールごとのコールの最大数	
		中複雑度（DSP ごとに 4 コール）	高複雑度（DSP ごとに 2 コール）
NM-HDV NM-HDV-FARM	1 ～ 5 つの PVDM-12（PVDM-12 ごとに 3 つの DSP）	NM ごとに 12、24、36、48、または 60 コール	NM ごとに 6、12、18、24、または 30 コール
1751[1] 1760	次の DSP を 1 ～ 2 つ： PVDM-256K-4（1 DSP） PVDM-256K-8（2 DSP） PVDM-256K-12（3 DSP） PVDM-256K-16HD（4 DSP） PVDM-256K-20HD（5 DSP）	NM ごとのコール数： 4 または 8 8 または 16 12 または 24 16 または 32 20	NM ごとのコール数： 2 または 4 4 または 8 6 または 12 8 または 16 10
PA-VXA-1TE1-24+ PA-VXA-1TE1-30+ PA-VXB-2TE1+ PA-VXC-2TE1+	次の個数で固定： 7 DSP 8 DSP 12 DSP 30 DSP	PA ごとのコール数： 28 32 48 120	PA ごとのコール数： 14 16 24 60
PA-MCX-2TE1 PA-MCX-4TE1 PA-MCX-8TE1	固定（オンボード DSP なし）	PA-VX(*x*) によって異なる[2]	PA-VX(*x*) によって異なる[2]

1. 1751 は、最大 8 つの DSP（32 チャネル）をサポートします。また、これらのモジュールは、2 の倍数単位の PVDM を指定して発注できます。ただし、合計で 31 チャネルを超えることはできません。部品番号は、チャネル数を示しています。
2. マルチチャネル ポート アダプタは、混合バックプレーン全体で PA-VXA、PA-VXB、または PA-VXC の未使用の DSP を使用します。

C542 チップセットをベースとするハードウェアは、次のコーデックをサポートします。

- G.711（a-law、mu-law）
- FAX/ モデム パススルー
- クリア チャネル
- G.726（32K、24K、16K）
- GSM-FR
- FAX リレー
- G.729
- G.729（a、b、ab）
- G.728
- G.723.1（32K、24K、16K）
- G.723.1a（5.3K、6.3K）
- GSM-EFR
- モデム リレー

表 6-5 は、DSP ごとのコール密度を示しています。

表 6-5　C542 チップセットを持つ Cisco IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュール[1]	DSP 構成	DSP およびモジュールごとのコールの最大数
NM-1V	2 DSP で固定	DSP ごとに 1 コール NM ごとに 2 コール
NM-2V	4 DSP で固定	DSP ごとに 1 コール NM ごとに 4 コール

1. これらのモジュールは、複雑度モードを備えていませんが、すべてのコーデックを均等にサポートします。

表 6-6 は、DSP リソースに対応する非 IOS ハードウェアを示しています。すべての非 IOS ハードウェア プラットフォームでは、DSP 構成が固定されています（表 6-6 を参照）。

表 6-6　非 IOS ハードウェア プラットフォーム上の DSP リソース

ハードウェア モジュールまたはプラットフォーム	DSP 構成	DSP およびモジュールごとのコールの最大数	サポートされるコーデック
WS-6608-T1 WS-6608-E1	64 の C549 で固定 （ポートごとに 8 つの DSP）	DSP ごとに 2 コール モジュールごとに 256 コール[1]	G.711 a-law、mu-law G.729a
WS-6624-FXS	12 の C549 で固定	DSP ごとに 2 コール モジュールごとに 24 コール	G.711 a-law、mu-law G.729a
VG-248	12 の C5409 で固定	DSP ごとに 4 コール プラットフォームごとに 48 コール	G.711 a-law、mu-law G.729a
WS-SVC-CMM-ACT	4 つの Broadcom 1500 で固定	DSP ごとに 32 コール モジュールごとに 128 コール	G.711（10-30 ms） G.729（10-60 ms） G.723（30-60 ms）
WS-SVC-CMM-6T1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 144 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-6E1	12 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 180 コール	G.711（10、20、30 ms） G.729（10、20、30、40、50、60 ms）
WS-SVC-CMM-24FXS	3 の C5441 で固定	DSP ごとに 15 コール モジュールごとに 24 コール	G.711 a-law、mu-law G.729 G.729a
ATA-188[2]	1 つの Komodo 3880 で固定	プラットフォームごとに 2 コール	G.711 a-law、mu-law G.729

1. 物理ポートの数に基づいて、T1 の場合は最大 192 コール、E1 の場合は最大 240 コールが可能です。T1 または E1 に対して DSP が設定されていない場合は、最大 256 の DSP リソースが使用可能です。
2. ATA モジュールには複雑度が定義されていません。このモジュールは G.711、G.729、および G.723 のみをサポートします。

オーディオ会議

コンファレンス ブリッジとは、複数の参加者を 1 つのコールに参加させるリソースです。そのデバイス上で 1 つの会議に許可される最大ストリーム数まで、所定の会議用に任意の数の接続を受け入れることができます。会議に接続されているメディア ストリームと、その会議に接続されている参加者との間には、1 対 1 の対応があります。コンファレンス ブリッジは、ストリームを混合し、接続されている通話者ごとに固有の出力ストリームを作成します。所定の通話者の出力ストリームは、接続されている全通話者からのストリームの合成から、当事者の入力ストリームをマイナスしたものです。一部のコンファレンス ブリッジは、会議で通話量が最も多い 3 名の通話者だけを混合し、その合成ストリーム（通話量が最も多い通話者の 1 人である場合は、当事者の入力ストリームをマイナスしたもの）を各参加者に配信します。

オーディオ会議のリソース

ハードウェア コンファレンス ブリッジは、ソフトウェア コンファレンス ブリッジのすべての機能を備えています。さらに、一部のハードウェア コンファレンス ブリッジは、G.729、GSM、G.723 などの複数の低ビット レート（LBR）ストリーム タイプをサポートできます。この機能により、一部のハードウェア コンファレンス ブリッジが混合モードの会議を処理できるようになります。混合モードの会議では、ハードウェア コンファレンス ブリッジは、G.729、GSM、および G.723 のストリームを G.711 ストリームにトランスコードし、混合します。その後、混合したストリームを、ユーザに戻すために適切なストリーム タイプにエンコードします。一部のハードウェア コンファレンス ブリッジは、G.711 会議しかサポートしません。

Cisco Unified CallManager の制御下にあるすべてのコンファレンス ブリッジは、Cisco Unified CallManager との通信に Skinny Client Control Protocol（SCCP）を使用します。

Cisco Unified CallManager は、Cisco Unified CallManager クラスタに登録されている会議リソースから、コンファレンス ブリッジを割り当てます。ハードウェアとソフトウェアの両方の会議リソースを同時に Cisco Unified CallManager に登録でき、Cisco Unified CallManager は、どちらのリソースからでも、コンファレンス ブリッジを割り当て、使用することができます。Cisco Unified CallManager は、会議割り当て要求を処理するときに、これらのコンファレンス ブリッジのタイプを区別しません。

リソースがサポートできる会議の数、および 1 つの会議の最大参加者数は、リソースによって異なります。

Cisco Unified CallManager システムでは、次のタイプのコンファレンス ブリッジ リソースが使用されます。

- ソフトウェア オーディオ コンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）（P.6-9）
- ハードウェア オーディオ コンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 シリーズおよび 3800 シリーズ ルータ）（P.6-9）
- ハードウェア オーディオ コンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）（P.6-10）
- ハードウェア オーディオ コンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）（P.6-10）
- ハードウェア オーディオ コンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）（P.6-10）
- 組み込み会議（P.6-10）

ソフトウェア オーディオ コンファレンス ブリッジ（Cisco IP Voice Media Streaming Application）

ソフトウェア ユニキャスト コンファレンス ブリッジは、G.711 音声ストリームと Cisco Wideband オーディオ ストリームを混合できる標準の会議ミキサーです。Wideband または G.711 a-law および mu-law ストリームの任意の組み合せが、同じ会議に接続される場合があります。所定の設定でサポートできる会議数は、コンファレンス ブリッジ ソフトウェアが実行されるサーバと、アプリケーションで有効になっている他の機能によって決まります。Cisco IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ではすべての機能を同時に考慮する必要があります（P.6-22 の「Cisco IP Voice Media Streaming Application」を参照）。

ハードウェア オーディオ コンファレンス ブリッジ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 シリーズおよび 3800 シリーズ ルータ）

Cisco IOS で会議リソースとして設定されている DSP は、会議機能のみに特化した DSP にファームウェアをロードします。このような DSP は、他のメディア機能には使用できません。

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- C5510 DSP チップセットに基づき、NM-HDV2 およびルータ シャーシは PVDM2 モジュールを使用して DSP を提供します。
- PVDM2 ハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つの PVDM の複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててから、必要に応じて他の機能に割り当ててください。
- NM-HDV2 には、任意の組み合せで PVDM2 モジュールを取り付け可能な 4 つのスロットがあります。その他のネットワーク モジュールの DSP 数は固定されています。
- これらの DSP に基づく会議には、最大 8 人が参加できます。会議が始まるときに、8 つのポジションのすべてが予約されます。
- PVDM2-8 には、PVDM2-16 と比較して処理キャパシティが半分の DSP があるため、½ DSP と表示されています。たとえば、PVDM2-8 の DSP が G.711 用に設定されている場合、(0.5 * 8) ブリッジ /DSP = 4 コンファレンス ブリッジを提供できます。
- 表 6-1 および表 6-2 を使用して、特定のハードウェアでプロビジョニングできる DSP の数を判断してください。
- Cisco IOS の DSP ファーム設定によって、ファームで受け付けることができるコーデックを指定します。会議および G.711 用に設定されている DSP ファームは、8 つの会議を提供します。G.711 コールと G.729 コールの両方を受け付けるように設定されている場合、ストリームのトランスコーディングの実行用にリソースが予約されるため、1 つの DSP で 2 つの会議が提供されます。
- NM-HDV2 の I/O は 400 ストリームに制限されています。そのため、割り当てられている会議リソースの数がこの制限を超えないように注意してください。G.711 会議が設定されている場合、（48　～8）参加者 = 384 ストリームになるため、1 つの NM に割り当てることができる DSP は 48 までです。すべての会議を G.711 コーデックと G.729 コーデックの両方に設定した場合、各 DSP は、参加者がそれぞれ 8 人の会議を 2 つだけ提供します。この場合、NM がフル装備され、16 の DSP が設定されると、256 ストリームが可能になります。
- 会議は、GSM コーデックを利用したコールをネイティブに受け付けることはできません。これらのコールが会議に参加するには、個別にトランスコーダが必要です。
- NM-HDV2 などの PVDM2 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。

ハードウェア オーディオ コンファレンス ブリッジ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアの DSP は、音声インターフェイス、会議、メディア ターミネーション、またはトランスコーディングとして個別に設定されます。そのため、1 つのモジュールの複数の DSP を異なるリソース タイプとして使用できます。DSP は、まず音声インターフェイスに割り当ててください。
- この Cisco Catalyst ベースのハードウェアには、ブリッジごとに 32 人まで参加できるコンファレンス ブリッジを提供できる DSP リソースが用意されています。
- 各モジュールには、個別に設定可能な 4 つの DSP が含まれています。各 DSP は、32 のコンファレンス ブリッジをサポートします。
- これらのコンファレンス ブリッジでは、追加のトランスコーダ リソースなしで、G.711 コーデックおよび G.729 コーデックがサポートされます。ただし、その他のコーデックを使用する場合は、トランスコーダ リソースが必要になることがあります。

ハードウェア オーディオ コンファレンス ブリッジ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。
- このハードウェアを使用する会議は、1 つのブリッジで 6 人まで参加可能なブリッジを提供します。
- リソースは DSP ごとにコンファレンス ブリッジとして設定されます。
- NM-HDV は 4 つまでの PVDM-256K モジュールを使用でき、Cisco 1700 シリーズ ルータは、1 つまたは 2 つの PVDM-256K モジュールを使用できます。
- 各 DSP は、G.711 コールまたは G.729 コールを受け付け可能な 1 つのコンファレンス ブリッジを提供します。
- Cisco 1751 は、シャーシ 1 つで 5 つの電話会議に制限されています。Cisco 1760 は、シャーシごとに 20 の電話会議をサポートします。
- NM-HDV2 などの PVDM2 ベースのハードウェアは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。PVDM-256K および PVDM2 に基づく DSP は、異なる DSP ファーム設定を持つため、ルータで同時に設定できるのは 1 つだけです。

ハードウェア オーディオ コンファレンス ブリッジ（Cisco Catalyst WS-X6608-T1 および WS-X6608-E1）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアには、物理的にそれぞれのポートに関連付けられた 8 つの DSP があり、カードごとに 8 つのポートがあります。DSP の設定はポート レベルで行われるため、1 つのポートに関連付けられているすべての DSP が同じ機能を実行します。
- コンファレンス ブリッジには最大 32 人が参加でき、各ポートが 32 のコンファレンス ブリッジをサポートします。
- G.711 または G.723 の会議では、ポートごとに 32 の会議が可能です。G.729 コールを使用する場合は、ポートごとに 24 の会議が可能です。

組み込み会議

一部の電話機モデルには、3 方向の会議を可能にする組み込み会議リソースが用意されています。このブリッジは、割り込み機能によってのみ呼び出され、通常の会議リソースとしては使用されません。このブリッジが用意されている電話機の詳細については、P.19-1 の「IP テレフォニー エンドポイント」を参照してください。このブリッジは、G.711 コールのみを受け付けます。

トランスコーディング

トランスコーダは、あるコーデックからの入力ストリームを、別のコーデックを使用する出力ストリームに変換するデバイスです。同じコーデックを異なるサンプリング レートで利用する 2 つのストリームを接続することもできます。Cisco Unified CallManager システムでは、通常、G.711 音声ストリームと低ビットレート圧縮音声ストリームの G729a との間の変換を行うために、トランスコーダを使用します。次の場合には、どのようなときにトランスコーダ リソースが必要かが決まります。

- システム全体で単一のコーデックが使用されている。

  システムのすべてのコールに対して単一のコーデックが設定されている場合、トランスコーダ リソースは必要ありません。G.711 コーデックは、すべてのベンダーでサポートされています。単一サイトの配置では、通常、帯域幅を節約する必要がなく、単一のコーデックを使用できます。このシナリオで最も一般的に選択されるのは G.711 です。

- システムで複数のコーデックが使用され、すべてのエンドポイントがすべてのコーデック タイプに対応している。

  複数のコーデックを使用する最も一般的な理由は、LAN コールには G.711 を使用してコール品質を最大にし、帯域幅が制限されている WAN を通過するコールには低帯域幅コーデックを使用して帯域幅効率を最大にするためです。低帯域幅コーデックには、G.729a を使用することをお勧めします。G.729a は、すべての Cisco Unified IP Phone モデル、およびその他のほとんどの Cisco Unified Communications デバイスでサポートされるため、トランスコーディングの必要がなくなります。Cisco Unified CallManager では、リージョン間でその他の低帯域幅コーデックも設定できますが、現在の電話機モデルはこのコーデックをサポートしないため、トランスコーダが必要になります。ゲートウェイへのコールには 1 つのトランスコーダが必要で、別の IP Phone へのコールには 2 つのトランスコーダが必要です。すべてのデバイスが G.711 と G.729 の両方をサポートし、両方で設定されている場合は、デバイスがコールごとに適切なコーデックを使用するため、トランスコーダを使用する必要はありません。

- システムで複数のコーデックが使用され、一部のエンドポイントが G.711 だけをサポートしているか、または G.711 だけを使用するように設定されている。

  この条件は、システムで G.729a を使用し、このコーデックをサポートしないデバイスがある場合、または G.729a をサポートするデバイスが G.729a を使用するように設定されていない場合に発生します。この場合はトランスコーダが必要です。サードパーティ ベンダーのデバイスは、G.729 をサポートしない場合があります。また、G.729 をサポートしていても、Cisco Unity で設定されていないということもあります。Cisco Unity は G.729a でのコールの受け付けをサポートしますが、コーデックはソフトウェアで実装され、CPU に負荷がかかります。同時に 10 のコールが発生するだけで CPU 使用率が高くなるため、多くの配置では Cisco Unity で G.729 を無効にして、Unity サーバの外にある専用のトランスコーディング リソースにトランスコーディング機能の負荷を分散します。システムに Cisco Unity が含まれている場合は、Unity で G.729a コールを受け付けるか、または G.711 だけを使用するように設定するかを決定します。

(注) Cisco Unified MeetingPlace Express は、現在、G.711 だけをサポートしています。Cisco Unified MeetingPlace Express へのコールに対して G.729 が設定されている環境では、トランスコーダ リソースが必要です。

設計を最終決定するには、必要なトランスコーダの数と、トランスコーダを配置する場所を検討する必要があります。複数のコーデックが必要な場合は、すべてのコーデックをサポートしないエンドポイントの数、これらのエンドポイントを配置する場所、これらのリソースにアクセスする他のグループ、これらのデバイスがサポートする同時コールの最大数、およびネットワーク上でこれらのリソースを配置する場所を検討する必要があります。

トランスコーディング リソース

トランスコーディングを実行するには、DSP リソースが必要です。これらの DSP リソースは、音声モジュール、および次の項で示すトランスコーディング用のハードウェア プラットフォームに配置することができます。

ハードウェア トランスコーダ（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800、および 3800 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a または G.729ab との間で使用できます。1 つの DSP で 8 セッションをサポートできます。
- Cisco Unified IP Phone は、G.729 コーデックの G.729a バリアントだけを使用します。新規 DSP ファーム プロファイルのデフォルトは、G.729a/G.729ab/G.711u/G.711a です。単一の DSP が同時に提供できる機能は 1 つだけなので、プロファイルで設定する最大セッション数は、リソースを無駄にしないように、8 の倍数で指定する必要があります。
- トランスコーディングは、G.711mu-law/G.711a-law と G.729/G729b との間でも使用できますが、通常、Cisco Unified CallManager システムでは使用されません。1 つの DSP で 6 セッションをサポートできます。
- 特定のプラットフォームまたはネットワーク モジュールで使用できる DSP の数を確認するには、P.6-3 の「音声インターフェイスの DSP リソース」の項を参照してください。

ハードウェア トランスコーダ（Cisco WS-SVC-CMM-ACT）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729b、または G.723 との間で使用できます。
- 1 つの ACT ごとに、個別に DSP プールに割り当て可能な 4 つの DSP があります。
- CCM-ACT は、DSP ごとに 16（ACT ごとに 64）のトランスコーディングされたコールをサポートします。ACT は、リソースをコールではなくストリームとしてレポートします。単一のトランスコーディングされたコールは、2 つのストリームで構成されます。

ハードウェア トランスコーダ（Cisco NM-HDV および 1700 シリーズ ルータ）

これらの DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- このハードウェアは、C549 DSP チップセットに基づく PVDM-256K タイプのモジュールを利用します。
- NM-HDV は、4 つまでの PVDM-256K モジュールを使用できます。Cisco 1700 シリーズ ルータは、1 ～ 2 の PVDM-256K モジュールを使用できます。
- NM-HDV モジュールと NM-HDV2 モジュールは、単一のシャーシで同時に音声インターフェイスに使用できますが、同時に他のメディア リソース機能には使用できません。会議、MTP、またはトランスコーディングに対して同時にアクティブにできる DSP ファームのタイプは 1 つだけです（NM-HDV または HM-HDV2）。
- G.711 mu-law または a-law から G.729、G.729a、G.729b、G.729ab、または GSM コーデックへのトランスコーディングがサポートされます。
- 1 つの DSP で 2 つのトランスコーディング セッションを提供できます。
- Cisco 1751 のシャーシは 16 セッションに制限されています。Cisco 1760 のシャーシは 20 セッションに制限されています。

ハードウェア トランスコーダ（Cisco WS-X6608）

この DSP リソースには、次のガイドラインおよび考慮事項が適用されます。

- DSP はポート レベルで機能に割り当てられます。1 つのポートで 24 のトランスコーディング セッションを提供できます。
- ブレードごとに 8 つのポートがあります。
- トランスコーディングは、G.711 mu-law または a-law と G.729a、G.729ab、G.729、または G.729b との間で使用できます。

トランスコーダは、メディア ターミネーション ポイント（MTP）と同じ機能も実行できます。トランスコーダ機能と MTP 機能の両方が必要な場合、トランスコーダがシステムによって割り当てられます。MTP 機能が必要な場合、Cisco Unified CallManager はトランスコーダまたは MTP をリソース プールから割り当てます。リソースの選択は、P.6-25 の「メディア リソース グループとメディア リソース グループ リスト」の項に説明があるように、メディア リソース グループによって決まります。

メディア ターミネーション ポイント（MTP）

メディア ターミネーション ポイント（MTP）は、2 つの全二重 G.711 ストリームを受け入れるエンティティです。MTP は、この 2 つのメディア ストリームをブリッジします。また、これらのメディア ストリームは、個々にセットアップと終了ができるようになります。ある接続の入力ストリームから受信されるストリーミング データは、他の接続の出力ストリームに渡され、逆も同様です。次の項で説明するように、MTP には多くの用途があります。

ストリームの再パケット化

MTP は、a-law から mu-law（およびその逆）にトランスコードしたり、パケット化にかかる時間が異なる（使用するサンプル サイズが異なる）2 つの接続をブリッジしたりすることができます。

H.323 補足サービス

MTP は、補足サービスに使用され、Empty Capabilities Set（ECS）機能を使用している H.323v2 の OpenLogicalChannel および CloseLogicalChannel 要求機能をサポートしていない H.323 エンドポイントの機能を拡張することができます。この要件はあまり発生しません。Cisco H.323 エンドポイント、およびほとんどのサードパーティのエンドポイントが ECS をサポートしています。必要に応じて、MTP が割り当てられ、H.323 エンドポイントに代わってコールに接続されます。メディア ストリームは、挿入された後、MTP と H.323 デバイス間で接続され、これらの接続は、コールの期間中、存在します。MTP のもう一方の側に接続されるメディア ストリームは、保留、転送などの機能を実行するために、必要に応じて接続されたり、接続解除されたりします。

MTP が H.323 コールで要求され、使用できるものがない場合、コールは処理されますが、補足サービスを呼び出すことはできません。

H.323 発信時の Fast Start

H.323 では、Fast Start という機能が定義されています。これは、コール セットアップ時に交換されるパケット数を削減し、メディアを確立する時間を短縮する機能です。H.323 を利用する 2 つのデバイスのネットワーク遅延が高いとき、この遅延がメディアを確立する時間に影響を与えるため、この機能が役立ちます。Cisco Unified CallManager は、コール セットアップの方向に基づき、着信 Fast Start と発信 Fast Start を区別します。MTP 要件が同じではないため、この区別は重要です。着信 Fast Start の場合、MTP は必要ありません。H.323 トランクの発信コールは、Fast Start が有効なとき、MTP を必要とします。問題になるのは、多くの場合、着信コールだけです。問題を解決するには、発信 Fast Start を有効にせずに着信 Fast Start を使用します。

Named Telephony Event（RFC 2833）

コール中に DTMF トーンを使用して、メニュー システムのナビゲート、データの入力、またはその他の操作の目的で、遠端のデバイスに信号を送信できます。これらは、コール制御の一部としてコール セットアップ中に送信される DTMF トーンとは異なる方法で処理されます。

RFC 2833 で定義されている Named Telephony Event（NTE）は、コール メディアが確立された後で、あるエンドポイントから別のエンドポイントに DTMF を送信する方式です。トーンは、すでに確立されている RTP ストリームを使用して、パケット データとして送信されます。これは、RTP パケット タイプ フィールドによって、オーディオとは区別されます。たとえば、コールのオーディオは、G.711 データとして識別する RTP パケット タイプを使用してセッションで送信されます。DTMF パケットは、NTE として識別する RTP パケット タイプを使用して送信されます。ストリームの受信側は、G.711 パケットと NTE パケットを別々に利用します。

Named Telephony Event がメディア ターミネーション ポイントを必要とする条件

Cisco Unified CallManager 4.x では、SIP トランクだけがサポートされ、SIP トランクを使用するすべてのコールに MTP が割り当てられる必要があります。SIP トランクには設定パラメータ「MTP required」があります。これはデフォルトで選択されいて、変更できません。

Cisco Unified CallManager 5.0 では、回線デバイスの SIP サポートが追加され、SIP トランクを使用するすべてのコールに MTP を割り当てる必要がなくなりました。Cisco Unified CallManager 5.0 で MTP が必要になるのは、2 つのエンドポイントの間で DTMF を送信する共通の方式がない場合、またはシステム設定で MTP を割り当てるように指定した場合です。次の説明は非常に詳細に述べたものであり、Cisco Unified CallManager 5.0 だけに適用されます。

次の規則に基づいて、システムに対して計画されているエンドポイントのタイプを確認します。

1. SIP 以外のエンドポイントが 2 つの場合、MTP は必要ありません。

   SIP 以外のすべての Cisco Unified Communications エンドポイントは、さまざまなシグナリング パスによって、DMTF を Cisco Unified CallManager に送信します。Cisco Unified CallManager は、異なるエンドポイント間で DTMF を転送します。たとえば、IP Phone は Cisco Unified CallManager への SCCP メッセージを使用して DTMF を送信します。次に、DTMF は H.245 シグナリング イベントによって H.323 ゲートウェイに送信されます。2 つのエンドポイントには、Cisco Unified CallManager に DTMF を送信する共通の方式を持っています。SIP エンドポイントを使用しない場合は、これで終了です。

2. Cisco SIP エンドポイントが 2 つの場合、MTP は必要ありません。

   すべての Cisco SIP エンドポイントは NTE をサポートするため、MTP は完全に排除できます。DTMF は NTE を使用して、エンドポイント間で直接送信されます。すべてのエンドポイントが Cisco SIP デバイスの場合、DTMF を変換する MTP は必要ありません。

3. SIP エンドポイントと SIP 以外のエンドポイントの組み合せの場合、MTP が必要になることがあります。

   使用するデバイスで NTE がサポートされているかどうかを確認するには、表 6-7 を参照してください。RFC 2833 は SIP に限定されていないため、その他のコール制御プロトコルを使用するデバイスでサポートされていることがあります。たとえば、SCCP または SIP スタックを実行する Cisco Unified IP Phone は、両方のモードで NTE をサポートします。一部のデバイスは、複数の方式で DTMF をサポートします（たとえば、SCCP スタックを使用する Cisco Unified IP Phone 7960 は、NTE を他のデバイスに送信することも、SCCP を Cisco Unified CallManager に送信することもできます）。Cisco Wireless IP Phone 7920 など別のデバイスは SCCP だけを送信でき、さらに別のデバイスは NTE だけを送信できます（SIP スタックを使用する Cisco Unified IP Phone 7960 など）。Cisco Unified CallManager は、エンドポイントのペアの機能に基づき、MTP をコール単位に動的に割り当てることができます。表 6-7 を使用して、MTP をプロビジョニングする必要があるかどうかを判断してください。

4. MTP の動的割り当ては、発信コールだけに適用されます。

   MTP を必要としない SIP トランクは、規則 3 で説明したように動的割り当てを使用します。SIP トランクは、Invite に Session Description Protocol（SDP）を使用しているコールと使用していないコールの両方を受け付けることができるため、着信コールには MTP を割り当てません。上で説明したように、発信コールにだけ MTP が割り当てられます。特定の SIP トランクを着信コールだけに使用する場合、そのトランクのコールを受信するためにシステムの MTP リソースを割り当てる必要はありません。

5. 設定により、MTP が強制的に割り当てられることがあります。

   Cisco Unified CallManager 5.0 では、SIP トランク パラメータ **MTP Required** がデフォルトで選択されておらず、フィールドはロック解除されています。SIP トランクが Cisco のデバイス（SIP ゲートウェイなど）用に定義されている場合、デバイスは NTE をサポートするように設定する必要があります。通常は、MTP Required のデフォルト設定を使用し、必要な場合にだけ MTP を割り当てます。

他の理由で MTP が強制的に割り当てられることもあります。コール セットアップが開始する前に MTP が割り当てられると、SIP ダイアログ確立の動作が変わります。SIP は Session Description Protocol（SDP）を使用してセッション パラメータを確立し、SDP は SIP メッセージに埋め込まれます。MTP を強制すると、コールを開始する Invite メッセージと共に SDP が送信されます。MTP が強制されない場合、Invite メッセージの後で（必要な場合）割り当てられます。SDP は Invite メッセージに含まれず、コール セットアップの後の時点で送信されます。遠端のデバイスが、SDP が埋め込まれた Invite メッセージだけをサポートする場合は、MTP Required パラメータをオン（有効）にする必要があります。

この設定パラメータによって MTP が強制割り当てされる場合は、MTP から遠端の SIP デバイスへのコール レッグで使用されるコーデックが G.711 mu-law または a-law である必要があります。MTP Required を選択するとロック解除されるトランク設定の追加パラメータがあります。このパラメータによって、使用する G.711 のバリアントを選択できます。この設定パラメータによって MTP が強制割り当てされなかった場合は、コーデックを判断する通常のメカニズムが適用されます。

（注） **MTP Required** の設定によって MTP をメディア ストリームに配置すると、MTP リソースの Cisco IP Voice Media Streaming Application または Cisco IOS Release 12.4(6)T 以降を使用する CMM-ACT モジュールが使用されることがあります。この制限は、複数の方式で DTMF を送信するエンドポイントによるものです（たとえば、Cisco Unified IP Phone 7960 は、SCCP イベントと NTE イベントを同時に送信します）。現在、ここで示した MTP だけが、このような状況に対処します。

表 6-7　DTMF 方式をサポートするエンドポイント

エンドポイント プロトコル スタック：エンドポイント	DTMF 方式		
	SCCP	NTE	KPML[1]
SCCP スタック 12SP+、30 VOIP、 7910, 7920, 7935, 7936 VG248、 DPA-7610、DPA-7630、 CTI ポート、ファーストパーティ制御	あり	なし	なし
SCCP スタック 7902, 7905, 7912,7940, 7941, 7960, 7961, 7970 将来の新しい電話機モデル	あり	あり	なし
SIP スタック 7905, 7911, 7912, 7940, 7941, 7960, 7961, 7970 将来の新しい電話機モデル	なし	あり	あり（7911、7941、7961、7970） なし（7905、7912、7940、7960）

1. Key Press Markup Language（KPML）

（注）IP Phone は、DTMF を SCCP 経由で受信した場合、エンドユーザに対して DTMF を再生しますが、NTE で受信したトーンは再生しません。ただし、DTMF を別のエンドユーザに送信する必要はありません。DTMF を必要とするエンドポイント（公衆網ゲートウェイ、アプリケーション サーバなど）と対応するコールを発信するエンドポイントについてのみ検討する必要があります。

例 6-1　NTE 変換用に MTP を必要とするコール フロー

例として、ファーストパーティ制御の CTI ルート ポイントがあり（CTI ポートがメディアの終端）、IVR メニューをナビゲートするために DTMF を使用するシステムに統合されているシステムを考えます。システムのすべての電話機が SCCP を実行している場合、MTP は必要ありません。この場合、Cisco Unified CallManager が CTI ポートを制御し、IP Phone からの DTMF を SCCP 経由で受信します。Cisco Unified CallManager が、DTMF 変換を提供します。

ただし、SIP スタックを実行している電話機がある場合は、MTP が必要です。NTE はメディア ストリームの一部なので、Cisco Unified CallManager は受信しません。MTP がメディア ストリームの中に呼び出され、SCCP を使用する 1 つのコール レッグと NTE を使用する 2 番目のコール レッグを持ちます。MTP は Cisco Unified CallManager の SCCP 制御下にあり、Cisco Unified CallManager の制御下で NTE から SCCP への変換を実行します。

SIP および H.323 ゲートウェイでの DTMF の設定

SIP ダイヤル ピアの下での方式として **sip-notify** または **rtp-nte** を設定します。SIP ダイヤル ピアの最適な設定は、システムに存在するエンドポイントの混在状況によって異なります（表 6-7 を参照）。ゲートウェイで Unsolicited Notify を使用する場合、MTP リソースを必要とせずに、SCCP をサポートするエンドポイントでダイヤル ピアを使用できます。NTE だけをサポートするエンドポイントは、ゲートウェイを使用するために、MTP を呼び出す必要があります。

逆に、SIP ダイヤル ピアで NTE が設定されている場合は、NTE を使用できるすべてのエンドポイントが、MTP を必要とせずにゲートウェイに DTMF を直接送信できます。SCCP だけをサポートするエンドポイントは、MTP を呼び出す必要があります。

SIP ゲートウェイは、NTE、Unsolicited Notify、またはメディア ストリームのオーディオ トーンを使用して DTMF を送信できます。Unsolicited Notify はシスコ固有の方式で、DTMF トーンを含むイベントと共に SIP Notify メッセージを送信します。この方式は、Cisco Unified CallManager でもサポートされます。

次の例は、Named Telephony Event 用の SIP ゲートウェイ設定を示しています。

```
dial-peer voice 10 voip
dtmf-relay rtp-nte
```

Cisco IOS SIP ゲートウェイは、現在、Key Press Markup Language（KPML）をサポートしていません。

H.323 ゲートウェイは、H.245 Alphanumeric、H.245 Signal、NTE、およびメディア ストリームのオーディオをサポートします。現時点では H.323 を使用する Cisco Unified CallManager において、NTE オプションはサポートされていないため、使用できません。これに適したオプションは H.245 Signal です。他のエンドポイントに Cisco Unified CallManager と共通のシグナリング機能がない場合、H.323 ゲートウェイへのコールを確立するために、MTP が必要です。たとえば、SIP スタックを実行している Cisco Unified IP Phone 7960 は NTE だけをサポートするため、H.323 ゲートウェイを使用する場合は MTP が必要です。

H.323 ゲートウェイでの DTMF 方式に推奨される設定を示します。

```
dial-peer voice 10 voip
dtmf-relay h.245-signal
```

（注）SIP デバイスは、Key Press Markup Language（KPML）という DTMF を送信する別の方式をサポートしていることがあります。多くのシスコ製電話機は KPML をサポートしていますが、まだ広くサポートされてはいません。Cisco IOS SIP ゲートウェイは、Cisco IOS Release 12.4(4)T の時点では KPML をサポートしていませんが、間もなくサポートが追加される予定です。追加された時点で、Unsolicited Notifies の代わりにゲートウェイで KPML を使用できるようになります。

CTI ルート ポイント

電話コールのファーストパーティ制御を持つ CTI ルート ポイントは、コールのメディア ストリームに参加し、MTP の挿入を必要とします。CTI がコールのサードパーティ制御を持つ場合（メディアが CTI で制御されているデバイスを通過するなど）、MTP が必要かどうかは制御されるデバイスの機能によって異なります。

MTP リソース

次のタイプのデバイスは、MTP として使用できます。

ソフトウェア MTP（Cisco IP Voice Media Streaming Application）

ソフトウェア MTP とは、サーバに Cisco IP Voice Media Streaming Application をインストールすることによって設定されるデバイスです。インストールされたアプリケーションが、MTP アプリケーションとして設定されると、そのアプリケーションは、Cisco Unified CallManager ノードに登録され、サポートする MTP リソース数を Cisco Unified CallManager に知らせます。ソフトウェア MTP デバイスは、G.711 ストリームだけをサポートします。IP Voice Media Streaming Application は、複数の機能に使用することもできるリソースで、設計ガイダンスではすべての機能を同時に考慮する必要があります（P.6-22 の「Cisco IP Voice Media Streaming Application」を参照）。

ソフトウェア MTP（Cisco IOS に基づく）

- ルータでソフトウェアベースの MTP を提供する機能は、Cisco 3800 シリーズ ルータでは Cisco IOS Release 12.3(11)T、その他のルータ モデルでは Release 12.3(8)T4 から使用できるようになりました。
- この MTP によって、G.711 mu-law および a-law、G.729a、G.729、G.729ab、G.729b、GSM、およびパススルーのコーデックを設定できます。ただし、同時に設定できるコーデックは 1 つだけです。一部のコーデックは、Cisco Unified CallManager の実装には関係しません。
- ルータ設定では、最大 500 の個別ストリームが可能で、250 のトランスコーディングされたセッションをサポートします。この数の G.711 ストリームを使用すると、5 MB のトラフィックが生成されます。

ハードウェア MTP（Cisco NM-HDV2、NM-HD-1V/2V/2VE、2800 および 3800 シリーズ ルータ）

- このハードウェアは、PVDM-2 モジュールを使用して DSP を提供します。
- 各 DSP は、16 の G.711 mu-law または a-law MTP セッション、または 6 つの G.729、G.729b、または GSM MTP セッションを提供できます。

ハードウェア MTP（Cisco WS-SVC-CMM-ACT）

- このモジュールには、個別に設定できる 4 つの DSP があります。
- 各 DSP は、128 の G.729、G.729b、または GSM MTP セッション、または 256 の G.711 mu-law または a-law MTP セッションをサポートします。

ハードウェア MTP（Catalyst WS-X6608-T1 および WS-X6608-E1）

- サポートされるコーデックは、G.711 mu-law または a-law、G.729、G.720b、または GSM です。
- 設定はポート レベルで行います。モジュールごとに 8 つのポートを使用できます。
- MTP リソースとして設定されたポートごとに、24 のセッションが提供されます。

Annunciator

Annunciator 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。この機能は、複数の片方向 RTP ストリームを Cisco IP Phone やゲートウェイなどのデバイスに送信できます。さらに、SCCP メッセージを使用して、RTP ストリームを確立します。この機能を使用するには、デバイスが SCCP に対応している必要があります。トーンとアナウンスは、システムで事前に定義されています。アナウンスでは、ローカリゼーションがサポートされています。また、適切な .wav ファイルを置き換えて、アナウンスをカスタマイズすることもできます。Annunciator は、トランスコーディング リソースを使用しないで、G.711 a-law および mu-law、G.729、および Wideband コーデックをサポートすることができます。

次の機能には、Annunciator リソースが必要です。

- Cisco Multilevel Precedence Preemption（MLPP）

  この機能には、次のようなコール障害の状態に応じて再生されるストリーミング メッセージが用意されています。

  - 優先順位の高い既存のコールが原因で、プリエンプション処理できない。
  - 優先順位アクセス制限に到達した。
  - 試行された優先順位レベルが許可されていない。
  - 着信番号が、プリエンプション処理またはコール ウェイティングに対応していない。

- SIP トランクを介した統合

  SIP エンドポイントには、トーンを生成し、RTP ストリームでインバンドで送信する機能があります。SCCP デバイスにはこの機能がないため、SIP エンドポイントと統合した場合、DTMF トーンの生成または受け入れ時には Annunciator と MTP が併用されます。次のタイプのトーンがサポートされます。

  - コールプログレストーン（ビジー、アラート、およびリングバック）
  - DTMF トーン

- Cisco IOS ゲートウェイとクラスタ間トランク

  これらのデバイスには、コールプログレストーン（リングバック トーン）のサポートが必要です。

- システム メッセージ

  次のようなコール障害の状態では、システムはエンドユーザにストリーミング メッセージを再生します。

  - ダイヤル番号をシステムが認識できない。
  - サービスが中断したためコールがルーティングされない。
  - 番号が通話中で、その番号がプリエンプション処理またはコール ウェイティング用に設定されていない。

- 会議

  電話会議の間、システムは、参加者がブリッジに参加、またはブリッジから退出したことをアナウンスするときに、割り込み音を再生します。

Cisco IP Voice Media Streaming Application をサーバ上でアクティブにすると、Annunciator がシステム内に自動的に作成されます。Media Streaming Application を非アクティブにすると、Annunciator も削除されます。単一の Annunciator インスタンスは、パフォーマンス要件を満たす場合は、Cisco Unified CallManager クラスタ全体にサービスを提供できます（P.6-21 の「Annunciator のパフォーマンス」を参照）。そうでない場合は、追加の Annunciator をクラスタ用に設定する必要があります。追加の Annunciator を設定するには、クラスタ内の他のサーバ上で Cisco IP Voice Media Streaming Application をアクティブにします。

Annunciator は、そのデバイス プールで定義されたとおり、一度に 1 つの Cisco Unified CallManager に登録されます。デバイス プールに対してセカンダリが設定されている場合、Annunciator は自動的にセカンダリ Cisco Unified CallManager にフェールオーバーします。障害発生時に再生されるアナウンスはいずれも保持されません。

Annunciator はメディア デバイスと見なされるため、メディア リソース グループ（MRG）に含めて、電話機およびゲートウェイで使用される Annunciator の選択を制御することができます。

Annunciator のパフォーマンス

デフォルトでは、Annunciator は 48 のストリームを同時にサポートするように設定されています。この設定値は、Cisco Unified CallManager サービスが同一のサーバ（共存）上で動作する Annunciator に推奨される最大値です。サーバの接続性が 10 Mbps しかない場合は、設定を下げて同時ストリームを 24 にします。

Cisco CallManager サービスを含まないスタンドアロン サーバでは、最大 255 のアナウンス ストリームを同時にサポートできます。デュアル CPU と高性能ディスク システムを持つ高性能サーバでは、最大 400 のストリームをサポートできます。複数のスタンドアロン サーバを追加して、必要な数のストリームをサポートすることができます。

Cisco RSVP Agent

トポロジ対応型のコール アドミッション制御を提供するために、Cisco Unified CallManager は 1 つまたは 2 つの RVSP Agent をコール セットアップ時に呼び出し、IP WAN で RSVP 予約を実行します。これらのエージェントは、RSVP 機能を提供するように設定された MTP またはトランスコーダ リソースです。RSVP リソースは、Cisco Unified CallManager による MTP またはトランスコーダ リソースの割り当てという観点から見て、通常の MTP またはトランスコーダと同様に処理されます。

Cisco RSVP Agent 機能は、Cisco IOS Release 12.4(6)T で最初に導入されました。RSVP および Cisco RSVP Agent の詳細については、P.9-1 の「コール アドミッション制御」の章を参照してください。

Cisco IP Voice Media Streaming Application

Cisco IP Voice Media Streaming Application は、ソフトウェアに次のリソースを組み込みます。

- Music on Hold（MoH）
- Annunciator
- ソフトウェア コンファレンス ブリッジ
- メディア ターミネーション ポイント（MTP）

Media Streaming Application をアクティブにすると、上記の各リソースが 1 つずつ自動的に設定されます。Annunciator、ソフトウェア コンファレンス ブリッジ、または MTP が必要ない場合は、Cisco IP Voice Media Streaming Application の Run Flag サービス パラメータを無効にして、これらのリソースを無効にすることをお勧めします。

複数のリソースが必要になる状況や、それらのリソースによって Media Streaming Application にかかる負荷を慎重に検討してください。各リソースには、処理可能な接続の最大数を制御するサービス パラメータと、関連付けられたデフォルト設定があります。デフォルト設定を変更しない限り、制限付きで 4 つのリソースすべてを同じサーバ上で実行できます。ただし、配置においてデフォルトを超える数のリソースが 1 つでも必要になった場合は、そのリソースを独自の専用サーバ上で実行するように設定します（そのサーバ上では、その他すべてのリソースおよび Cisco CallManager サービスを実行しないでください）。

Annunciator は、IP Voice Media Streaming Application でのみ使用できる唯一のメディア リソースです。会議、MTP、および Music On Hold（MoH; 保留音）はすべて、Cisco Unified CallManager サーバの外に置くことができます。Cisco Unified CallManager では MTP および会議リソースを無効にして、これらの機能には外部の専用リソースを用意することをお勧めします。

また、IP Voice Media Streaming Application は、コール処理を担当するパブリッシャ、または任意の Cisco Unified CallManager サーバとは異なるサーバ上で実行することを強くお勧めします。メディア リソースのために CPU 負荷が増加すると、コール処理のパフォーマンスに悪影響が発生する可能性があります。ユーザ データグラム プロトコル（UDP）トラフィックは、Cisco Unified CallManager サーバ上で受信されなければならないので、セキュリティ上の問題が発生する恐れがあります。

ハードウェアおよびソフトウェアのキャパシティ

この項では、DSP を含むネットワークモジュールおよびシャーシのキャパシティ、ネットワーク モジュールを含むシャーシのキャパシティ、およびハードウェアに対するソフトウェアの依存性に関するデータを提供します。

PVDM

表 6-8 および表 6-9 に、PVDM の 2 つのモデルまたは固定構成ネットワーク モジュールに配置できる DSP の数を示します。PVDM2-*xx* モジュールは PVDM-256K-*xx* モジュールよりも新しく、この 2 つのタイプは交換できません。

表 6-8　PVDM-256K モジュールあたりの DSP 数

モジュール	DSP 数
PVDM-256K-4	1 DSP
PVDM-256K-8	2 DSP
PVDM-256K-12	3 DSP
PVDM-256K-16HD	4 DSP
PVDM-256K-20HD	5 DSP

表 6-9　PVDM2 モジュールまたは固定構成ハードウェアあたりの DSP 数

ハードウェア モジュールまたはシャーシ	DSP 数
PVDM2-8	½ DSP
PVDM2-16	1 DSP
PVDM2-32	2 DSP
PVDM2-48	3 DSP
PVDM2-64	4 DSP
NM-HD-1V NM-HD-2V	1 DSP
NM-HD-2VE	3 DSP

表 6-10 に、各ハードウェア プラットフォームおよびネットワークモジュールでメディア リソース機能をサポートするために必要な、Cisco IOS ソフトウェアの最小バージョンを示します。

表 6-10　メディア サポートに必要な使用可能 PVDM2 スロット数と Cisco IOS のバージョン

シャーシまたは ネットワーク モジュール	PVDM2 スロット数	メディア用 Cisco IOS 最小リリース
2801	2	12.3(11)T
2811	2	12.3(8)T4
2821 または 2851	3	12.3(8)T4
3825 または 3845	4	12.3(11)T
NM-HDV2	4	

Cisco 2800 および 3800 シリーズ プラットフォーム

Cisco 2800 および 3800 シリーズ ルータはすべて、2 つの AIM スロットを備えていますが、AIM-VOICE-30 または AIM-ATM-VOICE-30 カードをサポートしません。これは、これらのカードの機能は、マザーボード上に取り付けられた PVDM2 モジュールによって代わりに提供されるためです。

ネットワーク モジュール

NM-HDV2、NM-HD-*xx*、および NM-HDV モジュールは、表 6-11 に示されている Cisco IOS プラットフォームに取り付けることができます。その場合の最大モジュール数は、表のとおりです。

表 6-12 内の 3 つのモジュール ファミリはすべて 1 つのシャーシに取り付けることができます。ただし、会議機能とトランスコーディング機能は、NM-HDV ファミリと、残りのファミリのどちらか（NM-HD-*xx* または NM-HDV2）との両方で同時に使用することはできません。また、NM-HDV（TI-549）、NM-HD-*xx*、および NM-HDV2（TI-5510）を、1 つのシャーシ内で同時に会議およびトランスコーディングに使用することはできません。

NM-HDV モジュールと NM-HDV-FARM モジュールは、同じシャーシに混在できます。すべてのシャーシがこれらのモジュールをフル装備できるわけではありません。表 6-11 では、各タイプのハードウェア プラットフォームがサポートする最大モジュール数を示しています。

表 6-11　プラットフォーム タイプごとのモジュール スロット数

Cisco IOS プラットフォーム	スロット数
2691, 2811, 2821, 2851	1
3620[1] , 3725, 3825	2
3640	3
3745, 3845	4
3660	6

1. Cisco 3620 ルータは 2 つの NM スロットを備えていますが、サポートする NM-HDV モジュールは 1 つだけです。

表 6-12　プラットフォーム タイプでサポートされるモジュール

Cisco IOS プラットフォーム	プラットフォームでサポートされるモジュール		
	NM-HDV2	NM-HD-1V NM-HD-2V NM-HD-2VE	NM-HDV NM-HDV-FARM
VG2001 26002 36203 3640	なし	なし	あり
3660	なし	あり	あり
2600XM、2691、 3725, 3745 2811, 2821, 2851 3825, 3845	あり	あり	あり

(注) Cisco VG200、2620、2621、および 3620 は、NM-HDV-FARM をサポートせず、さらに MTP、会議、およびトランスコーディングもサポートしません。Cisco 2801 には NM スロットがありません。

NM-HDV の DSP 要件の計算

状況によっては、NM-HDV がフル装備されないことがあります。サンプリング レートは通常、システム デフォルトから変更されません。サンプリング レートを変更する必要がない場合は、この問題を無視してかまいません。

音声アクティビティ検出（VAD）を有効または無効にしたサンプル レート 20、30、40、60 ms の場合（または、VAD を有効にした 10 ms の場合）、PVDM を 5 台フル装備した NM-HDV または NM-HDV-FARM を構成して、使用可能な DSP リソースを 60 得ることが可能です。

VAD を無効にした 10 ms サンプリング レートの場合、フル装備の NM-HDV 上のすべての DSP を利用することは不可能です。パケット レートが、NM-HDV のキャパシティである毎秒 6600 パケット（pps）を超えないことを確認するには、さらに次の計算が必要です。

100 pps（音声インターフェイス数）+ 600 pps（会議数）+ 200 pps（トランスコーディング セッション数 ）< 6600 pps

一般的な設計ガイドライン

Cisco Unified CallManager のメディア 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）のコンストラクトは、この章で説明されているリソースの編成とアクセスの方法を制御するために使用されます。この項では、これらのコンストラクトを効率的に利用する方法について説明します。また、さまざまな Cisco Unified CallManager 配置モデルに固有の考慮事項についても説明します。

メディア リソース グループとメディア リソース グループ リスト

メディア リソース グループとメディア リソース グループ リストは、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 タイプなどが含まれます。この項では、読者がメディア リソース グループを理解しているものとして、次の設計上の考慮事項について詳しく説明します。

- システムは、ユーザ インターフェイスに表示されず、すべてのリソースが作成時にメンバーとなるデフォルト メディア リソース グループを定義します。メディア リソースの使用側は、まず、設定で指定されている任意のメディア リソース グループ（MRG）またはメディア リソース グループ リスト（MRGL）のリソースを使用します。必要なリソースが使用できない場合、デフォルト MRG でリソースが検索されます。単純な配置では、デフォルトの MRG だけを使用することがあります。
- MRG を使用してリソースへのアクセスを制御する場合は、リソースを明示的に別のグループに設定することによって、デフォルト MRG の外に移動する必要があります。すべてのコールに対する最後の手段としてのみリソースを使用できるようにする場合は、そのリソースをデフォルト グループに残しておくことができます。また、リソースの制御が必要ない場合も、デフォルト グループに残しておくことができます。
- MRG には、複数のタイプのリソースが含まれていることがあります。必要な機能に基づいて、適切なリソースがグループから割り当てられます。MTP とトランスコーダは、特別な例です。トランスコーダは MTP としても使用できます。
- MRG の用途の 1 つは、類似したタイプのリソースのグループ化です。コンファレンス ブリッジ リソースがサポートする参加者の数は異なります。MRG を使用して、コンファレンス ブリッジのサイズ別に会議リソースをグループ化できます。

- 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）を使用して、複数の Cisco Unified CallManager 間でリソースを共有します。MRG と MRGL を使用しない場合、リソースは、1 つの Cisco Unified CallManager からしか使用できません。
- また、MRG と MRGL を使用すると、地理的なロケーションに基づいてリソースを分離できます。その結果、WAN 帯域幅を節約できる場合もあります。
- MRGL は、設定にリストされている順序で MRG を使用します。ある MRG に必要なリソースがない場合、次の MRG が検索されます。すべての MRG が検索され、リソースが見つからない場合、検索は終了します。
- MRG から類似のリソースを割り当てるアルゴリズムでは、類似したリソース間での負荷分散が試みられます。リソースが使用されると、その MRG のポインタは次のデバイスにインクリメントされます。1 つのデバイスが複数の MRG に存在することがあります。この場合、このデバイスがメンバーであるすべてのグループのポインタに影響を与えます。MTP が必要で、トランスコーダが同じグループに存在する場合、すべての MTP が使用されるまで、MTP が常に割り当てられます。すべての MTP が使用されると、トランスコーダが MTP として使用されます。同じグループにキャパシティの異なるリソースがある場合、ロード シェアリングはキャパシティに基づいてリソースを割り当てようとします。システムはリソース間で負荷を分散しますが、上記の要素により、動作がラウンドロビンになることはあまりありません。
- Cisco Unified CallManager Administration には MRG のデバイスがアルファベット順に表示されますが、割り当てられる順序は設定データベースの順序に基づきます。この順序は変更できません。メディア リソースを特定の順序で割り当てるには、リソースごとに別の MRG を作成し、MRGL を使用して割り当て順序を指定します。
- メディア リソース自身には、別のメディア リソースを呼び出さない設定が必要です。たとえば、MTP がコールに挿入され、この MTP で設定されているコーデックが、このコールに対して Cisco Unified CallManager が必要とするコーデックと異なる場合、トランスコーダも呼び出されます。よくある間違いは、Cisco Unified CallManager が G.729a を必要とする場合に、MTP を G.729 または G.729b に設定することです。

配置モデル

ここでは、MTP リソースとトランスコーディング リソースが、どこで、いつ使用されるかを説明します。具体的には、次の 3 つの企業 IP テレフォニー配置のモデルと、4 つ目のアプリケーション シナリオで示します。

- P.6-26 の「単一サイト配置」は、1 つのサイト内の 1 つ以上のコール処理エージェントから構成され、音声トラフィックは IP WAN を介して伝送されません。
- P.6-27 の「集中型コール処理を使用するマルチサイト WAN 配置」は、IP WAN を通じて接続された複数のサイトにサービスを提供する、単一のコール処理エージェントから構成されます。
- P.6-28 の「分散型コール処理を使用するマルチサイト WAN 配置」は、IP WAN を通じて接続される複数のリモート サイトのそれぞれに置かれている、コール処理エージェントから構成されます。
- P.6-29 の「IP 公衆網アクセス」は、MTP リソースを必要とするもう 1 つのシナリオです。このシナリオは、上記の配置モデルのすべてに適用されます。

単一サイト配置

単一サイト配置では、低ビット レート（LBR）コーデックを使用する根拠となっている低速リンクが不要のため、トランスコーディングの必要はありません。H.323v2 に準拠していない相当数のデバイス（旧バージョンの Microsoft NetMeeting や特定のビデオ デバイスなど）が存在する場合、なんらかの MTP リソースが必要なことがあります。SIP エンドポイントがある場合は、DTMF 変換用に MTP リソースが必要になることがあります（P.6-14 の「Named Telephony Event（RFC 2833）」を参照）。

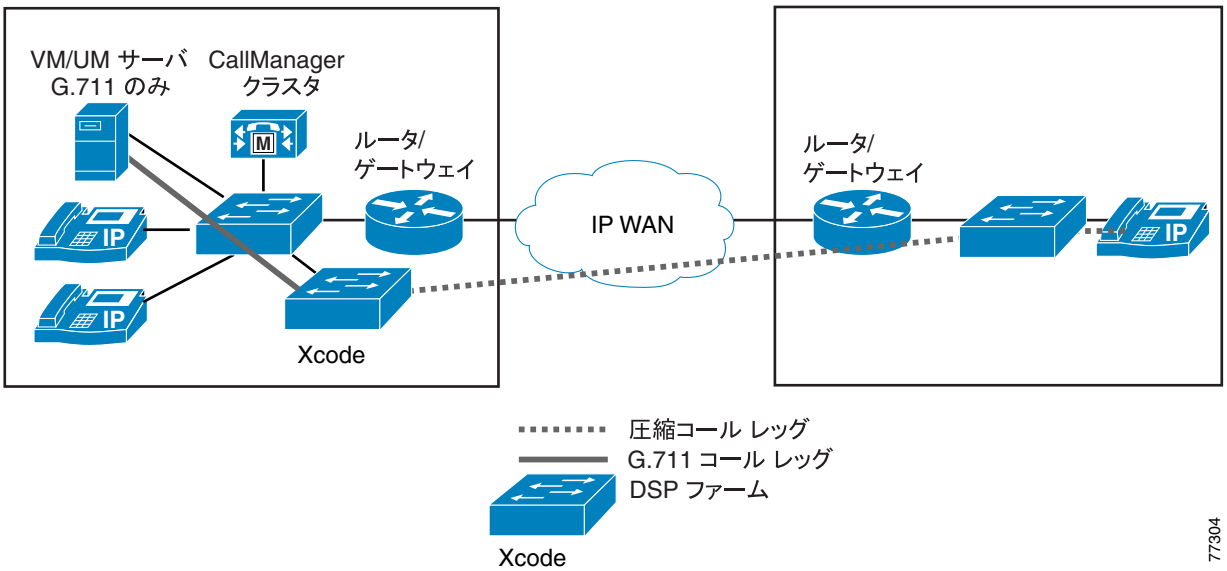
集中型コール処理を使用するマルチサイト WAN 配置

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

WAN 帯域幅は一般に制限されるので、WAN を通過するときは、G.729 などの低ビット レート コーデックを使用するようにコールが設定されます（図 6-1 を参照）。

IP Phone 間の音声圧縮は、Cisco Unified CallManager の *リージョン*と *ロケーション*を使用して簡単に設定されます。リージョンは、そのリージョン内のデバイスが使用する圧縮のタイプ（たとえば、G.711 または G.729）を指定します。ロケーションは、そのロケーションのデバイスに出入りするコールに使用可能な、合計帯域幅量を指定します。

図 6-1　集中型コール処理を使用する WAN のトランスコーディング



Cisco Unified CallManager は、MRG（メディア リソース グループ）を使用して、クラスタ内の Cisco Unified CallManager サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、異なるリージョンを通過するコールに LBR コーデック（たとえば、G.729a）を使用する場合、トランスコーディング リソースが使用されるのは、エンドポイントの一方（または両方）が、LBR コーデックを使用できない場合だけです。

図 6-1 では、Cisco Unified CallManager がトランスコーダが必要であることを認識し、高帯域幅コーデックを使用するデバイスの MRGL または MRG に基づいてトランスコーダを割り当てます。この場合、VM/UM サーバが、使用するトランスコーダ デバイスを決定します。この Cisco Unified CallManager の動作は、トランスコーダ リソースが高帯域幅デバイスの近くに正しく配置されていることを前提としています。VM/UM サーバ用のトランスコーダがリモート サイトに配置されるようにこのシステムが設計されていた場合、G.711 は WAN を経由して送信されるため、設計の意図が失われます。結果として、G.711 のみのデバイスを使用する複数のサイトがある場合に WAN で LBR が実行されていると、これらの各サイトがトランスコーダ リソースを必要とします。

その他のリソースの配置も重要です。たとえば、リモート サイトの 3 つの電話機で会議が発生し、会議リソースが中央（コール処理）サイトにある場合、3 つのメディア ストリームが WAN で伝送されます。会議リソースがローカルにあれば、コールは WAN を経由しません。WAN の帯域幅とコール アドミッション制御を設計するときは、この要素を考慮する必要があります。

分散型コール処理を使用するマルチサイト WAN 配置

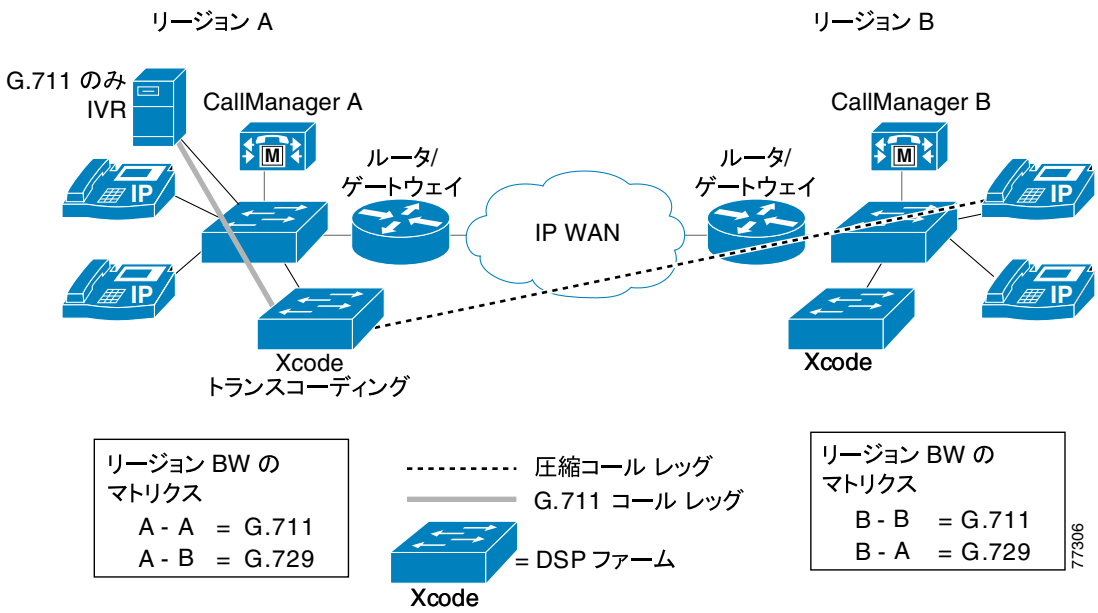
分散型コール処理配置では、IP WAN を介して複数のサイトが接続されます。各サイトには Cisco Unified CallManager クラスタが含まれ、単一サイト モデルか、集中型コール処理モデルになります。サイト間のコール アドミッション制御には、ゲートキーパーを使用できます。

WAN 帯域幅は一般に制限されているので、WAN を通過するときは、LBR コーデック（たとえば、G.729a）を使用するように、サイト間のコールが設定されていることがあります。H.323v2 クラスタ間トランクは、Cisco Unified CallManager クラスタの接続に使用されます。Cisco Unified CallManager は、ハードウェア MTP が使用される場合、MTP サービスを通じた圧縮音声コール接続もサポートします（図 6-2 を参照）。

次の状況では、分散型コール処理配置に、トランスコーディング サービスと MTP サービスが必要になる場合があります。

- 現行バージョンの Cisco アプリケーションを使用する場合は、トランスコーディング リソースの使用を回避できるため、回避することをお勧めします。特別な例として、特定のデバイスの G.711 を回避できないことがあります。
- 一部のエンドポイント（たとえば、映像エンドポイント）が、H.323v2 機能をサポートしません。

図 6-2　トランスコーディングを使用したクラスタ間コール フロー



Cisco Unified CallManager は、MRG（メディア リソース グループ）を使用して、クラスタ内の Cisco Unified CallManager サーバ間で、MTP リソースとトランスコーディング リソースの共有を可能にします。さらに、クラスタ間トランクを介したコールの場合、MTP リソースとトランスコーディング リソースは、必要な場合だけ使用されます。したがって、LBR コーデックをサポートしないアプリケーションに対して MTP サービスを設定する必要がなくなります。

次の特性が、分散型コール処理配置に適用されます。

- トランスコーディングを必要とするクラスタ間コールだけが、MTP サービスを使用します。たとえば、コールの両方のエンドポイントが G.729 コーデックを使用できる場合、トランスコーディング リソースは使用されません。
- クラスタ内のサーバ間で MTP リソースを共有すると、リソースの使用効率が向上します。

IP 公衆網アクセス

MTP リソースとトランスコーディング リソースのもう 1 つのアプリケーション シナリオには、従来の公衆網ではなく、IP 公衆網へのアクセスをカスタマーに提供するサービス プロバイダーが必要です。このようなシナリオでは、ゲートキーパーがサービス プロバイダーのネットワークに置かれます。ダイヤル プランを単純化するために、各カスタマーは、エンドポイントに割り当てられている個々の IP アドレスを隠せるように、MTP を使用してコールを固定する必要があります。その後、サービス プロバイダーのセントラル オフィスは、従来の公衆網を介してリレーし、他のカスタマーとの IP 接続を提供できます。図 6-3 は、この配置モデルを示しています。

図 6-3　IP 公衆網アクセスの例

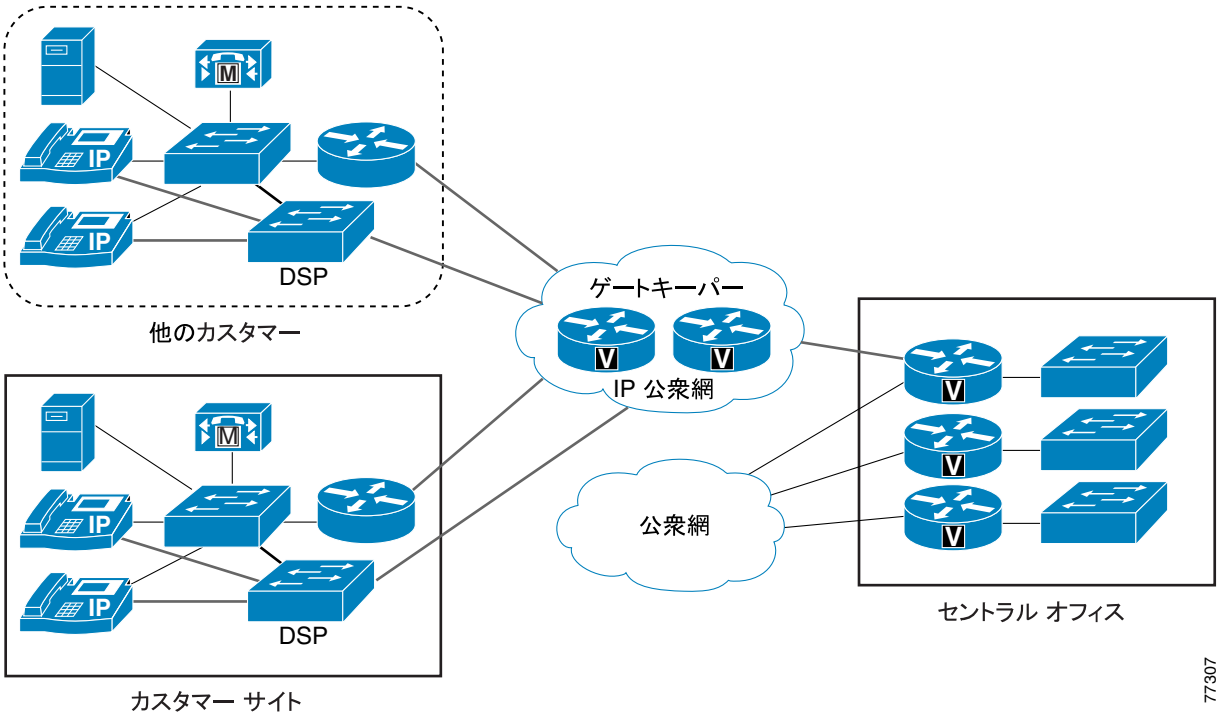


図 6-3 のカスタマー サイトは、前述の 3 つの配置モデル（単一サイト、集中型コール処理を使用するマルチサイト WAN、分散型コール処理を使用するマルチサイト WAN）の任意の 1 つを使用できることに注意してください。

カスタマー サイトから IP 公衆網までの H.323 トランクは、エンドポイントの IP アドレスがマスクされたままであるように、MTP を使用して設定される必要があります。したがって、すべての外部コールが MTP リソースを使用します。ただし、MTP リソースは、リソースの使用効率を高めるために、Cisco Unified CallManager クラスタ内で共有できます。MTP を利用してアドレスを隠蔽するこの手法は、SIP トランクでも使用できます。

Music on Hold

Music on Hold（MoH）は、Cisco Unified Communications システムの統合機能です。この機能は、発信者の通話が保留、転送、一時保留（コール パーク）、または ad-hoc 会議に追加されるときに、発信者に音楽を流します。MoH の実装は、比較的簡単ですが、ユニキャストおよびマルチキャスト トラフィック、MoH コール フロー、設定オプション、サーバの動作と要件について基本的な理解が必要です。この章では、Cisco エンタープライズ IP テレフォニー配置用に MoH リソースを設計し、プロビジョニングする方法について説明します。

Cisco Unified CallManager は、さまざまなメディア リソースにアクセスできます。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、接続されている音声データ ストリームに対して何らかの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、ある接続から別の接続にストリームを渡す機能、ある圧縮タイプから別の圧縮タイプにデータ ストリームをトランスコードする機能が含まれます。

Cisco Unified CallManager は、次のタイプのメディア リソースを割り当て、使用します。

- メディア ターミネーション ポイント（MTP）リソース
- トランスコーディング リソース
- ユニキャスト会議リソース
- Annunciator リソース
- Music on Hold リソース

メディア リソース全般の詳細については、P.6-1 の「メディア リソース」の章を参照してください。

この章では、MoH 機能の設計について次の項目を説明します。

- MoH の基本的な配置（P.7-2）
- 基本的な MoH と MoH コール フロー（P.7-6）
- MoH 設定上の考慮事項およびベスト プラクティス（P.7-10）
- MoH リソース用のハードウェアとキャパシティ プランニング（P.7-14）
- MoH に対する IP テレフォニー配置モデルの影響（P.7-16）
- ユニキャストとマルチキャスト MoH コール フローの詳細（P.7-22）

MoH の基本的な配置

発信者に保留音が聞こえるようにするには、Cisco Unified CallManager の MoH 機能を有効にする必要があります。MoH 機能には、次の 2 つの主な要件があります。

- MoH オーディオ ストリーム ソースを流す MoH サーバ
- 通話を保留にするときに、MoH サーバが流す MoH ストリームを使用するように設定された Cisco Unified CallManager

統合 MoH 機能により、ユーザは、オンネットとオフネットのユーザを保留にするときに、ストリーミング ソースから音楽を流すことができます。このソースは、保留になったオンネットまたはオフネット デバイスに音楽を流します。オンネット デバイスには、IVR（音声自動応答装置）またはコール ディストリビュータによって保留、確認保留、またはコール パーク保留にされた端末デバイスやアプリケーションが含まれます。オフネット ユーザには、メディア ゲートウェイ統合プロトコル（MGCP）、Session Initiation Protocol（SIP）、および H.323 ゲートウェイを通じて接続されたユーザが含まれます。また、MoH 機能は、Foreign Exchange Station（FXS）ポートを通じて Cisco IP ネットワークに接続された、一般電話サービス（POTS）の電話機にも使用できます。統合 MoH 機能には、メディア サーバ、データベース管理、コール制御、メディア リソース マネージャ、およびメディア制御の機能領域が含まれます。MoH サーバは、音楽リソースとストリームを提供します。

MoH 機能は、Cisco Unified CallManager Administration インターフェイスを介して設定できます。終端装置または機能が通話を保留にすると、Cisco Unified CallManager は、その保留デバイスを MoH メディア リソースに接続します。基本的に、Cisco Unified CallManager は、MoH サーバとの接続を確立するように、エンド デバイスに指示します。保留にされたデバイスが復帰すると、そのデバイスは MoH リソースから切り離され、通常のアクティビティを再開します。

ユニキャストおよびマルチキャスト MoH

Cisco Unified CallManager は、次の 2 つのタイプの MoH トランスポート メカニズムをサポートします。

- ユニキャスト
- マルチキャスト

ユニキャスト MoH は、MoH サーバから MoH オーディオ ストリームを要求するエンドポイントに直接送信されるストリームで構成されます。ユニキャスト MoH ストリームは、サーバとエンドポイント デバイス間のポイントツーポイント片方向オーディオ Real-Time Transport Protocol（RTP）ストリームです。ユニキャスト MoH は、ユーザまたは接続ごとに別々のソース ストリームを使用します。ユーザまたはネットワーク イベントを介して保留になるエンドポイント デバイスが増えるにつれて、MoH ストリームの本数も増加します。したがって、20 台のデバイスが保留になっている場合、サーバとこれらのエンドポイント デバイス間のネットワーク上で、RTP トラフィックとしてストリームが 20 本生成されます。このような MoH ストリームが生成されると、ネットワークのスループットと帯域幅に対してマイナスの影響を与える可能性があります。しかし、ユニキャスト MoH が非常に役立つのは、マルチキャストが使用可能になっていないネットワークの場合や、デバイスがマルチキャスト対応になっていないネットワークの場合です。このようなときに、管理者はユニキャスト MoH を使用することで、MoH 機能を利用できます。

マルチキャスト MoH は、MoH サーバからマルチキャスト グループ IP アドレスに送信されるストリームで構成されます。MoH オーディオ ストリームを要求するエンドポイントは、必要に応じてこの IP アドレスに加わることができます。マルチキャスト MoH ストリームは、MoH サーバとマルチキャスト グループ IP アドレス間の、ポイントツーマルチポイント片方向オーディオ RTP ストリームです。マルチキャスト Music on Hold では、複数のユーザが同じオーディオ ソース ストリームを使用して Music on Hold を提供できるようにするので、システム リソースと帯域幅を節約できます。したがって、20 台のデバイスが保留中であっても、ネットワーク上で 1 つの RTP トラフィッ

クのストリームだけしか生成されない場合もあります。したがって、マルチキャストは、ソース デバイスに対する CPU の影響を大幅に削減し、共通パス上の伝送の帯域幅使用量も大幅に削減するので、MoH などのサービスの配置に非常に魅力的なテクノロジーです。しかし、ネットワークがマルチキャスト対応になっていない状況や、エンドポイント デバイスがマルチキャストを処理できない状況では、マルチキャスト MoH に問題が生じます。

IP マルチキャスト ネットワークの設計については、次の Web サイトで入手可能なオンラインの『IP Multicast SRND』資料を参照してください。

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

推奨されるユニキャスト / マルチキャスト ゲートウェイ

次の推奨ゲートウェイは、ユニキャスト MoH とマルチキャスト MoH の両方をサポートします。

- Cisco 6624 および 6608 ゲートウェイ モジュールと、MGCP および Cisco Unified CallManager Release 3.3(3) 以降の組み合せ
- Cisco Communication Media Module（CMM; コミュニケーション メディア モジュール）と、MGCP または H.323、および Cisco Unified CallManager Release 4.0、Cisco IOS Release 12.2(13)ZP3 以降、または Catalyst OS Release 8.1(1) 以降の組み合せ
- Cisco 2600、2800、3600、3700、および 3800 シリーズ ルータと、MGCP または H.323、および Cisco IOS Release 12.2(8)T 以降の組み合せ

共存 MoH サーバとスタンドアロン MoH サーバ

MoH 機能を利用するには、Cisco Unified CallManager クラスタに含まれているサーバを使用する必要があります。MoH サーバは、次のいずれかの方法で設定できます。

- 共存配置

  共存配置では、MoH 機能は Cisco Unified CallManager ソフトウェアも実行している、クラスタ内の任意のサーバ（パブリッシャまたはサブスクライバ）で実行されます。このタイプの設定では、MoH と Cisco Unified CallManager はサーバ リソースを共有するので、MoH サーバが送信できる同時ストリーム数が大幅に減少します。
- スタンドアロン配置

  スタンドアロン配置では、MoH 機能は Cisco Unified CallManager クラスタ内の専用サーバに置かれます。この専用サーバの機能は、MoH ストリームをネットワーク内のデバイスに送信することだけです。スタンドアロン配置では、1 台の MoH サーバから最大数のストリームを送信できます。

MoH の固定ソースとオーディオ ファイル ソース

MoH のソースは、次のいずれかの方法で設定できます。

- Cisco Unified CallManager または MoH サーバ上のオーディオ ファイルを使用した MoH
  - オーディオ ファイルを使用したユニキャスト MoH
  - オーディオ ファイルを使用したマルチキャスト MoH
- 固定音楽ソースを使用した MoH（サウンド カード経由）
  - 固定ソースを使用したユニキャスト MoH
  - 固定ソースを使用したマルチキャスト MoH

MoH は、MoH サーバ上に格納されているオーディオ ファイルから生成できます。オーディオ ファイルは、次の形式のいずれかでなければなりません。

- G.711 A-law または mu-law
- G.729 Annex A
- ワイドバンド

MoH オーディオ ファイルは、MoH Audio File Management ページ（または Music On Hold Audio Source Configuration ページ）でファイル アップロード機能を使用して、.wav フォーマットのオーディオ ファイルを MoH サーバにアップロードすると、Cisco Unified CallManager によって自動的に生成されます。次に、Cisco Unified CallManager は、オーディオ ソース ファイルを指定されたコーデック タイプに適した MoH ソース ファイルに変換し、フォーマットします。MoH イベントが発生すると、MoH サーバは、設定されたオーディオ ソース ファイルを保留中の要求側デバイスにストリーミングします。

（注） MoH オーディオ ソースの設定前に、.wav フォーマットのオーディオ ソース ファイルをクラスタ内の各 MoH サーバにアップロードしておく必要があります。オーディオ ソース ファイルをアップロードするには、管理者がクラスタ内の各 MoH サーバ上で Cisco Unified CallManager Administration インターフェイスに移動し、MoH Audio File Management ページでファイルのアップロード機能を使用する必要があります。この手順は、オーディオ ソース ファイルごとに実行する必要があります。オーディオ ソースを MoH オーディオ ストリーム番号に割り当て、MoH オーディオ ソースとして設定するには、事前にクラスタ内のすべての MoH サーバにオーディオ ソース ファイルをアップロードしておく必要があります。

録音済みまたはライブ オーディオが必要である場合、固定ソースから MoH を生成できます。このタイプの MoH の場合、サウンド カードが必要です。固定オーディオ ソースは、ローカル サウンド カードのオーディオ入力に接続されます。

このメカニズムにより、ラジオ、CD プレーヤー、または互換性があるその他のサウンド ソースを使用できます。固定オーディオ ソースからのストリームは、リアルタイムで変換され、Cisco Unified CallManager Administration によって設定されたコーデックに対応します。固定オーディオ ソースは、G.711（A-law または mu-law）、G.729 Annex A、およびワイドバンドに変換することができる、リアルタイムで変換可能な唯一のオーディオ ソースです。

固定またはライブ オーディオ ソースを MoH サーバに接続するには、Cisco MoH USB オーディオ サウンド カード（MOH-USB-AUDIO=）を使用する必要があります。この USB サウンド カードは、Cisco Unified CallManager Release 5.0 をサポートするすべての MCS プラットフォームと互換性があります。

（注） Music On Hold を送信するときに固定オーディオ ソースを使用する場合は、事前に、著作権のあるオーディオ素材の再ブロードキャストについて、その適法性および問題を検討しておく必要があります。起こりうる問題については、貴社の法務部門に相談してください。

Cisco Unified CallManager クラスタに含まれる MoH サーバ

MoH 機能を利用するには、各 MoH サーバが Cisco Unified CallManager クラスタに含まれている必要があります。すべての MoH サーバは、パブリッシャ サーバと設定を共有し、データベース複製スキーマに加わる必要があります。具体的には、MoH サーバはデータベースによって次の情報を共有する必要があります（これらの情報は Cisco Unified CallManager Administration で設定されます）。

- オーディオ ソース：設定されたすべての MoH オーディオ ソースの数と ID
- マルチキャストまたはユニキャスト：これらのソースそれぞれに設定されたトランスポートの種類
- マルチキャスト アドレス：マルチキャストとしてストリーミングするように設定されたソースのマルチキャスト ベース IP アドレス

MoH サーバは、Cisco Unified CallManager クラスタの一部になり、自動的にデータベースの複製に加わります。スタンドアロン MoH サーバを設定するには、最初に、そのサーバに Cisco Unified CallManager を通常どおりにインストールします。次に、Cisco CallManager サービスを無効にし（スタンドアロン MoH サーバ上でのみ）、Cisco IP Voice Media Streaming Application を有効にします。

基本的な MoH と MoH コール フロー

ここでは、Cisco Unified CallManager で実装される MoH の基本的な動作、および標準的なコール フローのシナリオについて説明します。

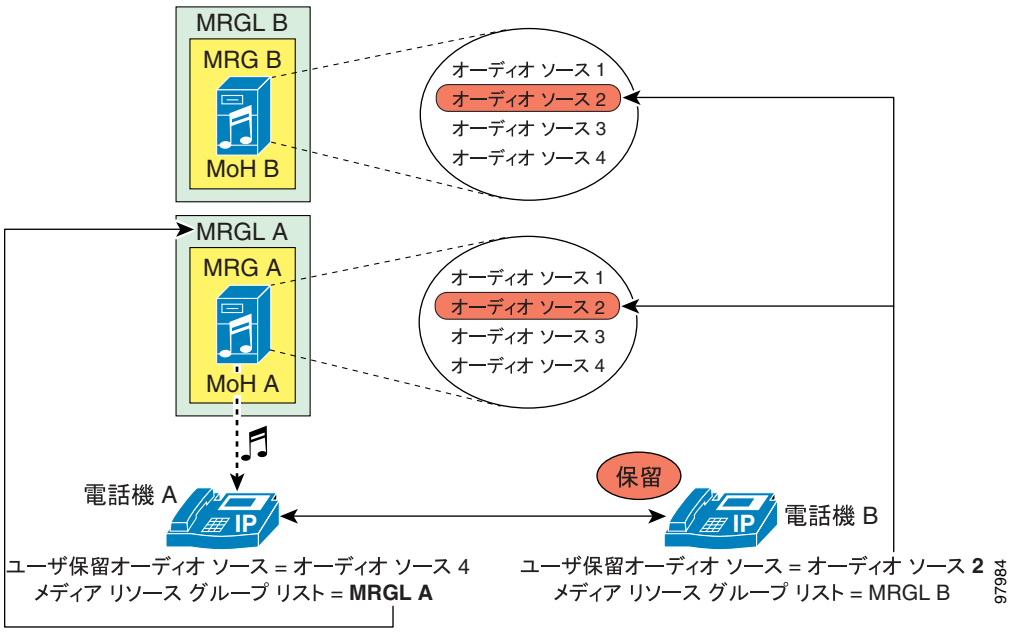
基本的な MoH

Cisco Unified Communications 環境における基本的な MoH の動作は、保留側と被保留側から構成されます。保留側とは、通話を保留にするエンドポイント ユーザまたはネットワーク アプリケーションです。一方、被保留側とは、保留にされたエンドポイント ユーザまたはデバイスです。

エンドポイントが受信する MoH ストリームは、エンドポイントを保留にするデバイス（保留側）のユーザ保留 MoH オーディオ ソースと、保留にされたエンドポイント（被保留側）に設定されたメディア リソース グループ リスト（MRGL）との組み合せによって決まります。保留側に対して設定されたユーザ保留 MoH オーディオ ソースによって、保留側が通話を保留にしたときに流されるオーディオ ファイルが決まります。被保留側に設定された MRGL は、被保留側が MoH ストリームを受信する元のリソースまたはサーバを指定します。

簡単に言えば、保留側の設定により、再生されるオーディオ ファイルが決まり、被保留側の設定により、そのファイルを再生するリソースまたはサーバが決まります。図 7-1 の例に示すように、電話機 A および B が通話中であるときに、電話機 B（保留側）で電話機 A（被保留側）を保留にする場合、電話機 A には、電話機 B に対して設定された MoH オーディオ ソース（Audio-source2）が聞こえます。ただし、電話機 A はこの MoH オーディオ ストリームを、電話機 A に対して設定された MRGL（リソースまたはサーバ）（MRGL A）から受信します。

図 7-1　ユーザ保留オーディオ ソースとメディア リソース グループ リスト（MRGL）



MRGL により、ユニキャスト専用デバイスが MoH ストリームを受信するサーバが決まるので、ユニキャスト専用デバイスを設定する場合は、ユニキャスト MoH リソースまたはメディア リソース グループ（MRG）を指定する MRGL を使用する必要があります。同様に、マルチキャスト対応デバイスは、マルチキャスト MRG を指定する MRGL を使用して設定する必要があります。

MoH 構成の設定値

MRGL、およびユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの設定値は、Cisco Unified CallManager Administration 内の複数の個所で指定できます。それぞれの個所で別々の（おそらく、競合する）設定値を設定できます。

個々のケースにユーザ オーディオ ソース設定値とネットワーク オーディオ ソース設定値のいずれかを適用するか決定するために、Cisco Unified CallManager は、次の優先順位で、保留側デバイスに対するこれらの設定値を使用します。

1. ディレクトリまたは回線設定（ゲートウェイなど、回線定義のないデバイスには、このレベルはありません）
2. デバイス設定値
3. デバイス プールの設定値
4. クラスタ全体のデフォルト設定

特定の保留側のオーディオ ソースを決定しようとする場合、Cisco Unified CallManager はまず、ディレクトリまたは回線レベルで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Cisco Unified CallManager は、保留側デバイスで設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Cisco Unified CallManager は、保留側デバイスのデバイス プールに対して設定されたユーザ（またはネットワーク）オーディオ ソースを調べます。このレベルが定義されていない場合、Cisco Unified CallManager は、Cisco Unified CallManager システム パラメータで設定された、クラスタ全体のデフォルト オーディオ ソース ID を調べます（デフォルトでは、このオーディオ ソース ID は、ユーザ保留オーディオ ソースとネットワーク保留オーディオ ソースの両方に対して 1 に設定されています。これは、SampleAudioSource です）。

Cisco Unified CallManager は、被保留側デバイスの MRGL 設定値も、次の優先順位で使用します。

1. デバイス設定値
2. デバイス プールの設定値
3. システムのデフォルト MoH リソース

特定の被保留側の MRGL を決定しようとする場合、Cisco Unified CallManager は、デバイス レベルで設定された MRGL を調べます。このレベルが定義されていない場合、Cisco Unified CallManager は、被保留側デバイスのデバイス プールに対して設定された MRGL を調べます。このレベルが定義されていない場合、Cisco Unified CallManager は、システムのデフォルト MoH リソースを使用します。システムのデフォルト MoH リソースとは、MRG に割り当てられていないリソースであり、これらのリソースは常にユニキャストです。

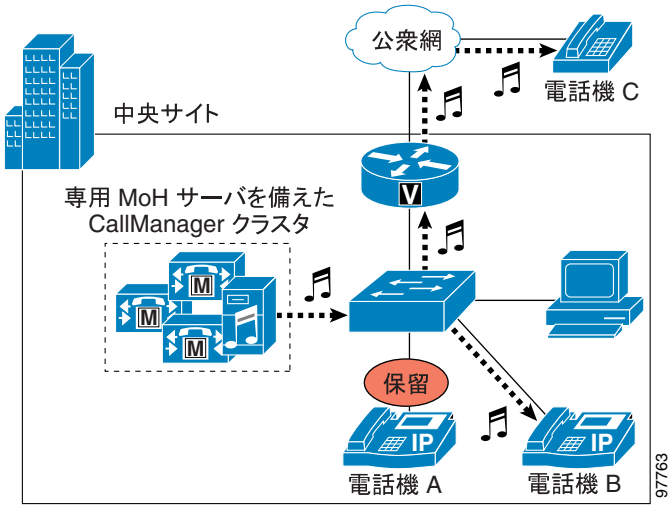
ユーザ保留とネットワーク保留

ユーザ保留には、次の 2 つの基本的なタイプがあります。

- IP Phone またはその他のエンドポイント デバイスでのユーザ保留
- MoH がゲートウェイにストリーミングされる公衆網でのユーザ保留

図 7-2 は、これらの 2 つのタイプのコール フローを示しています。電話機 A が電話機 B と通話中であるときに、電話機 A（保留側）で Hold ソフトキーを押すと、MoH サーバから電話機 B（被保留側）に音楽ストリームが送信されます。この音楽ストリームは、IP ネットワーク内の被保留側だけでなく、電話機 A が電話機 C を保留にする場合と同様に、公衆網上の被保留側にも送信できます。電話機 C の場合、MoH ストリームは音声ゲートウェイ インターフェイスに送信され、公衆網電話機に適したフォーマットに変換されます。電話機 A が Resume ソフトキーを押すと、被保留側（電話機 B または C）は、音楽ストリームから切り離され、電話機 A に再び接続されます。

図 7-2　ユーザ保留の基本的な例

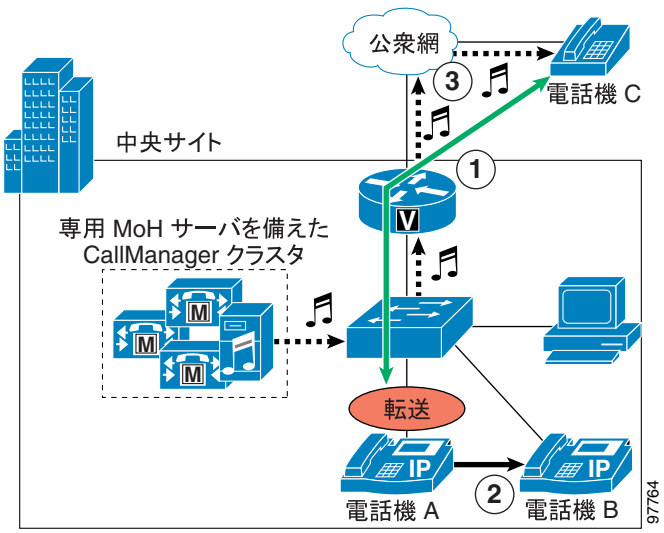


ネットワーク保留には次のタイプがあります。

- コール転送
- コール パーク
- 会議セットアップ
- アプリケーション ベースの保留

図 7-3 は、コール転送のコール フローを示しています。電話機 A が公衆網電話機 C からコールを受信する（ステップ 1）と、電話機 A はそのコールに応答し、電話機 B に転送します（ステップ 2）。転送プロセス時に、電話機 C は、ゲートウェイを介して MoH サーバから MoH ストリームを受信します（ステップ 3）。電話機 A が転送アクションを完了した後、電話機 C は音楽ストリームから切り離され、電話機 B（転送の宛先）に転送されます。このプロセスは、コール パークや会議セットアップなどの他のネットワーク保留操作の場合と同じです。

図 7-3　コール転送のネットワーク保留の基本的な例



ユニキャストとマルチキャスト MoH コール フロー

MoH 操作は、通常の電話のコール フローに非常によく似ています。MoH サーバは、被保留側デバイスが必要に応じて接続または切断されるエンドポイント デバイスの役目をします。しかし、ユニキャストとマルチキャストの MoH コール フローの動作には、明らかな相違点があります。ユニキャスト MoH コール フローは、Cisco Unified CallManager から MoH サーバへのメッセージによって初期化されます。このメッセージは、被保留側デバイスの IP アドレスにオーディオ ストリームを送信するように、MoH サーバに指示します。一方、マルチキャスト MoH コール フローは、Cisco Unified CallManager から被保留側デバイスへのメッセージによって初期化されます。このメッセージは、設定されたマルチキャスト MoH オーディオ ストリームのマルチキャスト グループ アドレスに加わるように、エンドポイント デバイスに指示します。

MoH コール フローの詳細については、P.7-22 の「ユニキャストとマルチキャスト MoH コール フローの詳細」の項を参照してください。

MoH 設定上の考慮事項およびベスト プラクティス

ここでは、堅牢な MoH ソリューションの設計に役立つ、MoH 設定上の考慮事項とベスト プラクティスについて説明します。

コーデックの選択

MoH 配置に複数のコーデックが必要な場合、Cisco CallManager Service Parameters Configuration の IP Voice Streaming Media App サービス パラメータでコーデックを設定します。Clusterwide Parameters セクションの下の Supported MoH Codecs リストの中から、必要なコーデック タイプを選択してください。デフォルトでは、G.711 mu-law のみが選択されています。別のコーデック タイプを選択するには、リストをスクロールさせて該当するコーデックをクリックしてください。複数選択する場合は、CTRL キーを押したまま、マウスを使用して、リストをスクロールさせて複数のコーデックを選択します。選択終了後、Update ボタンをクリックしてください。

（注） MoH オーディオ ストリームに G.729 コーデックを使用する場合、このコーデックは会話用に最適化されているので、音楽用としては最低限のオーディオ品質であることに注意してください。

マルチキャスト アドレッシング

マルチキャスト MoH を設定するには、適切な IP アドレッシングが重要です。IP マルチキャストのアドレス範囲は 224.0.1.0 ～ 239.255.255.255 です。しかし、IANA（Internet Assigned Numbers Authority）は、公衆マルチキャスト アプリケーション用に 224.0.1.0 ～ 238.255.255.255 の範囲のアドレスを割り当てています。公衆マルチキャスト アドレスを MoH に使用しないことを強くお勧めします。代わりに、プライベート ネットワーク上の管理制御アプリケーション用に予約されている、239.1.1.1 ～ 239.255.255.255 の範囲内の IP アドレスを使用するように、マルチキャスト MoH オーディオ ソースを設定することをお勧めします。

さらに、次の理由で、ポート番号ではなく、IP アドレスでインクリメントするように、マルチキャスト オーディオ ソースを設定することも必要です。

- 保留にされた IP Phone は、ポート番号ではなく、マルチキャスト IP アドレスに加わる。

  Cisco IP Phone には、マルチキャスト ポート番号という概念はありません。したがって、特定のオーディオ ストリームに対して設定されているすべてのコーデックが、同じマルチキャスト IP アドレス（別々のポート番号であっても）に送信される場合、1 本のストリームしか必要ない場合であっても、すべてのストリームが IP Phone に送信されます。IP Phone は 1 本の MoH ストリームしか受信できないので、不必要なトラフィックでネットワークが飽和状態になる可能性があります。
- IP ネットワーク ルータは、ポート番号ではなく、IP アドレスに基づいて、マルチキャストをルーティングする。

  ルータには、マルチキャスト ポート番号という概念はありません。したがって、同じマルチキャスト グループ アドレス（別々のポート番号であっても）に送信される複数のストリームを検出すると、ルータは、そのマルチキャスト グループのすべてのストリームを転送します。必要なストリームは 1 本だけなので、ネットワーク帯域幅が過剰に利用され、その結果、ネットワークの輻輳が発生する可能性があります。

MoH オーディオ ソース

オーディオ ソースは、Cisco Unified CallManager クラスタ内のすべての MoH サーバ間で共有されます。クラスタごとに最大 51 の固有オーディオ ソースを設定できます（50 のオーディオ ファイル ソースと、サウンド カードを介した 1 つの固定 / ライブ ソース）。この制限の例外については、P.7-11 の「複数の固定またはライブ オーディオ ソースの使用」および P.7-18 の「支店ルータのフラッシュからのマルチキャスト MoH」の項を参照してください。

複数の固定またはライブ オーディオ ソースの使用

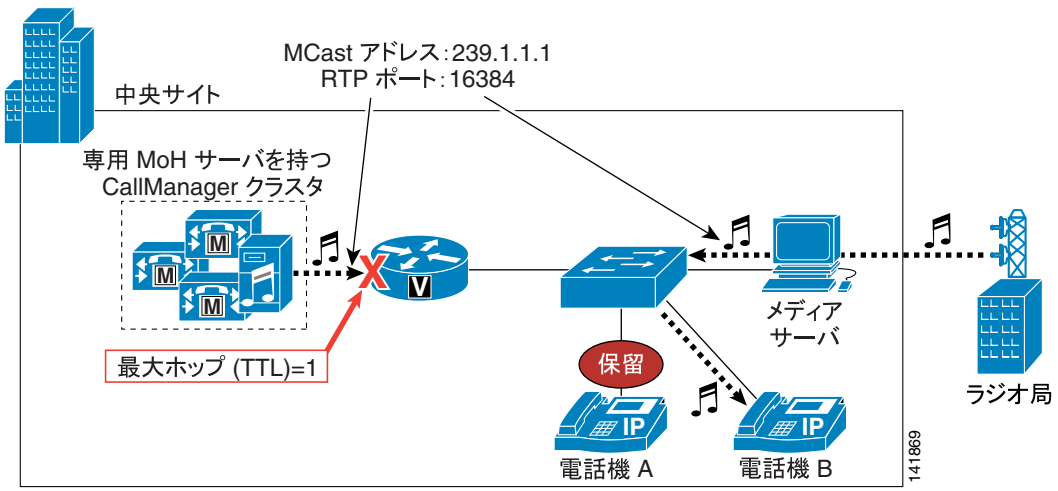
各 MoH サーバは、1 つの固定オーディオ ソースしか流すことができません。大部分の場合、複数の固定またはライブ オーディオ ソースが必要な場合は、ソースごとに別々の MoH サーバが必要です。しかし、固定またはライブ ソースからマルチキャストを流すことができる外部の非 MoH サーバまたはデバイスを使用すると、複数の固定ソース MoH オーディオ ストリームを提供することが可能です。

外部ソースごとに、外部ソース サーバまたはデバイスによってマルチキャストされるオーディオ ソース ストリームと同じマルチキャスト IP アドレス、およびポート番号を持つオーディオ ソースを使用して、MoH サーバを設定する必要があります。さらに、最大ホップ カウントを 1 に設定するか、アクセス コントロール リスト（ACL）を使用して、パケットがローカル サブネットの外に流れないようにすることによって、この設定された（非外部）オーディオ ソースが WAN を通過しないようにすることも必要です。

図 7-4 は、MoH ストリームとして使用される外部ライブ ソースの例を示しています。この図では、MoH サーバは、239.1.1.1（RTP ポート 16384 上で）にマルチキャスト オーディオ ソースを流します。このストリームは、最大ホップ カウント 1 に制限されているので、ローカル MoH サーバのサブネットから外に出ないことが保証されます。同時に、メディア サーバは、ラジオ局のライブ フィードから取得したオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.1.1.1 を使用し、RTP ポート番号として 16384 を使用します。ただし、電話機 A で Hold ソフトキーを押したときに、このストリームが電話機 B に到達できるようにするために、このストリームのホップ カウントまたは Time to Live（TTL; 存続可能時間）は 2 以上必要です。

（注） マルチキャストの TTL の値が減少する（または満了する）のは、パケットがレイヤ 3 インターフェイスを通過するときのみです。

図 7-4　外部のライブ オーディオ ソースの例



（注） マルチキャスト オーディオ ソースとしてラジオのライブ ブロードキャストを使用すると、法律上の問題が発生する恐れがあります。起こりうる問題については、貴社の法務部門に相談してください。

多数のストリームを、1 つまたは複数の外部メディア サーバからマルチキャストできます。これを行うには、追加のオーディオ ソースを複数の MoH サーバに設定し、MoH サーバに設定された同一のマルチキャスト グループ アドレスを使用して外部サーバからオーディオ ストリームを発信します。ただし、エンドポイント デバイスで聞こえる MoH ストリームは、保留側のユーザ / ネットワーク保留オーディオ ソースと被保留側の MRGL との組み合せによって決まるため、重複しているマルチキャスト グループ アドレスが多数存在する環境では、具体的にどのストリームをエンドポイントが受信するかを予測することは困難になる場合があります。このため、設定するマルチキャスト オーディオ ソースは MoH サーバごとに 1 つのみとすることをお勧めします。この推奨事項により、エンドポイントが受信するオーディオ ソースが、ユーザ / ネットワーク保留オーディオ ソースと MRGL の単一の組み合せによって一意に識別できることが保証されます。

同一 Cisco Unified CallManager クラスタ内のユニキャストとマルチキャスト

状況に応じて、管理者は、1 つの Cisco Unified CallManager クラスタを設定することにより、ユニキャストとマルチキャストの両方の MoH ストリームを処理できます。この設定が必要なのは、マルチキャストをサポートしないデバイス、またはエンドポイントがテレフォニー ネットワークに含まれている場合、あるいはネットワークの一部でマルチキャストが使用可能になっていない場合です。

クラスタがユニキャストとマルチキャストの両方の MoH オーディオ ストリームをサポートできるようにするには、次のいずれかの方法を使用してください。

- 別々の MoH サーバを配置します。一方のサーバをユニキャスト MoH サーバとして設定し、もう一方のサーバをマルチキャスト MoH サーバとして設定します。
- 同一 MoH サーバに対して別々のメディア リソース グループ（MRG）を設定します。オーディオ ストリームに対して、一方の MRG ではマルチキャストを使用するように設定し、もう一方の MRG ではユニキャストを使用するように設定します。

どちらの場合も、少なくとも 2 つの MRG、および少なくとも 2 つのメディア リソース グループ リスト（MRGL）を設定する必要があります。ユニキャスト MoH を必要とするエンドポイントには、1 つのユニキャスト MRG と 1 つのユニキャスト MRGL を設定します。同様に、マルチキャスト MoH を必要とするエンドポイントには、1 つのマルチキャスト MRG と 1 つのマルチキャスト MRGL を設定します。

別々の MoH サーバを配置する場合、一方のサーバをマルチキャスト無効（ユニキャスト専用）に設定し、もう一方の MoH サーバをマルチキャスト有効に設定してください。ユニキャスト専用 MoH サーバのユニキャスト オーディオ リソースをユニキャスト MRG に、マルチキャスト MoH サーバのマルチキャスト オーディオ リソースをマルチキャスト MRG に、それぞれ割り当てます。マルチキャスト MRG には **Use Multicast for MoH Audio** ボックスにチェックマークが付き、ユニキャスト MRG にはチェックマークが付いていないことを確認してください。また、これらのユニキャスト MRG とマルチキャスト MRG をそれぞれの MRGL に割り当てます。この場合、MoH ストリームを流す元のサーバ、および MRG がマルチキャストを使用するように設定されているかどうかに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

単一の MoH サーバをユニキャスト MoH とマルチキャスト MoH の両方に対して配置する場合は、サーバとそのオーディオ ソースをマルチキャスト用に設定します。同じオーディオ ソースをユニキャスト MRG とマルチキャスト MRG の両方に割り当て、マルチキャスト MRG に対して **Use Multicast for MoH Audio** ボックスにチェックマークを付けます。この設定により、MRG がマルチキャストを使用するように設定されているかどうかだけに基づいて、MoH ストリームのユニキャストまたはマルチキャストが行われます。

(注) ユニキャスト MRG を設定する場合は、混乱しないようにしてください。これは、オーディオ リソースをユニキャスト MRG に追加する場合であっても、オーディオ リソース名の最後に、[Multicast] が追加されるからです。このラベルは、リソースがマルチキャスト対応であるという単なる表示です。リソースがユニキャストとして送信されるか、マルチキャストとして送信されるかを決定するのは、**Use Multicast for MoH Audio** ボックスのチェックの有無です。

さらに、適切な MRGL を使用するように、個々のデバイスまたはデバイス プールを設定する必要があります。1 つまたは複数のデバイス プールにすべてのユニキャスト デバイスを含め、ユニキャスト MRGL を使用するようにこれらのデバイス プールを設定できます。あるいは、1 つまたは複数のデバイス プールにすべてのマルチキャスト デバイスを含め、マルチキャスト MRGL を使用するようにこれらのデバイス プールを設定することもできます。オプションとして、該当するユニキャスト MRGL またはマルチキャスト MRGL を使用するように、個々のデバイスを設定できます。あるいは、デバイス プール、個々のデバイス、または（電話デバイスの場合）個々の回線かディレクトリ番号ごとに、ユーザ保留オーディオ ソースおよびネットワーク保留オーディオ ソースを設定して、適切なオーディオ ソースを決定します。

マルチキャスト MoH とユニキャスト MoH の両方を同じクラスタに配置する方法を選択する場合は、必要なサーバの数を考慮することが重要です。単一の MoH サーバをユニキャストとマルチキャストの両方に使用すると、クラスタ全体に必要な MoH サーバの数が減ります。マルチキャスト MoH サーバとユニキャスト MoH サーバを別々に配置すると、クラスタ内に必要なサーバの数が明らかに増えます。

冗長性

完全な冗長性のある MoH 動作を確保するために複数の MoH サーバを設定し、配置することをお勧めします。最初の MoH サーバに障害が発生したり、要求を処理するために必要なリソースがなくなったために使用不能になると、2 番目のサーバが自動的に MoH 機能を引き継ぎ、要求に応答します。適切な冗長構成のために、クラスタ内の 2 つ以上の MoH サーバから各 MRG にリソースを割り当ててください。

MRG 内のリソースは、リストされている順に使用されます。デバイスが MoH オーディオ リソースを要求すると、Cisco Unified CallManager は、MRG 内の最初の MoH リソースをそのデバイスに送信しようとします。最初のリソースがサーバ障害またはリソースの不足により使用不能である場合、Cisco Unified CallManager は、MRG 内の次の MoH リソースを使用しようとします。

マルチキャストとユニキャストの両方の MoH が必要な環境では、ネットワーク内のすべてのエンドポイントの MoH 冗長性が確保されるように、必ず両方のトランスポート タイプに冗長性をもたせてください。

QoS

時間に依存する重要なリアルタイム アプリケーション（音声など）に遅延または損失がないように、1 つのネットワーク上のデータと音声のコンバージェンスには、適切な QoS が必要です。音声トラフィック用の適切な QoS を確保するには、ストリームがネットワークに入り、通過するときに、ストリームのマーク付け、分類、およびキューイングを行って、音声ストリームを重要度の低いトラフィックよりも優先的に処理する必要があります。MoH サーバは、オーディオ ストリーム トラフィックに、音声ベアラ トラフィックと同じマークを自動的に付けて、DSCP（Differentiated Services Code Point）を EF（ToS を 0xB8）にします。したがって、ネットワーク上で QoS が適切に設定されている限り、MoH ストリームは、音声 RTP メディア トラフィックとして分類され、プライオリティ キューイングとして扱われます。

MoH リソース用のハードウェアとキャパシティ プランニング

MoH リソースも、他のすべてのメディア リソースと同じように、ハードウェアを配置し、設定した後、予想されたネットワークのコール量を確実にサポートするために、キャパシティ プランニングが非常に重要です。このため、MoH リソースのハードウェア キャパシティを認識し、このキャパシティとの関連からマルチキャストとユニキャストの MoH の役割りを考慮することが重要です。

サーバ プラットフォームの最大同時セッション数

表 7-1 は、サーバ プラットフォームと、そのプラットフォームがサポートできる最大同時 MoH セッション数をリストしています。MoH セッションがこの最大同時セッション数を超えてから、さらに負荷が増えると、MoH 品質の低下、不規則な MoH 動作、または MoH 機能の喪失までも発生する恐れがあるので、ネットワークのコール量が最大同時セッション数を超えないようにしてください。

表 7-1　サーバ プラットフォーム タイプごとの最大 MoH セッション数

サーバ プラットフォーム	サポートされるコーデック	サポートされる MoH セッション数
MCS 7815 MCS 7825	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロン サーバ： 250 MoH セッション[1]
MCS 7835 MCS 7845	G.711（A-law および mu-law） G.729a ワイドバンド オーディオ	共存サーバまたはスタンドアロン サーバ： 500 MoH セッション

1. Cisco Unified CallManager クラスタごとに最大 51 の固有オーディオ ソースを設定できます。

MoH Server 設定ページの Maximum Half Duplex Streams フィールドと Maximum Multicast Connections フィールドを、表 7-1 に示されているキャパシティと一致するように設定する必要があります。これらのフィールドは、デフォルトで 250 と 30 にそれぞれ設定されていますが、表に示されているサーバ プラットフォームのタイプとサーバ配置のタイプ（共存またはスタンドアロン）に応じて設定変更する必要があります。推奨されるキャパシティの数値に一致させないと、サーバ リソースが十分に使用されない、またはサーバがネットワーク負荷を処理できないといった問題が発生する可能性があります。

（注） 表 7-1 にリストされている最大セッションの上限は、ユニキャスト、マルチキャスト、またはユニキャストとマルチキャストの同時セッションに適用されます。この上限は、トランスポート メカニズムに関係なく、プラットフォームがサポートできる推奨最大セッション数を示しています。

リソースのプロビジョニングとキャパシティ プランニング

共存またはスタンドアロンの MoH サーバ設定のプロビジョニングを行う場合、ネットワーク管理者は、MoH オーディオ ストリームに使用されるトランスポート メカニズムのタイプを考慮する必要があります。ユニキャスト MoH を使用する場合、保留される各デバイスには、別々の MoH ストリームが必要です。しかし、マルチキャスト MoH と単一のオーディオ ソースのみを使用する場合、保留にするタイプのデバイス数に関係なく、設定されているコーデック タイプごとに必要な MoH ストリームは 1 つだけです。

たとえば、30,000 台の電話機のあるクラスタがあり、保留率が 2% である（すべてのエンドポイント デバイスの 2% だけが、常に保留になる）場合、600 の MoH ストリームまたはセッションが必要です。ユニキャスト専用の MoH 環境の場合、次の計算で示されているように、この負荷を処理するには、2 つの共存（またはスタンドアロン）MoH サーバが必要です。

［（MCS 7815 または 7845 共存サーバごとに 500 セッション）*（共存サーバ 1 台）］+［（MCS 7835 または 7845 共存サーバごとに 250 セッション）*（共存サーバ 1 台）］> 600 セッション

一方、たとえば、36 の固有 MoH オーディオ ストリームがあるマルチキャスト専用 MoH 環境には、次の計算で示されているように、1 つの共存 MoH サーバ（MCS 7815 または 7825）だけが必要です。

（MCS 7815 または 7825 共存サーバごとに 250 セッション）*（共存サーバ 1 台）> 36 セッション

36 の固有マルチキャスト ストリームは、次のいずれかの方法でプロビジョニングできます。

- 単一のコーデックを使用して 36 の固有オーディオ ソースをストリーミングする。
- 2 つのコーデックだけを使用して 18 の固有オーディオ ソースをストリーミングする。
- 3 つのコーデックだけを使用して 12 の固有オーディオ ソースをストリーミングする。
- 4 つのコーデックすべてを使用して 9 つの固有オーディオ ソースをストリーミングする。

上記の例で示されているように、マルチキャスト MoH は、ユニキャスト MoH よりも、サーバ リソースを大幅に節約できます。

上記の例では、2% の保留率は、30,000 台の電話機に基づくものであり、保留になる可能性があるネットワーク内のゲートウェイまたはその他のエンドポイント デバイスを考慮していません。こうしたその他のデバイスは、電話機と同じように保留になる可能性があるので、保留率を計算するときは、これらのデバイスも考慮する必要があります。

上記の計算では、MoH サーバの冗長性を見込んでいません。MoH サーバに障害が発生する場合、またはユーザの 2% 以上が同時に保留になる場合、このシナリオでは、オーバーフローが発生したり負荷が増えたときに処理するための MoH リソースがありません。MoH リソースの計算には、冗長性に配慮して十分に余裕のあるキャパシティを含める必要があります。

（注） Cisco Unified CallManager クラスタごとに設定できる固有オーディオ ソースの上限は 51 で、MoH ストリームに使用可能なコーデックの上限は 4 つであるため、MoH サーバごとのマルチキャスト ストリームの最大数は 204 です。

MoH に対する IP テレフォニー配置モデルの影響

各種 IP テレフォニー配置モデルにより、MoH の構成設計にはさらに考慮事項が発生します。配置モデルの選択が、MoH のトランスポート メカニズム（ユニキャストまたはマルチキャスト）、リソースのプロビジョニング、およびコーデックの決定に影響を与える場合があります。ここでは、各種配置モデルに関連した問題について説明します。

配置モデルの詳細については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

単一サイト キャンパス（すべての配置に関連）

単一サイト キャンパス配置は、通常、LAN インフラストラクチャに基づくものであり、大量のトラフィックに対して十分な帯域幅が用意されています。LAN インフラストラクチャでは一般に帯域幅が制限されないので、単一サイト配置内のすべての MoH オーディオ ストリームには、G.711（A-law または mu-law）コーデックの使用をお勧めします。G.711 は、IP テレフォニー環境に、最適な音声と音楽のストリーミング品質を提供します。

MoH サーバの冗長性も考慮する必要があります。MoH サーバが過負荷になるか、使用不能になった場合でも、複数の MoH サーバを設定し、それらのサーバを優先順に MRG に割り当てておくと、別のサーバが制御を引き継いで、MoH ストリームを流すことができます。

ネットワーク テクノロジーの多様性が増すにつれて、大規模な単一サイト キャンパスでは、一部のエンドポイント デバイスがマルチキャストをサポートできなくなる可能性があります。このため、ユニキャストとマルチキャストの両方の MoH リソースを配置する必要があります。たとえば、無線 IP Phone は、無線テクノロジーの動作により、マルチキャストをサポートしません。したがって、無線 IP Phone を配置する場合は、マルチキャストとユニキャストの両方の MoH を設定する必要があります。

オフネット コールとアプリケーション処理コールが、保留時に期待された MoH ストリームを受け取るには、適切な MRGL とオーディオ ソースを使用してすべてのゲートウェイとその他のデバイスを設定するか、それらを適切なデバイス プールに割り当ててください。

集中型マルチサイト配置

集中型コール処理を使用するマルチサイト IP テレフォニー配置には、一般的に、中央以外の複数のサイトとの WAN 接続が含まれます。これらの WAN リンクは、通常、帯域幅とスループットの障害になります。これらのリンク上での帯域幅使用量を最小限にするには、WAN を通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。G.729 コーデックは、音楽アプリケーションではなく、音声用に最適化されています。したがって、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN 上でのみ、G.729 を使用してください。さらに、マルチキャスト トラフィックにより、帯域幅を大幅に節約できるので、WAN を介してエンドポイントにオーディオを流す場合は、常にマルチキャスト MoH を使用する必要があります。

WAN を介して G.729 を使用するときに MoH ストリームの音声品質が問題になる場合は、WAN を介した MoH オーディオ ストリームに G.711 コーデックを使用し、音声コールには引き続き G.729 を使用します。WAN を介した MoH ストリームの送信に G.711 コーデックを使用し、WAN を介した音声コールの送信に G.729 コーデックを使用するには、Cisco Unified CallManager リージョンにすべての MoH サーバだけを配置し、そのリージョンが他のリージョンとの間で G.711 を使用するように設定します。この設定により、WAN の一方の側にある 2 つの電話機間でコールを発信するときは、それぞれのリージョンの間で G.729 コーデックが使用されます。ただし、一方の通話者がコールを保留にした場合、MoH オーディオ ストリームは G.711 を使用して符号化されます。これは、G.711 が、MoH サーバのリージョンと、保留にされた電話機のリージョンとの間で使用するコーデックとして設定されているためです。

コール アドミッション制御と MoH

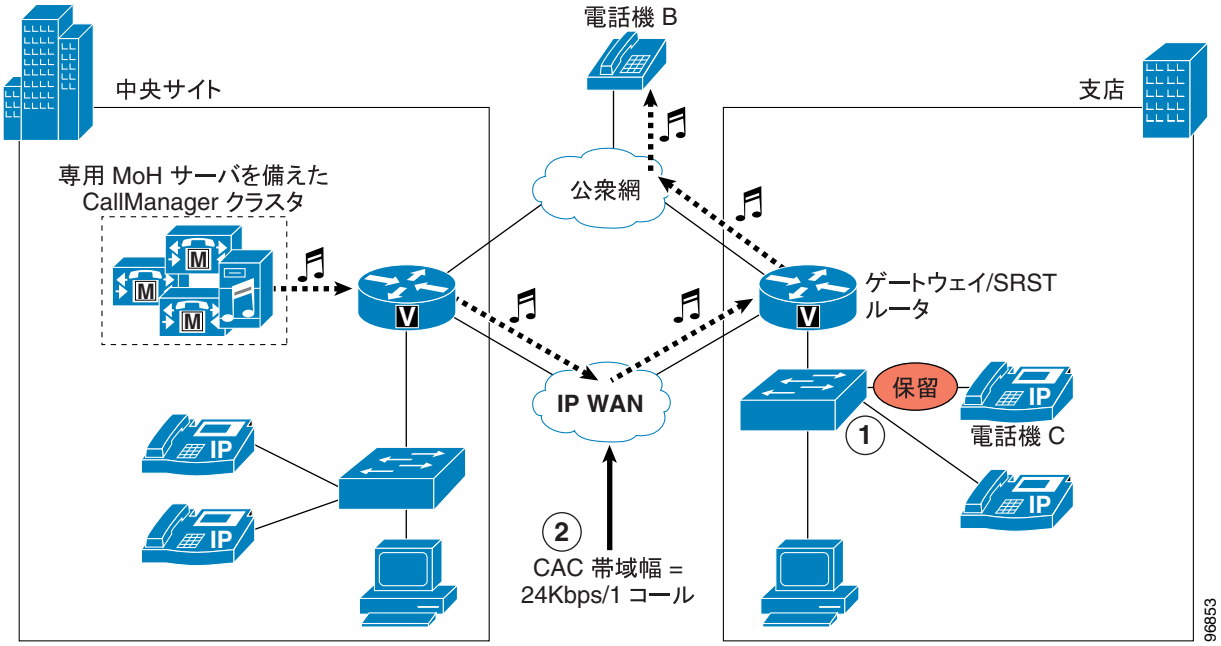
IP テレフォニー トラフィックが WAN リンク上を流れる場合は、コール アドミッション制御（CAC）が必要です。このようなリンク上では使用可能な帯域幅が制限されているので、適切なコール アドミッション制御がないと、音声メディア トラフィックの遅延または損失が起きる可能性が高くなります。詳細については、P.9-1 の「コール アドミッション制御」を参照してください。

Cisco Unified CallManager の（静的ロケーションまたは RSVP 対応ロケーションのいずれかに基づく）コール アドミッション制御は、WAN を通過するユニキャスト MoH ストリームをトラッキングできますが、マルチキャスト MoH ストリームはトラッキングできません。したがって、WAN 帯域幅が完全にサブスクライブされた場合であっても、マルチキャスト MoH ストリームは、コール アドミッション制御によって WAN へのアクセスを拒否されません。ストリームは WAN を介して送信され、その結果、オーディオ ストリームの品質が低下し、WAN を通過するその他のすべてのコールの品質も低下する可能性があります。マルチキャスト MoH ストリームがこのオーバーサブスクリプション状態にならないようにするには、帯域幅を追加して Low-Latency Queuing（LLQ）音声プライオリティ キューを設定することによって、すべてのダウンストリーム WAN インターフェイス上で QoS 設定を余分にプロビジョニングする必要があります。MoH ストリームは単方向であるため、ダウンストリーム インターフェイス（中央サイトからリモート サイトへ）の音声プライオリティ キューのみを余分にプロビジョニングする必要があります。WAN リンクを通過する可能性があるすべての固有マルチキャスト MoH ストリームに対して、十分な帯域幅を追加してください。たとえば、4 つの固有マルチキャスト オーディオ ストリームが WAN を通過する可能性がある場合、音声プライオリティ キューに 96 Kbps を追加します（4 * 24 Kbps（G.729 オーディオ ストリームごと）= 96 Kbps）。

図 7-5 は、集中型マルチサイト配置におけるコール アドミッション制御と MoH の例を示しています。この例の場合、IP Phone C が公衆網電話機（電話機 B）とコール中であると想定します。この時点では、WAN 上で帯域幅は消費されていません。電話機 C で Hold ソフトキーを押すと（ステップ 1）、電話機 B は、WAN を介して中央サイトの MoH サーバから MoH ストリームを受信するので、リンク上の帯域幅を消費します。コール アドミッション制御でこの帯域幅を考慮すべきかどうかは、MoH ストリームのタイプに応じて決まります。マルチキャスト MoH が流れる場合、コール アドミッション制御は、24 Kbps が消費されているとは見なしません（したがって、ダウンストリーム WAN インターフェイス上の QoS はそれに応じてプロビジョニングされなければなりません）。しかし、ユニキャスト MoH が流れる場合、コール アドミッション制御は、使用可能な WAN 帯域幅から 24 Kbps を差し引きます（ステップ 2）。

（注） 上記の例では、ユニキャスト MoH を WAN 上で流すことを示唆しているように見えますが、これは、MoH とのロケーションベースのコール アドミッション制御をわかりやすく示すための例に過ぎません。また、この設定の推奨または保証を意味するものではありません。前述のように、WAN を介した MoH オーディオ ストリームの送信用のトランスポート メカニズムには、マルチキャスト MoH をお勧めします。

図 7-5　ロケーションベースのコール アドミッション制御と MoH



支店ルータのフラッシュからのマルチキャスト MoH

Cisco IOS Release 12.2(15)ZJ および SRST Release 3.0 から、MoH は支店のルータのフラッシュを介して、リモートまたは支店のサイト内でマルチキャストできるようになりました。Cisco IOS ルータのフラッシュからのマルチキャスト MoH は、次の理由で MoH 機能を向上させます。

- 支店のゲートウェイまたはルータが SRST モードのときに、支店のデバイスが中央サイトの Cisco Unified CallManager との接続を失った場合、支店のゲートウェイまたはルータが MoH をマルチキャストします。
- この設定により、WAN を介してリモート支店サイトに MoH を転送する必要がなくなります。ただし、そのためには、WAN が稼働中で、電話機が Cisco Unified CallManager で制御されている場合でも、ローカルに発信される MoH を提供する必要があります。

例 7-1 は、ルータのフラッシュからのマルチキャスト MoH を可能にするために、Cisco IOS ルータ設定（SRST セクションの下）で使用するコマンドを示しています。

例 7-1　支店ルータのフラッシュからのマルチキャスト MoH を有効にする

```
SRST-router(config)#call-manager-fallback
SRST-router(config-cm-fallback)#ip source-address 10.1.1.1
SRST-router(config-cm-fallback)#moh music-on-hold.au
SRST-router(config-cm-fallback)#multicast moh 239.192.240.1 port 16384 route
10.1.1.254
```

例 7-1 では、ルータのフラッシュ上のオーディオ ファイルの名前は music-on-hold.au です。設定されたマルチキャスト アドレスとポート番号は、それぞれ 239.192.240.1 と 16384 です。オプションの **route** コマンドは、マルチキャスト ストリーム用のソース インターフェイス アドレスを指定します。route オプションを指定しない場合、マルチキャスト ストリームは、設定されている SRST のデフォルト アドレスから発信されます。このアドレスは、SRST 設定モードで **ip source-address** コマンドによって指定されたものです。フラッシュから流すことのできるオーディオ ファイルは 1 つのみで、ルータごとに使用可能なマルチキャスト アドレスとポート番号は 1 つのみです。

支店ルータが SRST モードで動作している場合、シャーシ内のすべてのアナログ ポートとデジタル ポートに、マルチキャスト MoH を流すことができます。これによりアナログ電話機および公衆網電話機に MoH を流すことができます。このとき、SRST モードの IP Phone は、SRST ルータのフラッシュからマルチキャスト MoH を受信できないので、代わりに保留音を受け取ります。

(注)　SRST 機能が実際に使用されるかどうかに関係なく、SRST ライセンスが必要です。ライセンスが必要なのは、支店ルータのフラッシュから MoH を流すための設定が SRST 設定モードで行われるため、および SRST 機能が使用されない場合でも少なくとも 1 つの **max-ephones** と 1 つの **max-dn** を設定する必要があるためです。これらの設定コマンドのほか、例 7-1 に示されているコマンドが必要です。

設定後、ルータは、SRST モードでないときでも継続的にフラッシュから MoH ストリームを流します。支店のルータが SRST モードで動作していない場合でも、フラッシュからすべてのローカル デバイス（IP Phone を含む）に MoH をマルチキャストできます。支店のルータに対して、フラッシュからの非 SRST マルチキャスト MoH を設定する方法は、SRST モードでの設定と同じです（例 7-1 を参照）。ただし、ルータに対して設定するマルチキャスト アドレスは、目的の動作によって異なります。フラッシュからのマルチキャスト MoH が SRST モードのみで必要な場合（たとえば、SRST モードでないときに、リモート デバイスで受信する MoH が中央の MoH サーバから発信される場合）は、ルータに対して設定するマルチキャスト アドレスとポート番号が、中央サイトの MoH サーバのオーディオ ソースと重複しないようにする必要があります。重複していると、リモート デバイスは、設定されているユーザ / ネットワーク保留オーディオ ソースに応じて、ローカル ルータのフラッシュから MoH を継続的に受信することがあります。

支店ルータのフラッシュからのマルチキャスト MoH が常に必要になる場合は、支店ルータ上で設定された内容と同じマルチキャスト IP アドレスとポート番号をもつオーディオ ソースを使用して、中央サイトのサーバを設定する必要があります。このシナリオでは、マルチキャスト MoH オーディオ ストリームが、常にルータのフラッシュから発信されるので、中央サイトの MoH サーバのオーディオ ソースが WAN を通過する必要はありません。

中央サイトのオーディオ ストリームが WAN を通過しないようにするには、次のいずれかの方法を使用してください。

- 最大のホップ カウントを設定する

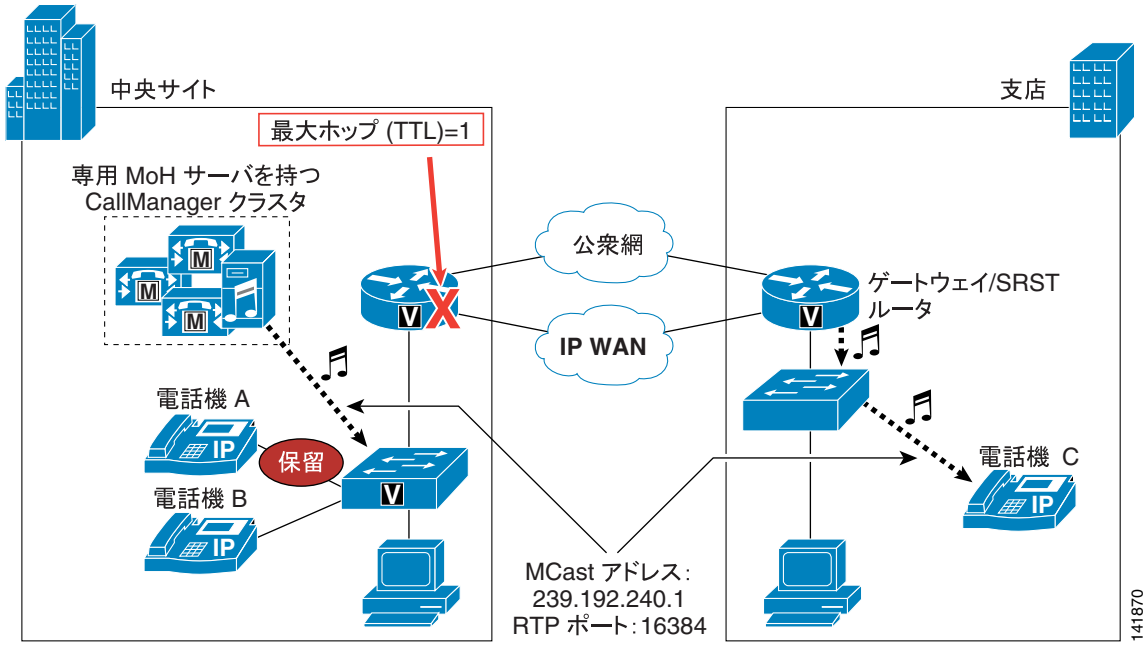
  中央サイトの MoH オーディオ ソースが、中央サイトの LAN より先に流れないように、最大ホップ カウントまたは TTL を十分に小さく設定します。
- WAN インターフェイス上でアクセス コントロール リスト（ACL）を設定する

  中央サイトの WAN インターフェイス上で ACL を設定して、マルチキャスト グループ アドレス宛のパケットがインターフェイスから発信されないようにします。
- WAN インターフェイス上でマルチキャスト ルーティングを無効にする

  WAN インターフェイス上ではマルチキャスト ルーティングを設定しないでください。設定しなければ、マルチキャスト ストリームが WAN に転送されないことが保証されます。

図 7-6 は、SRST モードでないときにリモート ルータのフラッシュからマルチキャスト MoH を流す仕組みを示しています。電話機 A で電話機 C を保留にすると、電話機 C は、ローカル SRST ルータからマルチキャスト MoH を受信します。この図では、MoH サーバは、（RTP ポート 16384 上で）239.192.240.1 にマルチキャスト オーディオ ソースを流します。しかし、最大ホップ数が 1 に制限されているので、このストリームは、ローカル MoH サーバのサブネットから WAN を通過して外に出ないことが保証されています。同時に、支店の SRST ルータまたはゲートウェイは、フラッシュからオーディオ ストリームをマルチキャストします。このストリームも、マルチキャスト アドレスとして 239.192.240.1 を使用し、RTP ポート番号として 16384 を使用します。電話機 A で Hold ソフトキーを押すと、電話機 C は、SRST ルータから発信された MoH オーディオ ストリームを受信します。

図 7-6　支店ルータのフラッシュからのマルチキャスト MoH



この方法を使用してマルチキャスト MoH を配信する場合は、Cisco Unified CallManager クラスタ内のすべてのデバイスが、同じユーザ保留およびネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータに同じマルチキャスト グループ アドレスとポート番号を設定します。保留側のユーザまたはネットワーク保留オーディオ ソースは、オーディオ ソースを特定するときに使用されるため、クラスタ内に複数のユーザまたはネットワーク保留オーディオ ソースを設定する場合、リモートの被保留側が常にローカルの MoH ストリームを受信することを保証する手段はありません。たとえば、中央サイトの電話機に設定されているオーディオ ソースが、そのユーザおよびネットワーク保留オーディオ ソースとして、グループ アドレス 239.192.254.1 を使用するものとします。この電話機がリモート デバイスを保留にすると、ローカル ルータのフラッシュの MoH ストリームがマルチキャスト グループ アドレス 239.192.240.1 に送信される場合でも、リモート デバイスは 239.192.254.1 に加わろうとします。代わりに、ネットワーク内のすべてのデバイスがマルチキャスト グループ アドレス 239.192.240.1 でユーザ / ネットワーク保留オーディオ ソースを使用するように設定し、すべての支店ルータが 239.192.240.1 でフラッシュからマルチキャストするように設定すると、リモート デバイスはすべて、そのローカル ルータのフラッシュから MoH を受信します。

フラッシュからマルチキャスト MoH を流すように設定された複数の支店ルータを含むネットワークでは、クラスタ内に 51 を超える固有 MoH オーディオ ソースを含めることができます。支店サイトの各ルータは、フラッシュから固有オーディオ ソースをマルチキャストできます。ただし、すべてのルータが同じマルチキャスト グループ アドレス上でこのオーディオをマルチキャストする必要があります。また、中央サイトの MoH サーバは、この同じマルチキャスト グループ アドレス上で MoH ストリームをマルチキャストできます。したがって、100 の支店サイトそれぞれがフラッシュからオーディオ ファイルをマルチキャストする場合、クラスタには 101 の固有 MoH オーディオ ソース（100 の支店ストリームと 1 つの中央サイト ストリーム）を含めることができます。中央サイトで複数の固有オーディオ ストリームが必要な場合は、追加の MoH サーバまたは外部メディア サーバから固定 / ライブ ソースを流すことができます（P.7-11 の「複数の固定またはライブ オーディオ ソースの使用」を参照）。ただし、サーバごとに複数のオーディオ ソースを設定しないでください。

分散型マルチサイト配置

分散型コール処理を使用するマルチサイト IP テレフォニー配置には、通常、サイト間の WAN または MAN 接続が含まれます。これらの低速リンクは、通常、帯域幅とスループットの障害になります。リンク上での帯域幅使用量を最小限にするには、リンクを通過するすべての MoH オーディオ ストリームとして G.729 コーデックを使用することをお勧めします。ただし G.729 コーデックは、音楽用ではなく、音声用に最適化されているので、MoH トランスポートに G.729 がもたらす品質の低下よりも、帯域幅の節約がはるかに重要な問題である WAN/MAN 上でのみ、G.729 を使用してください。

集中型マルチサイト配置の場合とは異なり、WAN を介して流れる MoH オーディオ ストリーム用に G.711 が必要になる可能性がある状況では、分散型マルチサイト環境で MoH オーディオ ストリームが G.711 を使用するように強制することはできません。MoH サーバが別の Cisco Unified CallManager リージョンに配置されている状況で、このリージョンとクラスタ間トランクまたは SIP トランクのリージョンとの間で G.711 コーデックが設定されている場合でも、2 つのクラスタ間のコールが一方の電話機によって保留にされたときは、元の音声コールのコーデックが保持されます。これらのクラスタ間コールは、一般に、帯域幅の節約のために G.729 を使用して符号化されるため、一方のクラスタからの MoH ストリームも G.729 を使用して符号化されます。

さらに、Cisco Unified CallManager クラスタ間のコール（クラスタ間コール）では、マルチキャスト MoH はサポートされません。したがって、クラスタ間トランクまたは SIP トランク上で MoH が必要な場合は、各 Cisco Unified CallManager クラスタで少なくとも 1 つのユニキャスト MoH リソースを設定する必要があります。

分散型クラスタ間環境では、適切なマルチキャスト アドレス管理も、設計上の重要な考慮事項です。分散型ネットワーク全体で流れるリソースの重複を防止するために、いかなる MoH オーディオ ソース マルチキャスト アドレスも、配置内のすべての Cisco Unified CallManager クラスタに対して固有でなければなりません。

WAN を介したクラスタ化

その名前が示すように、WAN を介したクラスタ配置には、他のマルチサイト配置と同様、低速 WAN リンクを含みます。したがって、これらの配置にも、G.729 コーデック、マルチキャスト トランスポート メカニズム、および低速 WAN リンクを介した MoH トラフィックに対して欠かせない安定した QoS の、3 つの要件が必要です。

さらに、このタイプの設定では、WAN の各端部に MoH サーバ リソースを配置することも必要です。WAN に障害が発生した場合には、WAN の各端部のデバイスは、ローカルに配置された MoH サーバから、引き続き MoH オーディオ ストリームを受信できます。さらに、適切な MoH 冗長設定がきわめて重要です。WAN の各端部のデバイスには、MRGL を指定する必要があります。この MRGL の MRG には、少なくとも 1 つのローカル リソースが最優先になった MoH リソースの優先順位リストが必要です。プライマリ サーバが使用不能になるか、要求を処理できない場合に備えて、この MRG に対して、MoH リソースを追加設定しておく必要があります。WAN のローカル側のリソースは使用不能になった場合に備えて、リスト内で他に少なくとも 1 つの MoH リソースは、リモート側の MoH リソースを指定しておく必要があります。

ユニキャストとマルチキャスト MoH コール フローの詳細

次の各項では、SCCP および SIP エンドポイントの両方について、ユニキャストとマルチキャスト MoH コール フローの詳細な図と説明を示します。

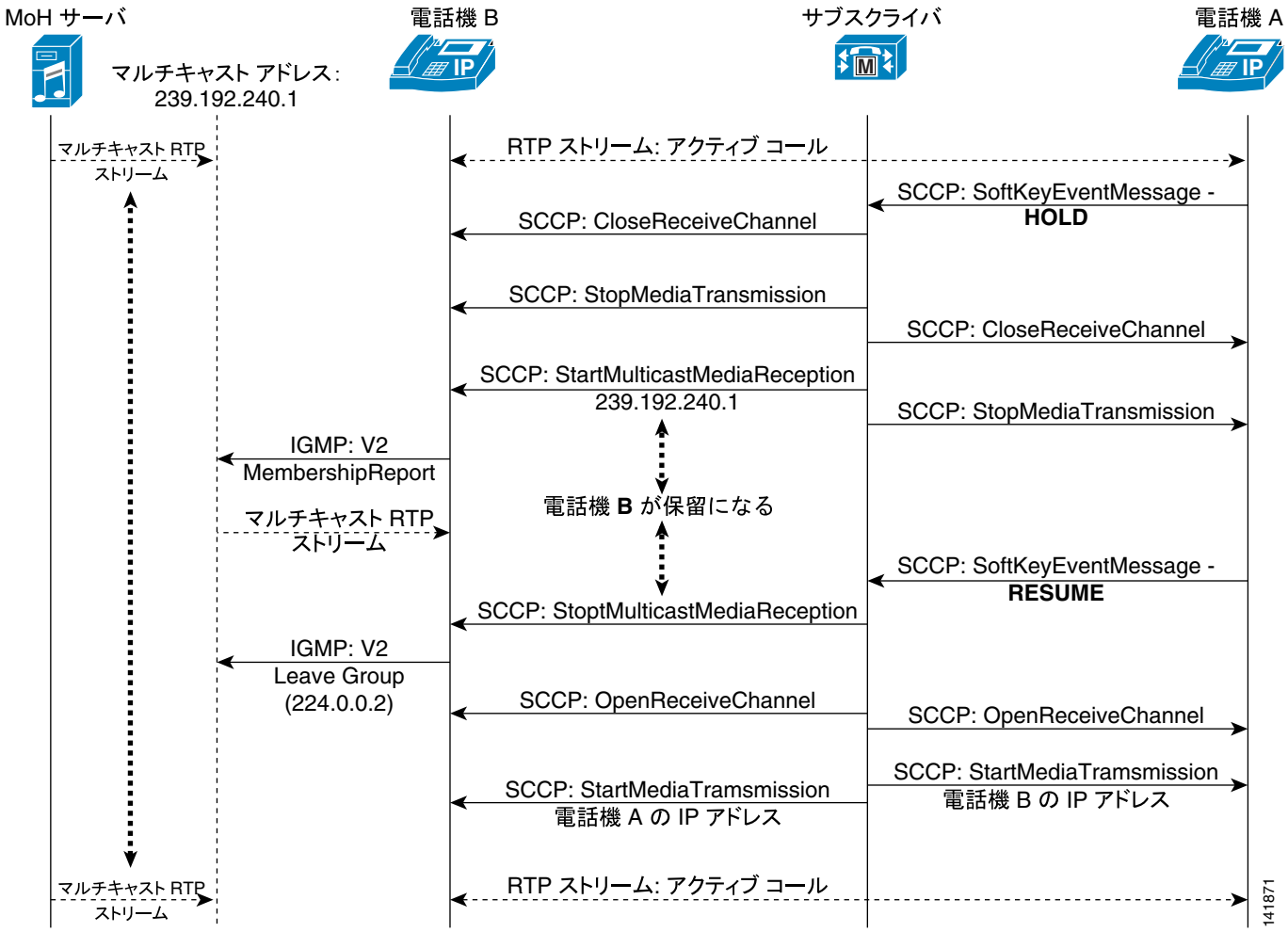
SCCP コール フロー

ここでは、Skinny Client Control Protocol（SCCP）エンドポイントでの Music On Hold のコール フローについて説明します。

SCCP マルチキャスト コール フロー

図 7-7 は、標準的な SCCP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、Cisco Unified CallManager は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。次に、Cisco Unified CallManager は、マルチキャスト グループ アドレス 239.192.240.1 から、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を電話機 B（被保留側）に指示します。その後、電話機 B はインターネット グループ管理プロトコル（IGMP）V2 の Membership Report メッセージを発行して、電話機 B がこのグループに加わることを示します。

図 7-7　SCCP マルチキャスト MoH コール フローの詳細



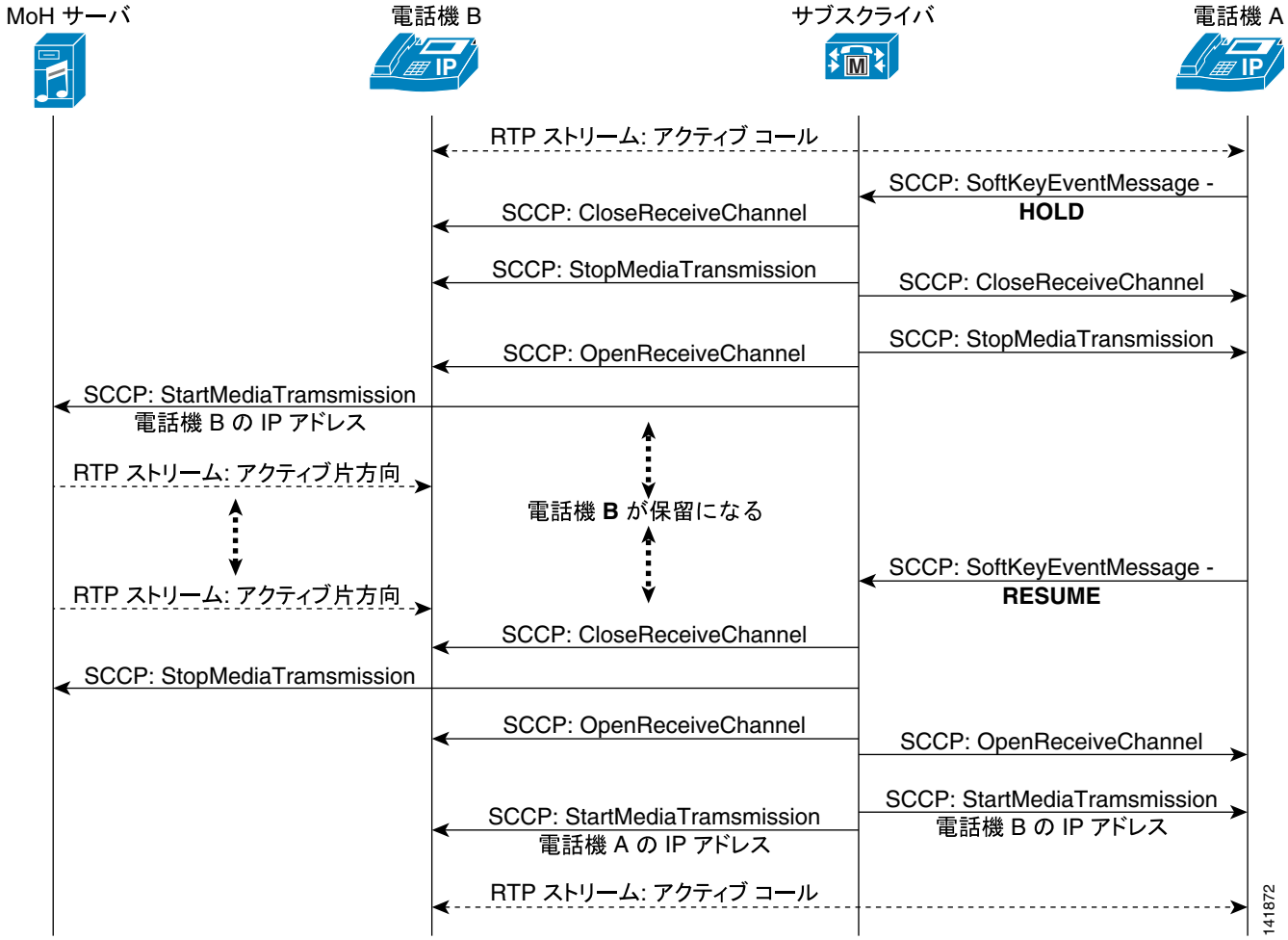
一方、MoH サーバがこのマルチキャスト グループ アドレスに RTP オーディオを発信したので、電話機 B はそのマルチキャスト グループに加わった後、MoH ストリームの受信を開始します。電話機 A で Resume ソフトキーが押されると、Cisco Unified CallManager は、電話機 B に Stop Multicast Media Reception（マルチキャスト メディア受信の停止）を指示します。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。これにより、実質的に MoH セッションが終了します。次に、Cisco Unified CallManager は、電話機 A と電話機 B 間の通話の開始時に送信するように、両方の電話機に一連の Open Receive Channel（受信チャネルのオープン）メッセージを送信します。その後すぐに、Cisco Unified CallManager は、互いの IP アドレスへの Start Media Transmission（メディア送信の開始）を両方の電話機に指示します。電話機は、RTP 双方向オーディオ ストリームを介して再び接続されます。

（注）　図 7-7 と図 7-8 のコール フロー図では、双方向 RTP オーディオ ストリームを使用して、初期化コールが電話機 A と電話機 B の間で行われることを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、確認応答、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される Hold ソフトキー アクションです。

SCCP ユニキャスト コール フロー

図 7-8 は、SCCP ユニキャスト MoH コール フローを示しています。このコール フロー図では、電話機 A で Hold ソフトキーが押されると、Cisco Unified CallManager は、Close Receive Channel（受信チャネルのクローズ）と Stop Media Transmission（メディア送信の停止）を電話機 A と電話機 B の両方に指示します。このアクションは、実質的に、RTP 双方向オーディオ ストリームを停止させます。この時点まで、ユニキャストとマルチキャストの MoH コール フローは、まったく同じように動作します。

図 7-8　SCCP ユニキャスト MoH コール フローの詳細



次に、Cisco Unified CallManager は、Open Receive Channel（受信チャネルのオープン）を電話機 B（被保留側）に指示します。これは、マルチキャストの場合とまったく異なっています。マルチキャストでは、Cisco Unified CallManager は、Start Multicast Media Reception（マルチキャスト メディア受信の開始）を被保留側に指示します。次に、Cisco Unified CallManager は、MoH サーバに、電話機 B の IP アドレスへの Start Media Transmission（メディア送信の開始）を指示します。これも、マルチキャスト MoH コール フローとはまったく異なる動作です。マルチキャストの場合、マルチキャスト グループ アドレスに加わるように、電話機に指示します。この時点で、MoH サーバは、片方向ユニキャスト RTP 音楽ストリームを電話機 B に送信します。電話機 A で Resume ソフトキーが押されると、Cisco Unified CallManager は、Stop Media Transmission（メディア送信の停止）を MoH サーバに指示し、Close Receive Channel（受信チャネルのクローズ）を電話機 B に指示して、実質的に MoH セッションを終了させます。マルチキャスト シナリオの場合と同じように、Cisco Unified CallManager は、一連の Open Receive Channel（受信チャネルのオープン）メッセージおよび Start Media Transmissions（メディア送信の開始）メッセージを電話機 A と電話機 B に相互の IP アドレスを使用して送信します。電話機は、RTP 双方向オーディオ ストリームを介して再び接続されます。

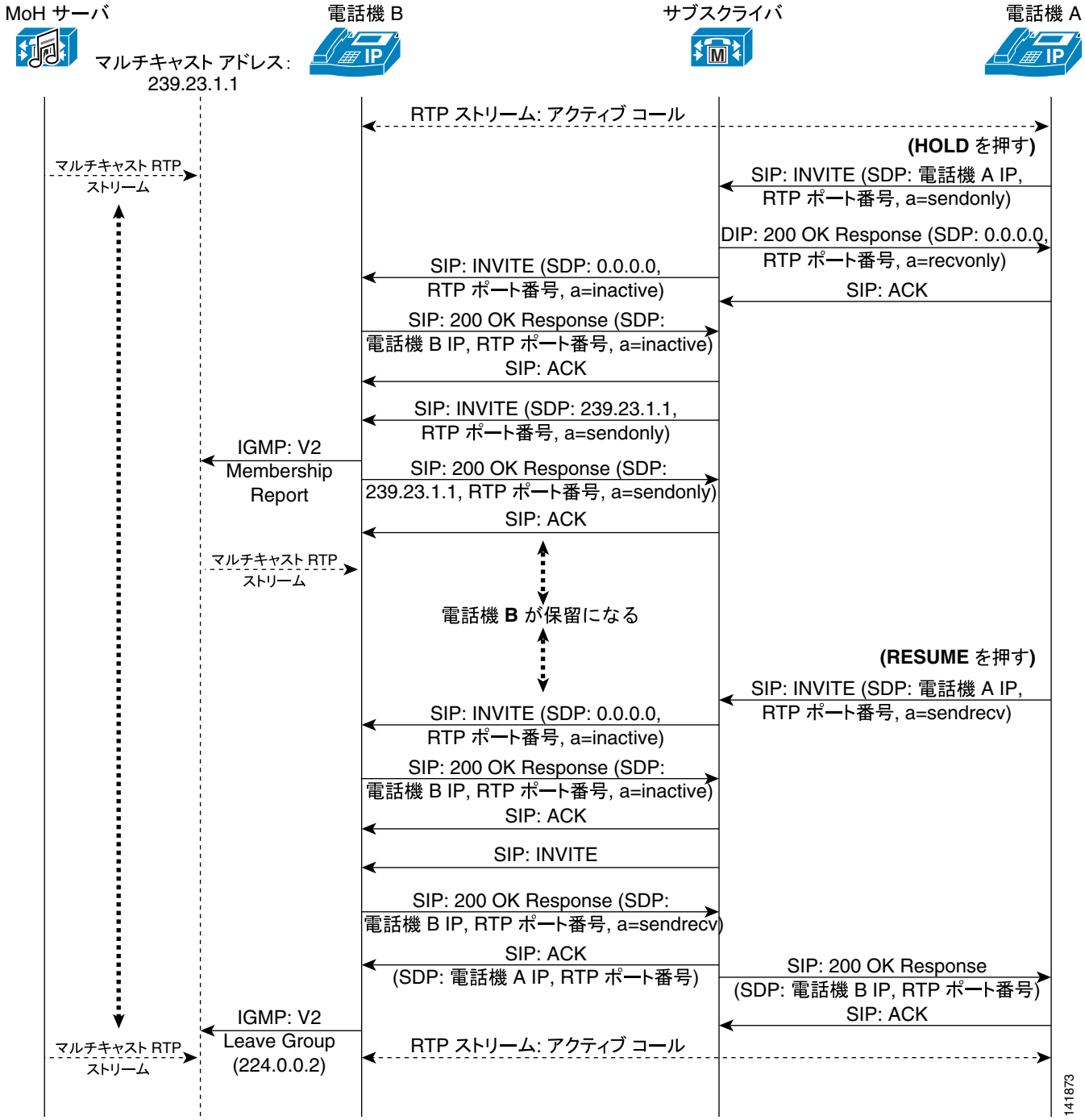
SIP コール フロー

ここでは、Session Initiation Protocol（SIP）エンドポイントでの Music On Hold のコール フローについて説明します。

SIP マルチキャスト コール フロー

図 7-9 は、標準的な SIP マルチキャスト コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの Session Description Protocol（SDP）接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Cisco Unified CallManager は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response を介して、RTP ストリームを切断するように電話機 A に指示します。電話機 B は、Cisco Unified CallManager からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。電話機 B から Cisco Unified CallManager に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されると、Cisco Unified CallManager は SIP INVITE を電話機 B に送信します。このときの SDP 接続情報は MoH マルチキャスト グループ アドレス（この場合は 239.23.1.1）を示し、メディア属性は sendonly です。

図 7-9　SIP マルチキャスト MoH コール フローの詳細



次に、図 7-9 の電話機 B は IGMP V2 の Membership Report メッセージを発行して、電話機 B がこのマルチキャスト グループに加わることを示します。さらに、電話機 B は、前の SIP INVITE に応答して、SDP メディア属性が sendonly を示す SIP 200 OK Response を Cisco Unified CallManager に返します。一方、MoH サーバがこの MoH マルチキャスト グループ アドレスに RTP オーディオを発信したので、電話機 B はそのマルチキャスト グループに加わった後、一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Cisco Unified CallManager は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE を介して、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Cisco Unified CallManager に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。

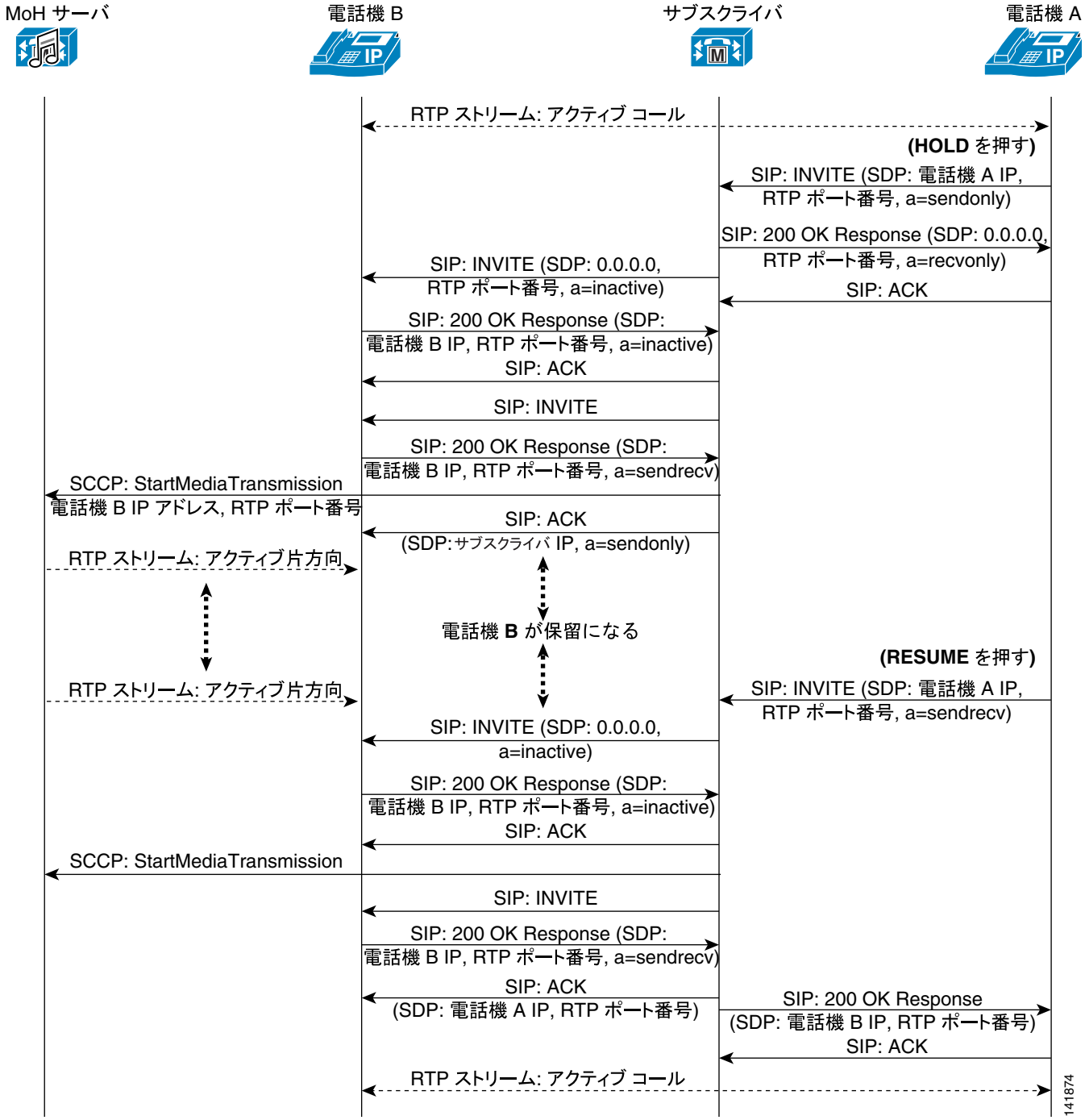
次に、Cisco Unified CallManager は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Cisco Unified CallManager はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Cisco Unified CallManager は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号です。電話機 B は、マルチキャスト ストリームが必要なくなったことを示すために、IGMP V2 の Leave Group メッセージを 224.0.0.2 に送信します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

（注） 図 7-9、図 7-10、および図 7-11 のコール フロー図では、双方向 RTP オーディオ ストリームを使用して、初期化コールが電話機 A と電話機 B の間で行われることを前提としています。これらの図は、コール フローを示しているので、適切な MoH 動作に必要な関連トラフィックのみが記載されています。したがって、インタラクションがわかりやすいように、キープアライブ、一部の確認応答、進行状況表示、およびその他のトラフィックは省略されています。各図の初期化イベントは、電話機 A によって実行される Hold ソフトキー アクションです。

SIP ユニキャスト コール フロー

図 7-10 は、SIP ユニキャスト MoH コール フローを示しています。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は sendonly を示しています。Cisco Unified CallManager は、SDP 接続情報が 0.0.0.0、メディア属性が recvonly を示す SIP 200 OK Response を介して、RTP ストリームを切断するよう電話に機 A に指示します。電話機 B は、Cisco Unified CallManager からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Cisco Unified CallManager に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。この時点まで、ユニキャストとマルチキャストの MoH コール フローはまったく同じです。

図 7-10　SIP ユニキャスト MoH コール フローの詳細



Cisco Unified CallManager は電話機 B に SIP INVITE を送信し、電話機 B は、それに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Cisco Unified CallManager は、SCCP の StartMediaTransmission メッセージを MoH サーバに送信して、電話機 B のアドレスおよび受信 RTP ポート番号を伝えます。この後、Cisco Unified CallManager から電話機 B への SIP ACK が続き、このときの SDP 接続情報には Cisco Unified CallManager の IP アドレス、メディア属性には sendonly が示されます。一方、MoH サーバが RTP オーディオの発信を開始したので、電話機 B は一方向 MoH ストリームの受信を開始します。

電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートおよび sendrecv を示しています。Cisco Unified CallManager は、SDP 接続情報が 0.0.0.0、メディア属性が inactive を示す SIP INVITE を介して、電話機 B にマルチキャスト MoH ストリームから切断するように指示します。電話機 B から Cisco Unified CallManager に、SDP メディア属性が inactive を示す SIP 200 OK Response が返されます。その後、Cisco Unified CallManager は、SCCP の StopMediaTransmission メッセージを MoH サーバに送信します。これによって、MoH サーバは電話機 B への MoH ストリームの転送を停止します。

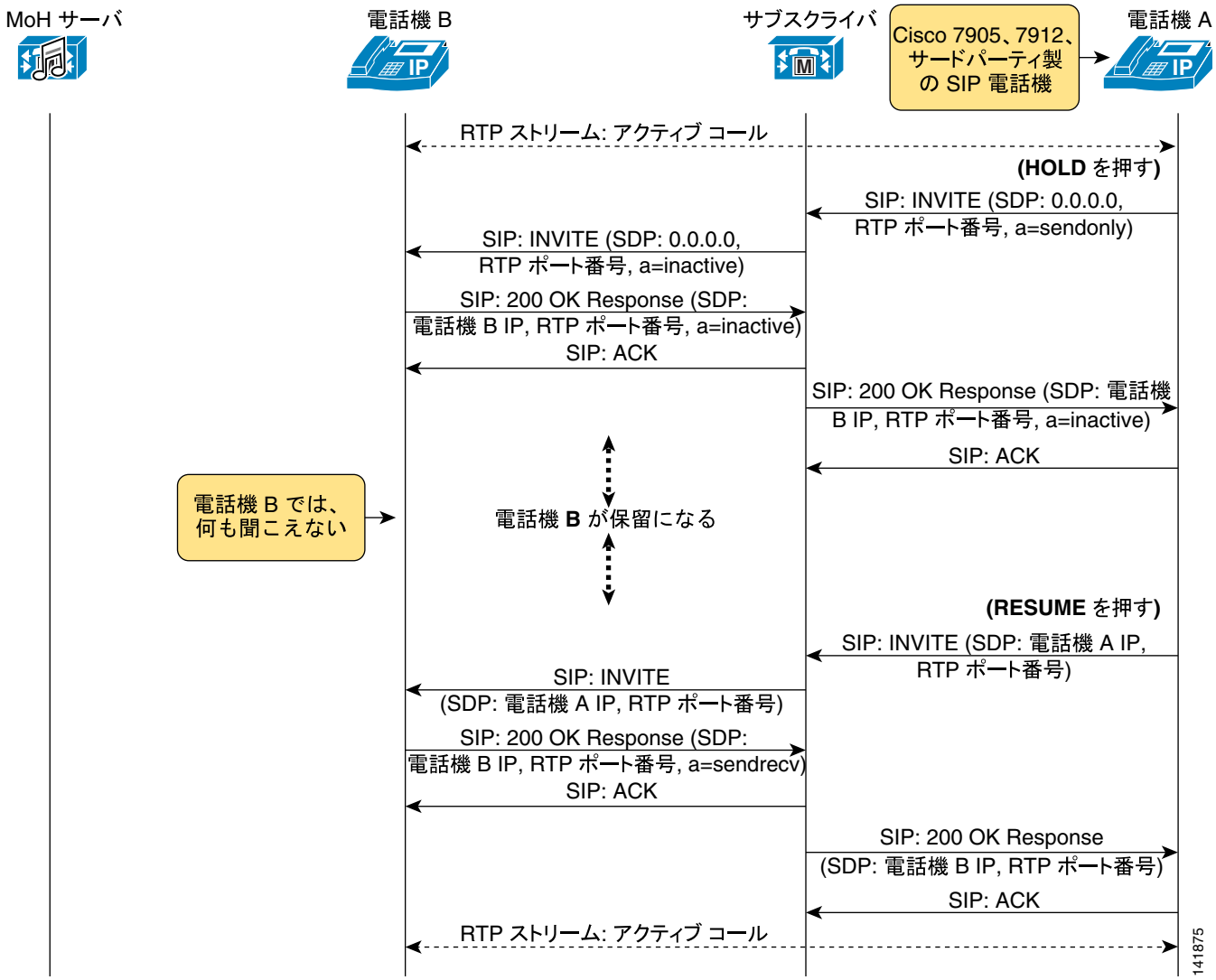
次に、Cisco Unified CallManager は電話機 B に SIP INVITE を送信し、電話機 B はそれに対して、SDP 接続情報が電話機 B の IP アドレスを示し、メディア属性が電話機 B の受信 RTP ポートおよび sendrecv を示す SIP 200 OK Response で応答します。Cisco Unified CallManager はそれに応答し、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポート番号の SIP ACK を電話機 B に送信します。同様に、Cisco Unified CallManager は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートです。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

SIP メディア保留コール フロー

図 7-11 は、RFC 2543 のメディア保留コール フローを示しています。このコール フローが発生するのは、コールを保留にする電話機（この場合は電話機 A）が Cisco Unified IP Phone 7905、7912、またはサードパーティ製の SIP 電話機の場合だけです。この図に示されているように、電話機 A で Hold ソフトキーが押されると、電話機 A は SIP INVITE を送信します。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は sendonly を示しています。電話機 B は、Cisco Unified CallManager からの SIP INVITE を介して RTP ストリームを切断するように指示されます。このときの SDP 接続情報は 0.0.0.0 を示し、メディア属性は inactive です。次に、電話機 B から Cisco Unified CallManager に SIP 200 OK Response が返されます。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポート番号および inactive を示します。そして、Cisco Unified CallManager は、電話機 A の最初の保留 SIP INVITE に応答して、SIP 200 OK Response を電話機 A に返します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび inactive を示します。

この時点で、電話機 B は保留状態ですが MoH を受信していないため、電話機 B のユーザには何も聞こえません。

図 7-11　SIP メディア保留コール フローの詳細



電話機 A のユーザが Resume ソフトキーを押すと、電話機 A は、SIP INVITE を送信します。このときの SDP 接続情報は電話機 A の IP アドレスを示し、メディア属性は電話機 A の受信 RTP ポートを示しています。次に、Cisco Unified CallManager は、SDP 接続情報が電話機 A の IP アドレスを示し、メディア属性が電話機 A の受信 RTP ポートを示す SIP INVITE を電話機 B に送信します。それに対して、電話機 B が SIP 200 OK Response で応答します。このときの SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートおよび sendrecv を示します。同様に、Cisco Unified CallManager は、SIP 200 OK Response を電話機 A の最初の保留解除 SIP INVITE に転送します。この応答の SDP 接続情報は電話機 B の IP アドレスを示し、メディア属性は電話機 B の受信 RTP ポートを示します。最後に、電話機 A と電話機 B の間に RTP 双方向オーディオ ストリームが再確立されます。

(注)　メディア保留が以上のように発生するのは、Cisco Unified IP Phone 7905 または 7912 およびサードパーティ製の SIP 電話機がコールを保留にする場合だけです。また、これらの電話機は、他の Cisco Unified IP Phone モデルによって保留にされたときに MoH を受信し、そのシナリオのコール フローは、図 7-9 および図 7-10 に示したフローとほぼ同じようになります。

CHAPTER 8

コール処理

この章では、Cisco Unified CallManager 5.0 におけるスケーラブルで復元性のあるコール処理システムの設計ガイドラインを示します。ここでは、次に示す個々の要件に基づいて、Cisco Unified CallManager に適切なハードウェアおよび配置シナリオを選択する方法についても説明します。

- 規模：ユーザ、ゲートウェイ、アプリケーションなどの数
- パフォーマンス：コールのレート
- 復元性：冗長性の規模

この章では、次のトピックについて説明します。

- Cisco Unified CallManager クラスタのガイドライン（P.8-2）

  ここでは、Cisco Unified CallManager の最小ハードウェア要件について説明します。また、Cisco Unified CallManager サーバで有効にすることができる各種の機能サービス、およびそれぞれの目的についても説明します。

- Cisco Unified CallManager プラットフォームのキャパシティ プランニング（P.8-16）

  ここでは、Cisco CallManager キャパシティ ツールの使用に関するガイドラインを示します。このツールは、IP テレフォニー配置のプランニング時に使用する必要があります。Cisco CallManager キャパシティ ツールは、特定の配置要件に基づいて、Cisco Unified CallManager サーバ上で使用されるリソースについてのガイダンスを提供します。

- ゲートキーパーの設計上の考慮事項（P.8-22）

  ここでは、IP テレフォニー配置でゲートキーパーをどのように使用できるかについて説明します。シスコのゲートキーパーは、もう 1 台のスタンバイ ゲートキーパーとペアにすることも、クラスタ化してさらに高いパフォーマンスと復元性を実現することもできます。ゲートキーパーは、コール ルーティングとコール アドミッション制御に使用することもできます。

- Cisco Unified CallManager と CallManager Express の相互運用性（P.8-33）

  ここでは、分散型コール処理配置における Cisco Unified CallManager と Cisco Unified CallManager Express 間での H.323 と SIP の統合について説明します。

Cisco Unified CallManager クラスタのガイドライン

Cisco Unified CallManager アーキテクチャでは、複数の物理サーバを 1 つの IP PBX システムとして連携させることができます。このサーバ グループを「クラスタ」と呼びます。Cisco Unified CallManager サーバのクラスタは、設計上の制限事項を遵守している限り、IP ネットワークを介して分散していてもかまいません。クラスタを使用することで、空間的な冗長性、およびそれに伴う復元性を IP Communications システムの設計にもたらすことができます。

ここでは、Cisco Unified CallManager クラスタを形成しているサーバが実行する各種の機能について説明し、必要な規模、パフォーマンス、および復元性を達成するようにサーバを配置する方法について、ガイドラインを示します。

ハードウェア プラットフォーム

Cisco Unified CallManager クラスタでは、必要となる規模、パフォーマンス、および冗長性に応じて、さまざまなタイプのサーバを利用します。利用するサーバの範囲は、冗長性のないシングル プロセッサのサーバから、冗長性の高いマルチプロセッサ ユニットにまで及びます。

表 8-1 では、クラスタ内で使用できる一般的なサーバのタイプとその主な特性を一緒にリストしています。

表 8-1　Cisco Unified CallManager サーバのタイプ

サーバ タイプ	Cisco サーバ モデル	特性
標準サーバ（高可用性でない）	MCS 7815 または同等のサーバ	• 単一プロセッサ • 単一電源装置 • 非 RAID ハードディスク
高可用性標準サーバ	MCS 7825 または同等のサーバ	• 単一プロセッサ • 複数の電源装置 • 単一 SCSI RAID ハードディスク アレイ
高性能サーバ	MCS 7835 および MCS 7845 または同等のサーバ	• 複数のプロセッサ • 複数の電源装置 • 複数の SCSI RAID ハードディスク アレイ

Cisco Unified CallManager 5.0 は、特定の Cisco MCS 7815、MCS 7825、MCS 7835、および MCS 7845 の各サーバでサポートされます。あるいは、シスコですでに確認されている、次の最小要件を満たすサーバであれば、お客様が用意した HP サーバおよび IBM サーバでもサポートされます。

- プロセッサ速度：2.0 GHz 以上
- 物理メモリ サイズ：2 GB 以上
- 物理ハード ディスク サイズ：72 GB 以上

現在サポートされているハードウェア コンフィギュレーションの全リストについては、次の Web サイトにあるドキュメントを参照してください。

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

サーバは、IP ネットワークに加えて電源と冷却についても可用性の高い環境に配置する必要があります。建物の電力が必要な可用性を備えていない場合は、サーバの電力を無停電電源装置（UPS）から供給する必要があります。二重化電源を備えたサーバについても、それぞれの電源を 2 つの異なる電力源に接続しておくと、1 つの電源回路が故障しただけでサーバに障害が発生することを回避できます。

IP ネットワークへの接続性によっても、最大限のパフォーマンスと可用性が保証されます。Cisco Unified CallManager サーバは、イーサネットに 100 Mbps 全二重で接続する必要があります。小規模な配置で 100 Mbps が使用可能でない場合、10 Mbps 全二重を使用してください。多くのサーバはオプションとして、ギガビット イーサネットを使用する機能も備えています。サーバが全二重を使用してネットワークに接続していることを確認してください。全二重接続は、スイッチ ポートおよびサーバ NIC の設定で 10 Mbps と 100 Mbps が可能です。1000 Mbps の場合は、NIC およびスイッチ ポートの両方で速度とデュプレックス モードの設定に Auto/Auto を使用することをお勧めします。Cisco Unified CallManager 5.0 のデフォルトは Auto/Auto で、この設定は以前の Cisco Unified CallManager リリースからアップグレード後のデフォルトでもあります。

(注)　サーバ ポートまたはイーサネット スイッチ ポートのどちらか一方が Auto モードのままであり、もう一方のポートが手動で設定される場合、ミスマッチが生じます。ベスト プラクティスは、サーバ ポートとイーサネット スイッチ ポートの両方を手動で設定することです。ただし、ギガビット イーサネット ポートの場合は、Auto/Auto に設定する必要があります。

ネットワークの耐障害性に対応する NIC チーミング

2 枚のイーサネット ネットワーク インターフェイス カード（NIC）を備えた Hewlett-Packard（HP）サーバ プラットフォームは、Cisco Unified CallManager 5.0 でのネットワークの耐障害性に対応する NIC チーミングをサポートできます。この機能は、サーバを 2 枚の NIC、つまり 2 本のケーブルでイーサネットに接続できるようにするものです。NIC チーミングは、障害の発生したポートから正常なポートに作業負荷を転送することによって、ネットワークのダウンタイムを防止します。NIC チーミングは、ロード バランシングまたはインターフェイス速度向上用には使用できません。

クラスタリングに関する一般的なガイドライン

すべての Cisco Unified CallManager クラスタに次のガイドラインが適用されます。

(注)　1 つのクラスタに複数のサーバ プラットフォームを組み合せることができますが、クラスタ内のすべてのサーバでは、同じ Cisco Unified CallManager ソフトウェア リリースを実行する必要があります。

- 通常の環境では、同一 LAN または MAN 内にクラスタのすべてのメンバーを入れます。クラスタのすべてのメンバーを同一の VLAN またはスイッチに配置することは、お勧めしません。
- 冗長性を持たせるには、クラスタのメンバーを次のように配置して、インフラストラクチャや建物で発生した障害によって受ける影響を最小限に抑える必要があります。
  - 同じディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 複数のディストリビューション スイッチまたはコア スイッチに、複数のアクセス スイッチが接続されている
  - 同じ LAN または MAN の中に複数の建物がある
- クラスタが IP WAN にわたって構築されている場合、P.2-19 の「IP WAN を介したクラスタ化」の項を参照して、IP WAN を介したクラスタリングのガイドラインに従ってください。

Cisco Unified CallManager クラスタのサービス

Cisco Unified CallManager クラスタの内部には、それぞれ固有のサービスを提供する複数のサーバが存在します。これらの各サービスは、同じ物理サーバ上で他のサービスと共存できます。たとえば、小規模なシステムでは、1 台のサーバがデータベース パブリッシャ、バックアップ サブスクライバ、Music On Hold（MoH）サーバ、TFTP サーバ、CTI Manager、およびコンファレンス ブリッジを兼ねることができます。クラスタの規模とパフォーマンスを強化する必要が高まった場合は、これらのサービスの多くを 1 台の専用物理サーバに移行する必要があります。

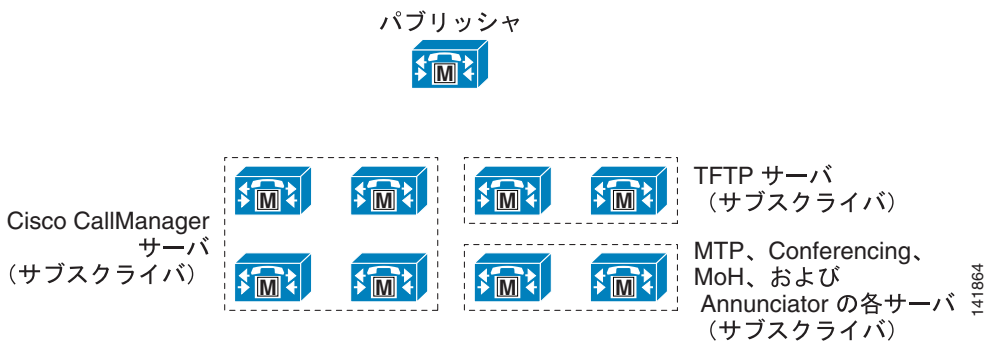
Cisco Unified CallManager 5.0 からは、1 つのクラスタに、20 のサーバを組み込めるようになりました。20 のサーバのうち、最大 8 つのサーバが、コール処理を提供する Cisco CallManager サービスを実行できます。残りのサーバは、専用データベース パブリッシャ、トリビアル ファイル転送プロトコル（TFTP）専用サーバ、または Music On Hold（MoH）サーバとして設定できます。メディア ストリーミング アプリケーション（コンファレンス ブリッジやメディア ターミネーション ポイント）も、クラスタに登録される別個のサーバにインストールできます。

Cisco MCS 7815 または同等のサーバを含んだクラスタを配置するときは、クラスタ内に最小限 2 台のサーバが必要です。1 台をパブリッシャ、TFTP サーバ、バックアップ コール処理サーバにし、もう 1 台をプライマリ コール処理サーバにします。Cisco MCS 7815 上では、この構成で最大 300 台の電話機がサポートされます。これよりキャパシティの大きいサーバを使用して 2 サーバ クラスタを配置する場合も、クラスタ内のユーザ数が 1,250 を超えないようにすることをお勧めします。1,250 ユーザを超える場合は、専用パブリッシャと別個のサーバをプライマリおよびセカンダリのコール処理サービス用にお勧めします。そのため、クラスタ内のサーバ数が増えます。

MCS 7825 以上のサーバを備えたシングル サーバ クラスタを配置することもできます。MCS 7825 または同等のサーバでは、上限は 500 ユーザです。これより可用性の高いサーバを使用する場合も、シングル サーバ クラスタのユーザ数が 1,000 を超えないようにする必要があります。シングル サーバ構成では、Survivable Remote Site Telephony（SRST）も配置して、Cisco Unified CallManager が使用不可になっている間にサービスが提供されるようにしない限り、冗長性はありません。シスコでは、実稼働環境でシングル サーバ配置を採用することはお勧めしません。ロード バランシングは、パブリッシャがバックアップ コール処理サブスクライバである場合には実装できません。

図 8-1 では、一般的な Cisco Unified CallManager クラスタを示しています。

図 8-1　一般的な Cisco Unified CallManager クラスタ

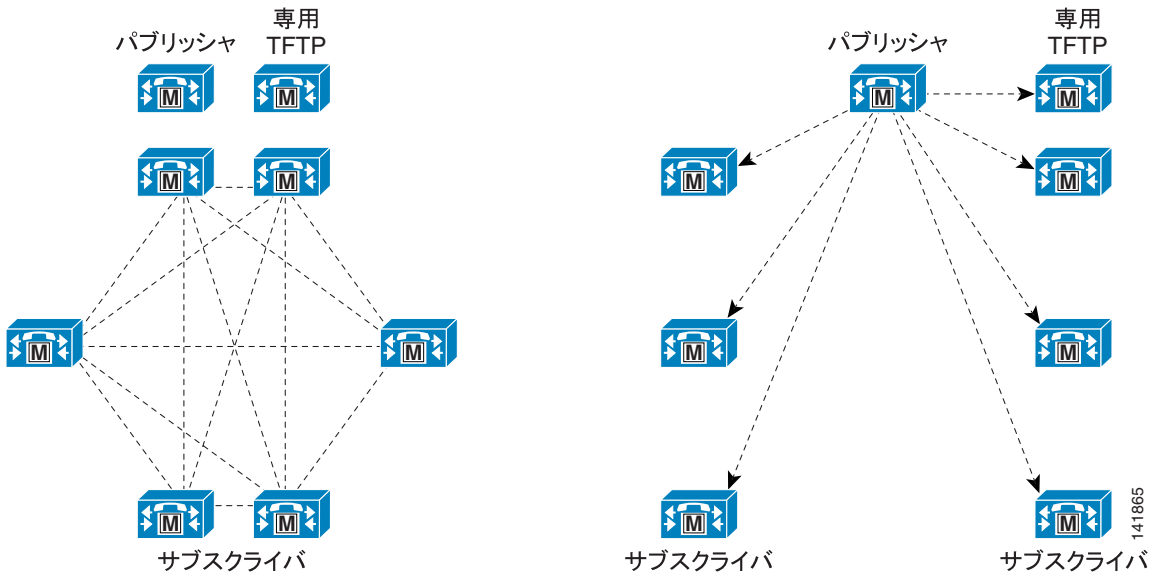


クラスタ内通信

Cisco Unified CallManager クラスタ内の通信（クラスタ内通信）には、2 種類あります（図 8-2 を参照）。1 つは、すべてのデバイス設定情報を含んでいるデータベースを配布するためのメカニズムです（図 8-2 の「データベース複製」を参照）。コンフィギュレーション データベースは、パブリッシャ サーバに保存され、読み取り専用のコピーがクラスタのサブスクライバ メンバーに複製されます。パブリッシャで加えられた変更は、サブスクライバ データベースに伝達され、クラスタのメンバー全体で設定を一貫させると共に、データベースの空間的な冗長性を実行します。

もう 1 つのクラスタ内通信は、デバイスの登録、ロケーションの帯域幅、共有メディア リソースなどのランタイム データの伝搬と複製です（図 8-2 の「ICCS」を参照）。この情報は、Cisco Unified CallManager Service を実行している、クラスタのすべてのメンバー全体で共有されます。クラスタのメンバーと関連ゲートウェイとの間で、コールの最適なルーティングが確保されます。

図 8-2　クラスタ内通信

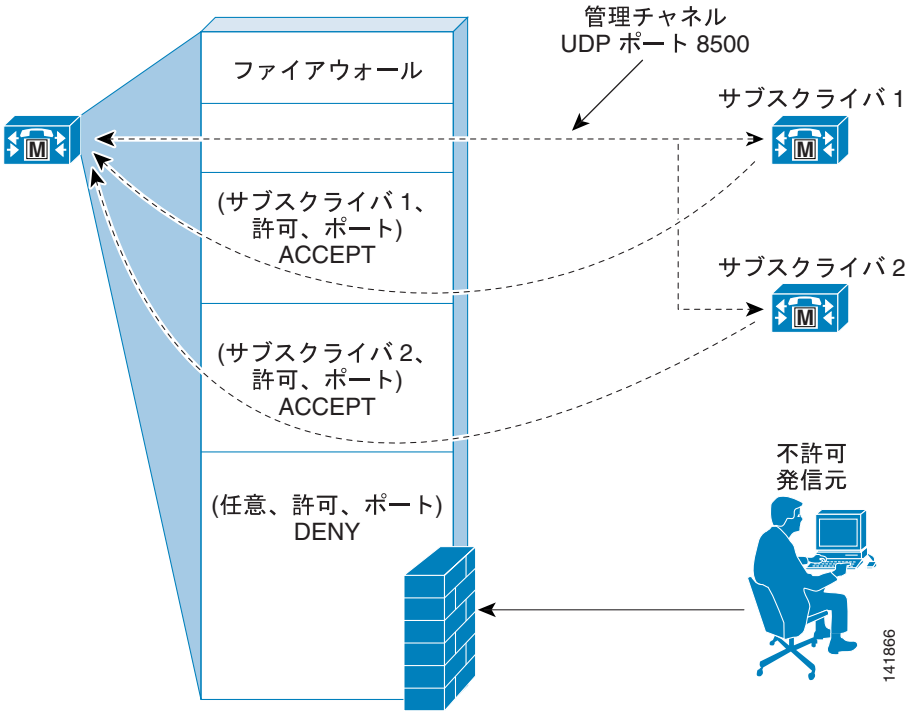


Intra-Cluster Communication Signaling (ICCS)　　データベース複製

クラスタ内セキュリティ

Cisco Unified CallManager 5.0 からは、Cisco Unified CallManager アプリケーションおよび通信リンクの保護のために、異なるアーキテクチャとメカニズムが実装されています。クラスタ内の各サーバが内部で動的ファイアウォールを実行します。Cisco Unified CallManager のアプリケーション ポートは、送信元 IP フィルタリングを使用して保護されます。動的ファイアウォールは、認証済みサーバまたは信頼できるサーバに対してだけ、これらのアプリケーション ポートを開きます（図 8-3 を参照）。

図 8-3　クラスタ内セキュリティ



このセキュリティ メカニズムは、単一の Cisco Unified CallManager クラスタ内のサーバ間にのみ適用できます。Cisco Unified CallManager のサブスクライバは、パブリッシャのデータベースにアクセスする前に、クラスタ内で認証されます。クラスタ内通信およびデータベース複製は、認証済みサーバ間でのみ発生します。インストール時にサブスクライバは、事前共有キー認証メカニズムでパブリッシャに対して認証されます。認証プロセスに必要な手順は次のとおりです。

1. セキュリティ パスワードを使用してパブリッシャ サーバをインストールします。
2. Cisco Unified CallManager Administration を使用することによって、パブリッシャ上にサブスクライバ サーバを設定します。
3. パブリッシャ サーバのインストール時に使用されたのと同じセキュリティ パスワードを使用して、サブスクライバ サーバをインストールします。
4. サブスクライバのインストール後、サーバは、UDP 8500 を使用する管理チャネル上でパブリッシャとの接続を確立しようとします。サブスクライバは、たとえば、ホスト名、IP アドレスなどのすべてのクレデンシャルをパブリッシャに送信します。クレデンシャルは、インストール時に使用されたセキュリティ パスワードを使用して認証されます。
5. パブリッシャは、独自のセキュリティ パスワードを使用してサブスクライバのクレデンシャルを確認します。

6. その情報が有効な場合、パブリッシャは、自身の動的ファイアウォール テーブルに、信頼できる送信元としてサブスクライバを追加します。サブスクライバは、データベースへのアクセスを許可されます。
7. サブスクライバは、パブリッシャから他のサブスクライバ サーバのリストを取得します。すべてのサブスクライバが互いに管理チャネルを確立し、メッシュ トポロジが作成されます。

パブリッシャ

パブリッシャはすべてのクラスタに必要なサーバで、現在はクラスタごとに 1 つのみ配置できます。このサーバは、最初にインストールする必要があります。クラスタ内の他のすべてのメンバーに対して、データベース サービスを提供します。パブリッシャ サーバは、コンフィギュレーション データベースに読み取りと書き込みのアクセスができる唯一のサーバです。設定が変更されたとき、クラスタの他のメンバーは、データベースの読み取り専用コピーを保持します。1,250 ユーザを超える大規模なシステムの場合には、管理操作によるテレフォニー ユーザへの影響を防止するために、専用パブリッシャをお勧めします。専用パブリッシャのサーバ上で、コール処理サービスまたは TFTP サービスが実行されることはありません。それ以外のサーバは、TFTP および Cisco Unified CallManager サービスを実行します。

クラスタ内のサーバは、初期化時にパブリッシャのデータベースを使用しようとします。パブリッシャが使用不可になっている場合は、自身のハード ドライブにあるローカルの読み取り専用コピーを使用します。

システムが動作していても、パブリッシャが使用不可になっている場合は、次の操作を実行できません。

- 自動転送の変更
- ライセンス サービスを必要とする操作
- 設定の変更
- エクステンション モビリティのログイン操作およびログアウト操作

エクステンション モビリティは、データベースに読み取りと書き込みのアクセスを行う必要があるため、パブリッシャなしでは機能しません。したがって、このサービスはパブリッシャ上でのみ実行することをお勧めします。

パブリッシャ用のハードウェア プラットフォームは、クラスタの規模とパフォーマンスを基準として選択します。パブリッシャは、コール処理サブスクライバと同等のパフォーマンスを持つものにすることをお勧めします。可能な場合には、パブリッシャを高可用性サーバにして、ハードウェアの障害による影響を最小限に抑えるようにします。

コール処理サブスクライバ

Cisco Unified CallManager ソフトウェアをインストールするときに、パブリッシャとサブスクライバという 2 タイプのサーバを定義できます。これらの用語は、データベース間の関係をインストール時に定義するために使用されています。ソフトウェアをインストールしたときに使用可能になるのは、データベース サービスとネットワーク サービスだけです。すべてのサブスクライバは、パブリッシャをサブスクライブして、データベース情報の読み取り専用コピーを取得します。

コール処理サブスクライバは、Cisco CallManager Service が使用可能になっているサーバです。このサービスをサブスクライバ上で使用可能にするには、シングル サーバ ライセンスが必要です。パブリッシャが使用不可になっていると、サーバ上で Cisco CallManager Service を使用可能にできません。パブリッシャはライセンス サーバとして機能し、Cisco CallManager Service をアクティブにするために必要なライセンスを配布するからです。このサービスが使用可能になった時点で、このサーバはコール処理機能を実行できるようになります。電話、ゲートウェイ、メディア リソースな

どのデバイスが登録やコール発信を実行できるのは、このサービスが使用可能になっているサーバに対してのみです。Cisco Unified CallManager 5.0　では、クラスタ内の　8　つまでのサーバで Cisco CallManager Service を使用可能にできます。

選択した冗長性方式に応じて（P.8-8 の「コール処理の冗長性」を参照）、コール処理サブスクライバは、プライマリ（アクティブ）サブスクライバまたはバックアップ（スタンバイ）サブスクライバのどちらかになります。ロード バランシングを実装する場合は、サブスクライバがプライマリ サブスクライバとバックアップ サブスクライバの両方を兼ねることもあります。クラスタの設計を計画するときは、通常はコール処理サブスクライバにこの機能を割り当てます。大規模なクラスタや高性能クラスタでは、コール処理サービスをパブリッシャおよび TFTP サーバ上で使用可能にしないでください。コール処理サブスクライバは、採用する冗長性方式に応じて、通常は専用ペアまたは共有ペアのどちらかで運用します。1：1 冗長性では、専用ペアを使用します。2：1 冗長性では、各ペアに含まれるサーバ 1 台（バックアップ サーバ）を共有する、2 組のサーバを使用します。

ハードウェア プラットフォームは、サーバの規模、パフォーマンス、冗長性、およびコストに応じて選択します。規模とパフォーマンスについては、P.8-16 の「Cisco Unified CallManager プラットフォームのキャパシティ プランニング」の項で説明しています。冗長性については、P.8-8 の「コール処理の冗長性」の項で説明しています。

コール処理の冗長性

Cisco Unified CallManager 5.0 では、次の冗長性設定の中から選択できます。

- 2:1 冗長性方式：プライマリ サブスクライバ 2 台ごとに、1 つの共用バックアップ サブスクライバを設置します。
- 1:1 冗長性方式：プライマリ サブスクライバごとに、1 つのバックアップ サブスクライバを設置します。

1:1 冗長性方式では、フェールオーバー期間だけがクラスタに影響を与えるアップグレードが可能です。このフェールオーバー メカニズムは、Skinny Client Control Protocol（SCCP）IP Phone のフェールオーバー レート、毎秒約 125 台の登録を実現できるように拡張されました。Session Initiation Protocol（SIP）電話機のフェールオーバー メカニズムでは、毎秒約 40 台の登録です。

Cisco Unified CallManager 5.0 からは、サービスへの影響なしにクラスタをアップグレードできます。Cisco Unified CallManager 5.0 では、2 つのバージョンの Cisco Unified CallManager を同じサーバ上に置いて、一方をアクティブ パーティションに、もう一方を非アクティブ パーティションに入れることができます。すべてのサービスとデバイスで、すべての Cisco Unified CallManager 機能に対して、アクティブ パーティションの Cisco Unified CallManager バージョンが使用されます。アップグレード時に、クラスタ操作はアクティブ パーティションにある現在のリリースの Cisco Unified CallManager を使用して続行されながら、アップグレード バージョンが非アクティブ パーティションにインストールされます。アップグレード プロセスの完了後は、サーバをリブートし非アクティブ パーティションをアクティブ パーティションに切り替えて、新しいバージョンの Cisco Unified CallManager を実行できます。

Cisco Unified CallManager 5.0.*x* から Cisco Unified CallManager 5.0.*x* へのアップグレード

1:1 冗長性方式で、クラスタをアップグレードする手順は、次のとおりです。

ステップ 1　新しいバージョンの Cisco Unified CallManager をパブリッシャにインストールします。リブートはしないでください。

ステップ 2　新しいバージョンの Cisco Unified CallManager をすべてのサブスクライバに同時にインストールします。リブートはしないでください。

ステップ 3　パブリッシャのみをリブートします。新しいバージョンの Cisco Unified CallManager に切り替え、データベースが初期化されるまでしばらく待ちます。

ステップ 4　TFTP サーバを 1 台ずつリブートします。新しいバージョンの Cisco Unified CallManager に切り替え、コンフィギュレーション ファイルが再作成されるまで待ってから、クラスタ内の他のサーバをアップグレードします。

ステップ 5　Music On Hold（MoH）専用サーバを 1 台ずつリブートします。新しいバージョンの Cisco Unified CallManager に切り替えます。

ステップ 6　バックアップ サブスクライバを 1 台ずつリブートします。新しいバージョンの Cisco Unified CallManager に切り替えます。50/50 ロード バランシングが設定されている場合、このステップは一部のユーザに影響を与えることがあります。

ステップ 7　プライマリ サブスクライバからバックアップ サブスクライバに、デバイスをフェールオーバーします。

ステップ 8　プライマリ サブスクライバを 1 台ずつリブートします。新しいバージョンの Cisco Unified CallManager に切り替えます。

このアップグレード方法では、異なるバージョンの Cisco Unified CallManager ソフトウェアを実行しているサブスクライバ サーバにデバイスが登録される期間（フェールオーバー期間を除く）がありません。

（注）　アップグレード プロセスが非アクティブ パーティションで開始された後は、パブリッシャのデータベースがアクティブ パーティションで変更されても、新しいバージョンのデータベースには移行されません。

2:1 冗長性方式では、クラスタ内のサーバ数を減らすことができますが、その結果、アップグレード時に障害が発生する可能性があります。

（注）　10,000 台以上の IP Phone が 2 つのプライマリ サブスクライバに登録される場合は、1:1 冗長性を使用する必要があります。これは、1 つのバックアップ サブスクライバで 10,000 台以上のバックアップ登録はできないからです。

（注）　アップグレードを行う前に、障害回復フレームワークを使用して、Cisco Unified CallManager および Call Detail Record（CDR; コール詳細レコード）データベースを外部ネットワーク ディレクトリにバックアップすることをお勧めします。このようにしておくと、アップグレードが失敗した場合のデータ損失を防止できます。

コール処理サブスクライバの冗長性

次の図では、Cisco Unified CallManager でコール処理の冗長性を実現するための一般的なクラスタ構成を示しています。

図 8-4　基本的な冗長性方式

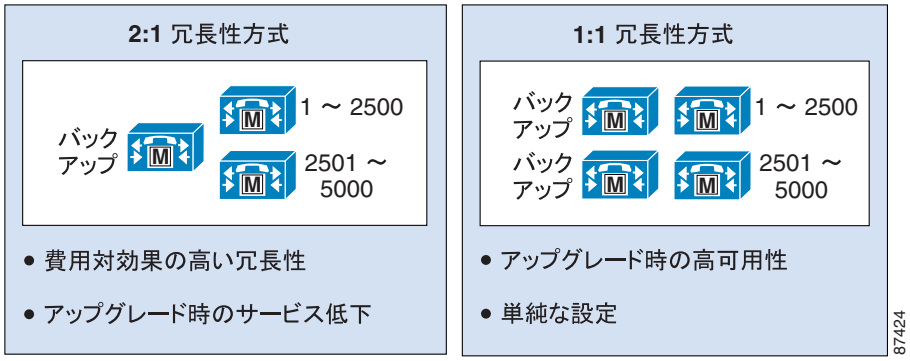


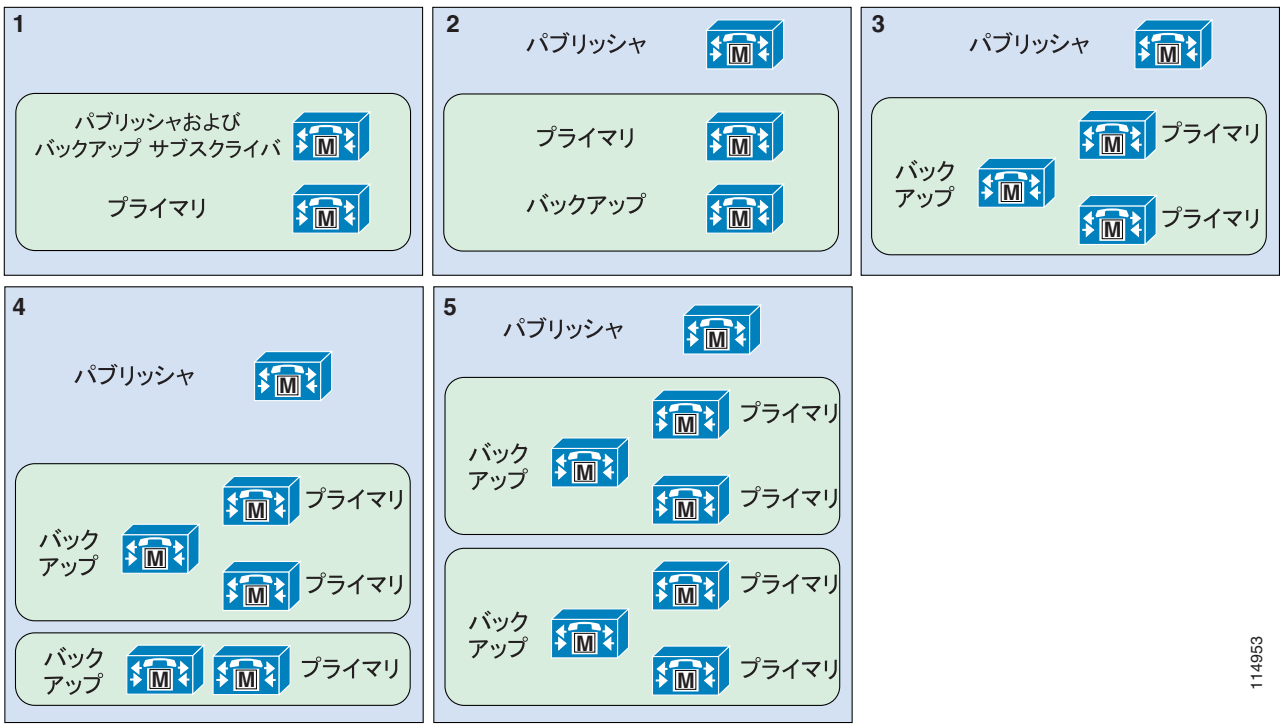
図 8-4 では、利用できる 2 つの基本的な冗長性方式を示しています。どちらの場合でも、バックアップ サーバは、障害の発生するプライマリコール処理サーバ 1 台分以上の処理能力を備えている必要があります。2：1 冗長性方式の場合、バックアップ サーバは、個々の配置の要件に応じて、障害の発生するコール処理サーバ 1 台分、または両方のプライマリ コール処理サーバに相当する処理能力を備えている必要があります。サーバのキャパシティの選定およびハードウェア プラットフォームの選択については、P.8-16 の「Cisco Unified CallManager プラットフォームのキャパシティ プランニング」の項で説明しています。

図 8-5　1：1 冗長構成のオプション

図 8-5 に示した 5 つは、すべて 1：1 冗長性のオプションを示しています。オプション 1 は、1,250 人未満のユーザをサポートするクラスタに使用します。オプション 2 ～ 5 は、クラスタを徐々に拡張した様子を示しています。正確な規模は、選択したハードウェア プラットフォームや必要なハードウェア プラットフォームによって異なります。

この図では、パブリッシャとコール処理サブスクライバのみ示していることに注意してください。

図 8-6　2：1 冗長構成のオプション



ロード バランシング

通常、プライマリが使用可能な場合、バックアップ サーバに登録されたデバイスはありません。このモデルには、次のような特長があります。

- トラブルシューティングが容易：すべてのコール処理がプライマリ サーバで行われるため、トレースおよび警告通知の取得が簡単になります。
- 設定が少ない：すべてのデバイスがプライマリ サーバに登録されるため、追加で Cisco Unified CallManager の冗長性グループまたはデバイス プールを各種のデバイス用に定義する必要性を 50% 減らすことができます。

1:1 冗長性方式を使用すると、プライマリ サーバとバックアップ サーバのペア上でデバイスを分散することができます。ロード バランシングを使用すると、Cisco Unified CallManager の冗長性グループとデバイス プールの設定値を使用して、デバイスにかかる負荷の半分までをプライマリ サブスクライバからセカンダリ サブスクライバに移すことができます。このモデルには、次のような特長があります。

- ロード シェアリング：コール処理の負荷が複数のサーバ上に分散され、応答時間をより速くすることができます。

- フェールオーバーとフェールバックが高速：すべてのデバイス（たとえば、IP Phone、CTI ポート、ゲートウェイ、トランク、ボイスメール ポートなど）がすべてのアクティブ サブスクライバにわたって分散されるため、プライマリ サブスクライバに障害が発生した場合に、セカンダリ サブスクライバにフェールオーバーするデバイスは一部のみです。この方法で、サーバが使用不能になる影響を 50% 減らすことができます。

50/50 ロード バランシングを計画するには、ロード バランシングを使用しない場合のクラスタのキャパシティを計算し、次に、デバイスおよびコールの量に基づいて、負荷をプライマリ サブスクライバとバックアップ サブスクライバに分散します。プライマリ サーバやバックアップ サーバの障害に対処できるようにするには、プライマリとバックアップのサブスクライバの合計負荷が、サブスクライバ サーバ 1 台分の負荷を超えないようにします。

TFTP サーバ

TFTP サーバ プラットフォームには、主に次の 2 つの機能があります。

- MoH　などのサービスのためのファイル、電話やゲートウェイなどのデバイスのコンフィギュレーション ファイル、電話および一部のゲートウェイのアップグレード用バイナリ ファイル、およびさまざまなセキュリティ ファイルの提供。
- コンフィギュレーション ファイルおよびセキュリティ ファイルの生成。シスコの TFTP サービスが生成するファイルのほとんどは、署名済みであり、ダウンロード用として提供する前に暗号化されることもあります。

TFTP サービスは、クラスタ内の任意のサーバで使用可能にすることができます。ただし、何らかの設定を変更すると、TFTP サービスがコンフィギュレーション ファイルを再生成するため、1,250 ユーザを超えるクラスタでは、他のサービスが影響を受ける場合があります。このため、1,250 ユーザを超えるクラスタ、エクステンション モビリティを使用するクラスタ、または設定の変更を伴うその他の機能を備えたクラスタでは、特定のサーバを TFTP サービス専用にすることをお勧めします。

TFTP サーバは、設定情報を取得するために電話および MGCP ゲートウェイが使用します。TFTP サービスを使用可能にできるサーバの数に制限はありませんが、より大規模なクラスタのために TFTP サーバを 2 台配置して、TFTP サービスのための冗長性を確保しておくことをお勧めします。クラスタ内に 3 台以上の TFTP サーバを配置できますが、そのような構成ではすべての TFTP サーバ上ですべての TFTP ファイルを再構築するために時間がかかります。DHCP を使用して TFTP オプションを設定する場合、または静的に TFTP オプションを設定する場合は、TFTP サーバの IP アドレス アレイ（複数の IP アドレス）を定義します。このように定義すると、半数のデバイスでは TFTP サーバ A をプライマリとして使用し、TFTP サーバ B をバックアップとして使用するように割り当てて、他の半数のデバイスでは、TFTP サーバ B をプライマリとして使用し、TFTP サーバ A をバックアップとして使用するように割り当てることができます。TFTP 専用サーバのパフォーマンスを向上させるには、サービス パラメータを設定して、サーバ上で許容する同時 TFTP セッションの数を増やします。

Cisco Unified CallManager クラスタをアップグレードするときは、パブリッシャの後に TFTP サーバをアップグレードし、次にその他のサーバをアップグレードすることを強くお勧めします。また、TFTP サーバをアップグレードした後は、すべてのコンフィギュレーション ファイルが再作成されるように十分な間隔を空けます。一般的な Cisco TFTP の BuildDuration 時間を使用するか、リアルタイム モニタリング ツールを使用して Cisco TFTP の DeviceBuildCount を監視して、これらの増加が止まるまで監視します。このアップグレード順序に従うと、新しいバイナリと設定変更が、クラスタ内の他のサービスをアップグレードする前に有効になります。電話やゲートウェイの個々のバイナリまたはファームウェア ロードを手動で追加する場合は、ファイルを必ずクラスタ内の各 TFTP サーバにコピーしてください。

Cisco Unified CallManager Release 5.0 では、デフォルトでコンフィギュレーション ファイルがメモリにキャッシュされ、TFTP サーバのハード ドライブには保存されません。このデフォルト設定を変更して、コンフィギュレーション ファイルを TFTP サーバのハード ドライブに入れることができますが、これを行うと、TFTP のパフォーマンスに影響があります。したがって、このデフォルト設定を変更しないことをお勧めします。

TFTP サーバのハードウェア プラットフォームには、コール処理サブスクライバと同じものを使用することをお勧めします。

CTI Manager

CTI Manager は、クラスタ内で TAPI または JTAPI コンピュータ / テレフォニー インテグレーション（CTI）を使用するアプリケーションに必要となるものです。CTI Manager は、CTI アプリケーションと Cisco Unified CallManager サービスの仲介者として機能します。アプリケーションの認証機能を提供し、許可済みのデバイスを制御および監視できるようにします。CTI アプリケーションはプライマリ CTI Manager と通信し、障害発生時にはバックアップ CTI Manager に切り替えます。CTI Manager は、コール処理サブスクライバ上でのみ使用可能にする必要があります。したがって、クラスタ内では最大で 8 つの CTI Manager を使用できます。復元性、パフォーマンス、および冗長性を最大限まで高めるには、CTI アプリケーションの負荷をクラスタ内の複数の CTI Manager に分散することをお勧めします。

一般に、アプリケーションによって制御または監視されるデバイスは、CTI Manager に使用するものと同じサーバ ペアに関連付けることをお勧めします。たとえば、IVR（interactive voice response; 音声自動応答装置）アプリケーションでは 4 つの CTI ポートが必要になります。1：1 冗長性と 50/50 ロード バランシングを使用する場合は、これらを次のように設定します。

- 2 つの CTI ポートは、サーバ A をプライマリ、サーバ B をバックアップ（セカンダリ）とする Cisco Unified CallManager 冗長性グループを持つようにします。残りの 2 つの CTI ポートは、サーバ B をプライマリ、サーバ A をバックアップとする Cisco Unified CallManager 冗長性グループを持つようにします。
- IVR アプリケーションは、サーバ A 上の CTI Manager をプライマリ、サーバ B をバックアップとして使用するように設定します。

上の例は、サーバ A 上の CTI Manager で障害が発生した場合の冗長性を備えており、IVR コールの負荷を 2 つのサーバに分散することもできています。この方法では、Cisco Unified CallManager サーバの障害による影響も最小限に抑えることができます。

IP Voice Media Streaming Application

会議や Music On Hold などのメディア リソースは、Cisco Unified CallManager サービスと同じ物理サーバ上で動作している IP Voice Media Streaming Application サービスによって提供されます。

メディア リソースには、次のものがあります。

- Music On Hold（MoH）：保留状態になっているデバイス、会議に転送または追加されるデバイスに対して、マルチキャストまたはユニキャストの保留音を提供できます（P.7-1 の「Music on Hold」を参照）。
- Annunciator サービス：電話番号を間違えていることや、コール ルーティングが使用不可になっていることを伝える場合に、トーンの代わりに音声アナウンスを流します（P.6-20 の「Annunciator」を参照）。
- コンファレンス ブリッジ：Ad Hoc 会議と Meet-Me 会議のための、ソフトウェア ベースの会議を提供します（P.6-8 の「オーディオ会議」を参照）。
- メディア ターミネーション ポイント（MTP）サービス：H.323 クライアント、H.323 トランク、および Session Initiation Protocol（SIP）トランク用の機能を提供します（P.6-14 の「メディア ターミネーション ポイント（MTP）」を参照）。

クラスタ内でメディア リソースを実行する場合は、メディアの処理とネットワークに関する要件が追加される場合に備えて、すべてのガイドラインに準拠することが重要です。一般に、マルチキャスト MoH と Annunciator には専用サーバを使用せず、ソフトウェア ベースの大規模な会議と MTP に専用のメディア リソース サーバを使用することをお勧めします（これらのサービスが、P.6-1 の「メディア リソース」、P.7-1 の「Music on Hold」の章で説明している設計ガイドラインの範囲内にない場合は除きます）。

音声アクティビティ検出

クラスタ内で音声アクティビティ検出（VAD）も使用不可にしておくことをお勧めします。デフォルトでは、Cisco CallManager サービス パラメータで VAD は使用不可になっています。H.323 および SIP ダイヤルピア上で使用不可にするには、**no vad** コマンドを使用してください。

Cisco Unified CallManager のアプリケーション

さまざまなタイプのアプリケーションを Cisco Unified CallManager 上で使用可能にすることができます。ここでは、Cisco Unified CallManager アプリケーションのスケーラビリティの面についてのみ取り上げます。設計ガイドラインの詳細については、P.20-1 の「Cisco Unified CallManager アプリケーション」の章を参照してください。

Cisco Unified CallManager のアプリケーションには次のものがあります。

Cisco Unified CallManager Assistant

Cisco Unified CM Assistant アプリケーションは CTI Manager Service と連携して動作します。クラスタ内で Cisco Unified CM Assistant を使用する場合は、必要となるキャパシティおよびパフォーマンスに応じて、Cisco Unified CallManager と CTI サブスクライバに選択するハードウェア プラットフォームが異なってきます。クラスタ内で他の CTI アプリケーションを使用する場合には、クラスタ内でサポートされる CTI 接続の数によって、Unified CM Assistant の最大設定が制限されることがあります。

Cisco Unified CallManager Release 5.0 での Unified CM Assistant 用に現在サポートされている上限は次のとおりです。

- クラスタ内に最大 2 台の Unified CM Assistant サーバ
- Unified CM Assistant サービス パラメータで最大 4 台の CTI サーバ
- Cisco MCS 7845 サーバでクラスタごとに 1,250 の Assistant と 1,250 の Manager

Unified CM Assistant のキャパシティの詳細については、次の Web サイトにある Cisco Unified CallManager と Unified CM Assistant のデータ シート、マニュアル、およびリリース ノートを参照してください。

http://www.cisco.com

シスコ エクステンション モビリティ

クラスタ内でエクステンション モビリティを使用する場合は、必要となるキャパシティおよびパフォーマンスに応じて、選択するパブリッシャ ハードウェア プラットフォームが異なってきます。ユーザが電話でログインまたはログアウトしたときに、コンフィギュレーション データベースに含まれているコンフィギュレーションをアップデートし、TFTP サービスでコンフィギュレーション ファイルを再生成し、次にデバイスをリセットして、変更内容を有効にする必要があります。これらの処理のほとんどは、パブリッシャ上で発生します。

Cisco Unified CallManager Release 5.0 でのエクステンション モビリティ用に現在サポートされている上限は次のとおりです。

- Cisco MCS-7845 パブリッシャ サーバは、1 分あたり 50 回の順次ログイン、ログアウトをサポートできます。
- Cisco MCS-7835 パブリッシャ サーバは、1 分あたり 30 回の順次ログイン、ログアウトをサポートできます。

EM のキャパシティの詳細については、次の Web サイトにある Cisco Unified CallManager のデータシート、マニュアル、およびリリース ノートを参照してください。

http://www.cisco.com

Cisco Attendant Console（AC）

Cisco AC アプリケーションは、回線監視および電話制御のために CTI Manager Service と対話します。クラスタ内で Cisco AC を使用する場合は、必要となるキャパシティおよびパフォーマンスに応じて、Cisco Unified CallManager と CTI サブスクライバに選択するハードウェア プラットフォームが異なってきます。クラスタ内で他の CTI アプリケーションを使用する場合には、クラスタ内でサポートされる CTI 接続の数によって、AC の最大設定が制限されることがあります。

Cisco Unified CallManager Release 5.0 での AC 用に現在サポートされている上限は次のとおりです。

- MCS 7845 は、最大で 1,250 の AC デバイスをサポートできます。Attendant Console アプリケーションは、最高 1,250 台のアテンダント コンソール デバイスと任意に組み合せて使用することができます。たとえば、125 のハント パイロットを用意して各ハント パイロットに 10 メンバーを含めたり、50 のハント パイロットを用意して各ハント パイロットに 25 メンバーを含めたりするように Cisco Unified CallManager を設定できます。
- MCS 7835 は最大で 1,000 の AC デバイスをサポートし、MCS 7825 は最大で 750 の AC デバイスをサポートします。

Cisco Unified CallManager プラットフォームのキャパシティ プランニング

Cisco Unified CallManager には、タイプの異なるデバイスを登録できます。たとえば、IP Phone、ボイスメール ポート、CTI（TAPI または JTAPI）デバイス、ゲートウェイ、および DSP リソース（トランスコーディングや会議）などです。これらの各デバイスは、登録先となるサーバ プラットフォームのリソースを必要とします。必要なリソースには、メモリ、プロセッサ使用、およびディスク I/O が含まれます。各デバイスは、トランザクション（通常、コールの形式）中に、追加のサーバ リソースを消費します。たとえば、1 時間当たり 6 回のコールだけを行うデバイスが消費するリソースは、1 時間当たり 12 回のコールを行うデバイスより少なくなります。

この項で示す推奨事項は、Cisco Unified CallManager Capacity Calculator を、デフォルトのトレース レベルと CDR を有効にして使用し、その結果として得た計算に基づいています。コール処理に直接関係しない他の機能を使用不可にしたり、縮小したり、再設定したりすると、より高いレベルのパフォーマンスが得られます。こうした機能の一部を増やすと、システムのコール処理機能に影響を与える可能性があります。これらの機能には、トレース、コール詳細レコード、複雑なダイヤル プラン、およびサーバ上に共存するその他のサービスが含まれます。複雑なダイヤル プランには、複数のライン アピアランス、多くのパーティション、コーリング サーチ スペース、ルート パターン、変換、ルート グループ、ハント グループ、ピックアップ グループ、ルート リスト、自動転送の拡張使用、共存サービス、およびその他の共存アプリケーションが含まれています。こうした機能はすべて、Cisco Unified CallManager サーバ内の追加リソースを消費します。

システム パフォーマンスを向上させるために、次のテクニックを活用すると便利なオプションが提供されます。

- 特定プラットフォーム用にサポートされている最大量まで、サーバに追加の保証メモリを取り付ける。MCS 7825 および MCS 7835、または同等のサーバ クラスの大規模構成では、これらのサーバの RAM を倍に増やすことをお勧めします。このメモリ アップグレードが必要かどうかは、パフォーマンス モニタを使用して検証することでわかります。サーバが物理メモリを最大量近くまで使用すると、オペレーティング システムは、ディスクへのスワップを開始します。このスワッピングが発生した場合は、追加の物理メモリを取り付ける必要があることを示しています。
- 多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランをもつ Cisco Unified CallManager クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Cisco Unified CallManager Administration オンライン ヘルプの「Service Parameters」を参照してください。

Cisco Unified CallManager Release 5.0 には、次のガイドラインが適用されます。

- クラスタ内では、Cisco Unified CallManager Service を使用して最大 8 台のサーバを使用可能にすることができます。それ以外のサーバは、TFTP、パブリッシャ、Music on Hold などの専用機能に使用できます。
- 標準サーバごとに CTI 接続またはアソシエーションを最大 800 設定できます。サーバ間で均等にバランスが取られる場合は、クラスタごとに最大 3200 設定できます。
- 高性能サーバごとに CTI 接続またはアソシエーションを最大 2,500 設定できます。サーバ間で均等にバランスが取られる場合は、クラスタごとに最大 10,000 設定できます。
- 各クラスタは、最大 30,000 台の SCCP または SIP 電話機をサポートできます。
- 各クラスタは、最大 600 台の H.323 デバイス（ゲートウェイ、トランク、クライアント）、デジタル MGCP デバイス、および SIP トランクをサポートできます。

キャパシティの計算

Cisco Unified CallManager Release 5.0 の Cisco CallManager キャパシティ ツールを使用すると、システムのキャパシティを各種の設定について計算することができます。キャパシティ プランニング ツールを使用できるのは、現時点ではログイン アカウントを持つすべての www.cisco.com ユーザです。システムが次のガイドラインを満たしていない場合や、システムをさらに複雑にするためにキャパシティを確認する必要があるのに Cisco CallManager キャパシティ ツールにアクセスできない場合は、シスコのシステム エンジニア（SE）または Cisco Technical Assistance Center（TAC）にお問い合せください。

Cisco CallManager キャパシティ ツールは次の Web サイトで入手可能です。

http://www.cisco.com/partner/WWChannels/technologies/resources/CallManager/

システムが次の要件を満たしている場合は、コンフィギュレーションを Cisco CallManager キャパシティ ツールで確認する必要はありません。

- システムに含まれているユーザ数が、サーバ プラットフォームの最大ユーザ数の 25% 未満である。
- 電話機ごとの平均の回線数が、1.1 を超えていない。
- ユーザごとの平均の Busy Hour Call Attempt（BHCA）が、1 時間あたり 4 コール未満である。
- クラスタ セキュリティが有効になっていない。
- ゲートウェイまたはトランクのどちらかを経由するトランキングが、20%（1 トランクあたり 5 ユーザ）以下である。
- ボイスメール ポートが 5%（1 ボイスメール ポートあたり 20 ユーザ）以下である。
- サーバ 1 台あたりの MoH ストリームが 20 以下である。
- CTI、JTAPI、および TAPI のデバイスがない。
- コンファレンス ブリッジが 5%（ブリッジ上の 1 ポートあたり 20 ユーザ）以下である。
- トランスコーダがない。
- トランキングに必要な最大コールをサポートする目的では、MTP のみ使用する。
- ロケーションが 20 未満である。
- システムには、上に定義されていないもの以外は、IP Phone、IP Communicator、ゲートウェイ、メディア リソース、ボイスメール ポート、トランクしか含まれていない。

Cisco Unified CallManager がサポートできるユーザの最大数は、サーバ プラットフォームによって異なります（表 8-2 を参照）。

表 8-2　サーバ プラットフォームごとの最大デバイス数

サーバ プラットフォームの特性	サーバ 1 台あたりの最大ユーザ数[1]	高可用性サーバ[2]	高性能サーバ
Cisco MCS-7845（すべてのサポート モデル）	7500	あり	あり
Cisco MCS-7835（すべてのサポート モデル）	2500	あり	なし
Cisco MCS-7825（すべてのサポート モデル）	1000	なし	なし
Cisco MCS-7815（すべてのサポート モデル）[3]	300	なし	なし

1. 高可用性サーバでないプラットフォームは、非冗長インストレーションで最大 500 の IP Phone をサポートできます。
2. 高可用性サーバは、電源装置とハードディスクの両方の冗長性をサポートします。
3. MCS-7815 サーバは N+1 冗長性のみサポートし、クラスタのメンバーになることはできません。

サポートされるプラットフォーム、サードパーティ プラットフォーム、個々のハードウェア設定の最新情報については、次の Web サイトにあるオンライン資料を参照してください。

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

(注)　高可用性に対応していないプラットフォームの場合は、非冗長インストレーションとして、サポートされる IP Phone の最大数は、500 台になります。

Cisco CallManager キャパシティ ツール

Cisco CallManager キャパシティ ツールは、さまざまな情報を要求して、システムに必要となるサーバの最小限のサイズとタイプについて、見積もりを提示します。要求される情報には、IP Phone、ゲートウェイ、メディア リソースなどのデバイスの、タイプと数が含まれています。キャパシティ ツールは、デバイス タイプごとに平均 BHCA と平均利用時間も要求します。たとえば、IP Phone で 1 時間あたり平均 5 件のコールが発生し、コールの平均持続時間が 3 分である場合、BHCA は 5 で、利用時間は 0.25 です（電話機上で 3 分間のコールが 5 件発生しているため、1 時間あたり 15 分、つまり 0.25 時間に相当します）。

デバイス情報に加えて、ルート パターンやトランスレーション パターンなどの、ダイヤル プランに関する情報も要求します。詳細をすべて入力すると、目的のサーバ タイプのプライマリ サーバがいくつ必要になるかについて、キャパシティ ツールが計算します。必要なキャパシティがクラスタ 1 つ分のキャパシティを超える場合は、クラスタの数も計算します。

キャパシティ ツールは、以前にデバイスの重み、BHCA 係数、コール タイプ係数、ダイヤル プランの重みと呼ばれていたメカニズムを置き換えるものです。

Cisco CallManager キャパシティ ツールを使用した場合の結果は、設定について計算された各種リソースの最高キャパシティを示します。リソースには絶対的な上限、メモリ、プロセッサの使用率、およびディスク I/O アクティビティが含まれます。さらにデバイスを追加したとき、追加の設定では、示されている現在の最高キャパシティを下回るリソースを使用しているため、見た目ではそれ以上のキャパシティが使用されていないことになります。

たとえば、サードパーティ制御の 2,500 台の SCCP IP Phone を Cisco CallManager キャパシティ ツールに追加した場合、必要な MCS 7845 サブスクライバは 1 つであり、そのキャパシティ使用率は 100% であることが示されます。さらに 1,000 台の電話機を追加した場合でも、必要な MCS 7845 サブスクライバは 1 つであり、そのキャパシティ使用率は 100% であるという結果が示されます。このような結果になる理由は、このサーバの CTI キャパシティが 100% 状態にあるためで、IP Phone を追加しても CTI 要件が追加されることはありません。他のデバイスの数が残りのいずれか 1 つの上限を超えるまで、追加のキャパシティは使用されていないように見えます。これは通常の状態であり、Cisco CallManager キャパシティ ツールに予想される動作です。

情報をキャパシティ カルキュレータに入力する場合は、次の項のガイドラインを使用してください。

電話機に関する計算

キャパシティ ツールのメインの Telephony セクションに（Contact Center セクションではなく）、次の電話機タイプがリストされます。

- SCCP 電話機（非セキュア）
- セキュア SCCP 電話機
- SIP 電話機（非セキュア）
- セキュア SIP 電話機

電話機タイプごとに、数、BHCA、使用率、ライン アピアランスの値を入力することができます。これらについては、続く各項で詳しく説明します。

数

この値は、クラスタ内に設定するタイプごとの IP Phone の合計数です。この数には、Cisco7900 シリーズのすべての IP Phone、VG248 ポート、VG224、IP Communicator、およびその他のサードパーティ SCCP エンドポイント デバイスを含めます。この数には、アクティブになっていないものも含めて、設定済みのすべての電話を含める必要があります。

BHCA

この値は、タイプごとのすべての電話の平均 BHCA です。複数の電話で共用している回線がある場合、BHCA には、回線を共用しているそれぞれの電話のコールを 1 つとして含める必要があります。複数の電話機タイプにわたるシェアドラインは、タイプごとの BHCA に影響します。つまり、シェアドラインへの 1 つのコールは、複数のコール（呼び出される電話機に 1 つずつ）として計算します。それぞれ別の BHCA を生成する複数の電話グループがある場合、Cisco CallManager キャパシティ ツールで使用する BHCA 値は、次の方法で指定します。

たとえば、次の特性を持つ 2 クラスのユーザがいるとします。

- 20 BHCA の電話 100 台 = 合計 2,000 BHCA
- 4 BHCA の電話 5,000 台 = 合計 20,000 BHCA

すべての電話デバイスの合計 BHCA は、この場合 22,000 です。

この合計 BHCA を電話デバイスの合計数で除算して、次の値を算出します。

電話デバイス 1 台あたりの平均 BHCA = 22,000/5,100 = 4.31 BHCA

使用率

この値は、電話ごとの平均コール使用率です。コールが電話上に存在した、すべての時間を含めます。電話の実際の使用率は、100% を超えることがあります。これは、電話が 1 回線あたり複数のコールを許可しているか、頻繁に使用される複数のライン アピアランスを備えている場合です。使用率は、1 時間における百分率で測定します。たとえば、最も混雑している時間に 3 分間のコールが発生した電話は、5% 使用されたものと見なします。BHCA の計算と同じ方法を、複数の電話グループがある場合の平均使用率の計算にも使用することができます。電話にシェアドラインがある場合は、その電話の予想使用率のみ計算し、共用されている回線の実際の使用率は計算しません。Cisco CallManager キャパシティ ツールで使用できるのは、現時点では、すべての電話の平均使用率です。

ライン アピアランス

この値は、すべての電話の平均回線数です。同じ DN を持つ電話が複数のパーティション内に出現している場合は、複数のライン アピアランスと見なします。シェアドラインは 1 つの回線としてカウントしますが、BHCA と使用率が正しく計算されていることを確認してください。回線ごとに複数のコールが発生した場合、ライン アピアランスの数は増加しませんが、BHCA と使用率の計算には影響します。たとえば、通常の状態として電話機に 2 コールあり、一方がアクティブでもう一方がさまざまな時間で保留になる場合、2 コールが実際に接続しているため、そのデバイスについての使用率は、より高くなります。

ゲートウェイ

ゲートウェイの数

ゲートウェイの数は、ゲートウェイのタイプに応じて異なるため、次のいくつかのエントリに分けられています。

- MGCP T1/E1 ゲートウェイ

  この値は、Cisco Unified CallManager データベース内に設定する必要のあるゲートウェイの合計数です。たとえば、Cisco IOS MGCP ゲートウェイは複数の T1 または E1 を保持できますが、単一のゲートウェイとして追加します。Cisco WS-6608 モジュールは、T1 または E1 ゲートウェイとして設定されているポートごとに、1 モジュールあたり最大で 8 つまで、ゲートウェイとして追加します。
- MGCP アナログ ゲートウェイ

  この値は、Cisco Unified CallManager データベースに追加するアナログ ゲートウェイの合計数です。通常は、モジュール全体（WS-6624 または Cisco Unified CallManager）またはハードウェア プラットフォーム（Cisco IOS ルータ プラットフォーム）を 1 つのゲートウェイとして追加します。
- H.323 ゲートウェイ

  モジュール全体またはハードウェア プラットフォームを、1 つのゲートウェイとして追加します。この数には、Cisco Unified CallManager に定義されていないものの、H.323 トランク経由で使用される H.323 ゲートウェイは含みません。

（注） SIP ゲートウェイはトランクとして追加されます。

DS0 の数

この値は、各タイプのゲートウェイがサポートする DS0 またはアナログ ポートの合計数です。DS0 の数は、次のように、ゲートウェイのタイプによって分かれています。

- T1 CAS：

  24 *（T1 CAS スパンの数）
- T1（E1）PRI：

  （23 または 30）*（PRI の合計数）
- H.323 ゲートウェイ

  （DS0 の合計数）/（すべてのデジタル、アナログ、IP インターフェイス上でサポートされるコールの数）

BHCA

この BHCA は、最も混雑している時間における、ゲートウェイ上のすべての DS0 またはアナログ ポートの平均値です。この平均値を計算する方法は、電話の BHCA に使用する方法と同じです。

使用率

この値は、最も混雑している時間における、すべての DS0 またはアナログ ポートの平均使用率です。

EM プロファイル

エクステンション モビリティ（EM）プロファイルには、電話の計算でも含めている、ライン アピアランスを含めます。エクステンション モビリティは、デバイスの数には影響しませんが、電話ごとのライン アピアランスの平均数が増加します。EM ユーザの BHCA および使用率は、ユーザのログイン先となる電話について、すでに計算したものです。

H.323 と SIP のトランク

トランクの数

この値は、Cisco Unified CallManager データベース内に設定されるトランクの合計数です。ゲートキーパーが制御するトランクは、宛先の数の影響を受けません。このため、設定済みのゲートキーパー制御トランクごとに 1 つとしてカウントします。これは、Session Initiation Protocol（SIP）プロキシを使用する SIP トランクにも当てはまります。SIP プロキシ経由で接続されない SIP ゲートウェイごとに、SIP トランクを Cisco Unified CallManager で定義する必要があります。

コールの数

この値は、すべてのトランク上で許容できる同時発生コールの合計数です。許容されるコールの数は、通常はロケーションまたはゲートキーパーのコール アドミッション制御によって制御されます。許容されるコールの数には、リージョンとコーデックも影響することに注意してください。

使用率

この値は、すべてのトランクにわたる、すべてのコールの平均使用率です。これは、最も混雑している時間における百分率（%）です。使用率が 75% の場合は、コールが 1 時間あたり 45 分アクティブであることを意味します。

MTP の要件

MTP の要件についても、カルキュレータで別個に検討する必要があります。H.323 または SIP トランク上で MTP が必要となる場合、そのトランク上でのすべての同時発生コールで MTP リソースが必要になります。RSVP エージェントは数に含める必要があり、また、サポートされる最大セッション数に基づいています。

CTI ルート ポイント、ポート、およびサードパーティ制御の回線

CTI ルート ポイントの計算には、合計数、平均 BHCA、および使用率の値が含まれます。割り当て済みのディレクトリ番号は、いずれもツールの Dial Plan セクションに追加する必要があります。

CTI ポートは、制御元のアプリケーションがさまざまな方法で使用することができます。説明を単純にするため、次の 2 つのグループに分けて考えます。

- 単純コールまたはリダイレクト コール

  単純コールとは、補足サービスの呼び出しが伴わない、ポートへのコールあるいはポートから別のデバイスへのコールのことです。一般的なコール シナリオとなり、発信者からコールがあって着信側が応答し、コールが進行して両者が電話を切る場合です。

  リダイレクト コールとは、実際には応答されない CTI ポートへのコールのことです。代わりに、別の宛先に転送されるか、リダイレクトされます。コールの接続がなく、そのためメディアが CTI ポートに接続されないため、このコールは単純コールよりもさらに単純です。

- 転送または会議

  これらのコール タイプは、IVR アプリケーションまたは自動応答アプリケーションに一般的です。

  転送タイプのコールは、CTI ポートに接続されるコールとしての特徴を備え、ある時点で、CTI ポートは、発信者を別の宛先に打診なしで転送（ブラインド転送）します。

  会議は転送のバリエーションの 1 つで、CTI ポートに接続したコールは、打診転送されるか（三者コール）、あるいはコール期間中に別の相手と会議を行います。

サードパーティ制御の回線

デバイスまたは回線に対するサードパーティ制御または監視が要求されるアプリケーションごとに、カルキュレータのこのフィールドでのカウントおよび入力が必要になります。複数のアプリケーションが同じデバイスを監視または制御している場合には、それを複数回としてカウントする必要があります。

ゲートキーパーの設計上の考慮事項

1 台の Cisco IOS ゲートキーパーで、分散型コール処理環境で最大 100 の Cisco Unified CallManager クラスタに対してコール ルーティングとコール アドミッション制御をサポートできます。複数のゲートキーパーを設定すると、数千の Cisco Unified CallManager クラスタをサポートできます。Cisco IOS ゲートキーパーを使用して、H.323 ゲートウェイと Cisco Unified CallManager 間の通信とコール アドミッション制御をサポートすることによって、ハイブリッド Cisco Unified CallManager とトール バイパス ネットワークを実装することもできます。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、ハブアンドスポーク トポロジに制限されます。

Cisco 2600、2800、3600、3700、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。この項では、ゲートキーパー ネットワークを構築するための設計要件について検討します。ただし、コール アドミッション制御やダイヤル プラン解決については扱いません。これらについては、P.9-1 の「コール アドミッション制御」と P.10-1 の「ダイヤル プラン」の章でそれぞれ説明しています。

ゲートキーパーの詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_configuration_guide_book09186a00801fcee1.html

ハードウェア プラットフォームの選択

ゲートキーパーのプラットフォームは、1 秒間あたりのコール数、および同時発生コール数に基づいて選択します。1 秒間あたりのコール数が多いほど、Cisco 3700、3800、7200 シリーズ ルータなどの高性能な CPU が必要になります。同時発生コールの数が大きいほど、より多くのメモリが必要になります。プラットフォームの選択に関する最新情報については、シスコ代理店またはシスコのシステム エンジニア（SE）にお問い合せください。

ゲートキーパーの冗長性

ゲートキーパーが、クラスタ間通信にすべてのコール ルーティングとアドミッション制御機能をサポートする場合は、冗長性が必要です。Cisco Unified CallManager Release 3.3 より前では、ゲートキーパーの冗長性をサポートする方法は、ホットスタンバイ ルータ プロトコル（HSRP）だけでした。Cisco Unified CallManager Release 3.3 以降は、ゲートキーパーの冗長性をサポートする方法として、ゲートキーパー クラスタリングと冗長ゲートキーパー トランクも使用できるようになりました。次の項では、これらの方法について説明します。

（注） 可能な場合、ゲートキーパーの冗長性をサポートするには、ゲートキーパー　クラスタリングを使用することをお勧めします。冗長性に HSRP を使用するのは、ソフトウェア機能セットでゲートキーパー クラスタリングが利用できない場合だけにしてください

ホットスタンバイ ルータ プロトコル（HSRP）

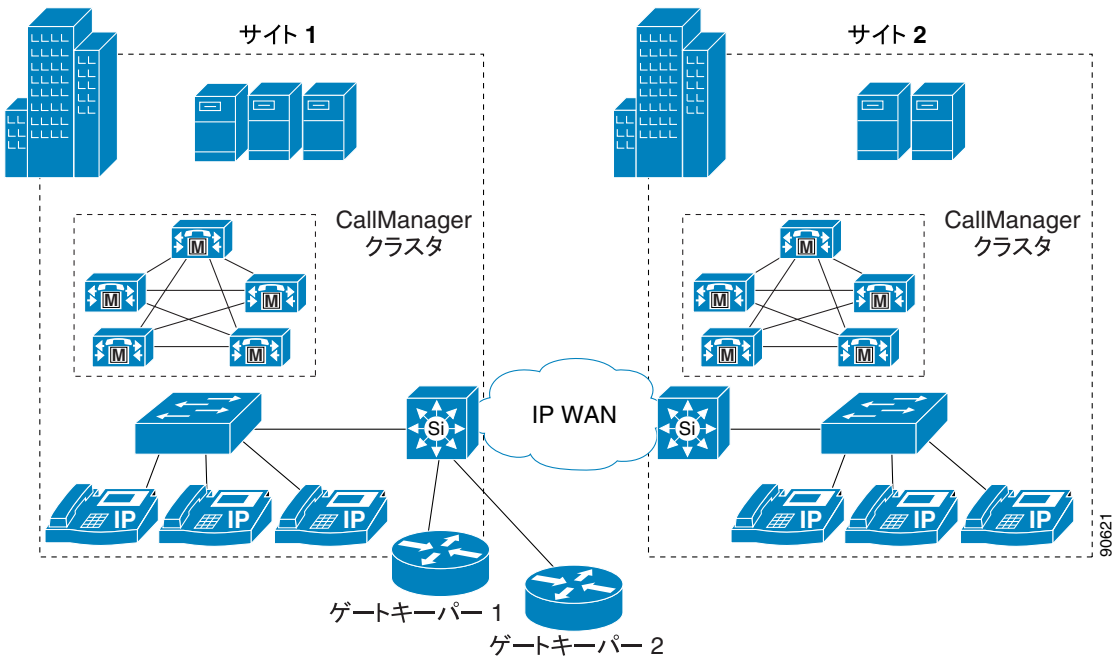
Release 3.3 より前の Cisco Unified CallManager では、ゲートキーパーの冗長性には、ホットスタンバイ ルータ プロトコル（HSRP）しか選択できませんでした。HSRP は、冗長かつスケーラブルなゲートキーパー ネットワークの構築に必要な機能をサポートしないので、Release 3.3 より前の Cisco Unified CallManager 環境でのみ使用してください。

HSRP には、次のガイドラインが適用されます。

- 一度に 1 つのゲートキーパーしかアクティブになりません。
  - スタンバイ ゲートキーパーは、プライマリに障害が発生した場合でなければ、コールを処理しません。
  - ロード バランシング機能は使用できません。
- すべてのゲートキーパーが同じサブネットまたはロケーションに存在しなければなりません。
- フェールオーバー後に以前の状態情報が使用できません。
- フェールオーバー後、スタンバイ ゲートキーパーは、すでにアクティブになっているコールを認識しないので、帯域幅のオーバーサブスクリプションが発生する可能性があります。
- コールの発信前に、HSRP スタンバイ ゲートキーパーにエンドポイントを再登録する必要があるので、フェールオーバーには相応の時間がかかることがあります。フェールオーバー時間は、登録タイマーの設定に依存します。

図 8-7 では、ゲートキーパーの冗長性に HSRP を使用するネットワーク設定を示しています。

図 8-7　HSRP を使用するゲートキーパー冗長性



例 8-1 では、図 8-7 のゲートキーパー 1 の設定を示しています。例 8-2 では、ゲートキーパー 2 の設定を示しています。イーサネット インターフェイス上の HSRP 設定を除いて、両方の設定は同一です。

例 8-1　ゲートキーパー 1 の設定

```
interface Ethernet0/0
 ip address 10.1.10.2 255.255.255.0
  standby ip 10.1.10.1
  standby priority 110

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-2　ゲートキーパー 2 の設定

```
interface Ethernet0/0
 ip address 10.1.10.3 255.255.255.0
 standby ip 10.1.10.1

gatekeeper
 zone local GK-Site1 customer.com 10.1.10.1
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone default 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-1 と例 8-2 について説明します。

- 各ルータには、それぞれが共有する仮想 IP アドレスを識別するために、HSRP 用に **standby** コマンドが設定されます。ゲートキーパー 1 は、コマンド **standby priority 110** を使用して、プライマリとして設定されています。
- Cisco Unified CallManager トランク登録をサポートするために、各 Cisco Unified CallManager クラスタには、各ルータ上でローカル ゾーンが設定されます。最初のゾーンに定義されている IP アドレスは、HSRP の使用する仮想 IP アドレスと一致する必要があることに注意してください。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、両方のルータでゾーンごとにゾーン プレフィックスが設定されます。
- 各ルータで、両方のサイトの帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- ローカルで解決されないすべてのコールを、ローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できるように、**gw-type-prefix 1# default-technology** コマンドが両方のルータで設定されます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- 冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避するために、**arq reject-unknown-prefix** コマンドが両方のルータで設定されます。

HSRP に関するこの他の高度な情報については、次の Web サイトにあるオンライン ドキュメントを参照してください。

- http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm
- http://www.cisco.com/warp/public/619/3.html
- http://www.cisco.com/warp/public/473/62.shtml

ゲートキーパー クラスタリング（代替ゲートキーパー）

ゲートキーパー クラスタリング（代替ゲートキーパー）により、「ローカル」ゲートキーパー クラスタの設定が可能になります。各ゲートキーパーは、一部の Cisco Unified CallManager トランクのプライマリ、およびその他のトランクの代替として機能します。GUP（Gatekeeper Update Protocol）は、ローカル クラスタ内のゲートキーパー間で状態情報を交換するために使用されます。GUP は、クラスタ内のゲートキーパーごとに CPU 使用率、メモリ使用率、アクティブ コール数、および登録されたエンドポイント数をトラッキングし、報告します。GUP メッセージングで次のパラメータにしきい値を設定すると、ロード バランシングがサポートされます。

- CPU 使用率
- メモリ使用率
- アクティブ コール数
- 登録されたエンドポイント数

ゲートキーパー クラスタリング（代替ゲートキーパー）と Cisco Unified CallManager Release 3.3 以降のサポートにより、ステートフル冗長性とロード バランシングが使用可能になります。ゲートキーパー クラスタリングは、次の機能を提供します。

- ローカルとリモートのクラスタ
- ローカル クラスタ内の最大 5 つのゲートキーパー
- ローカル クラスタ内のゲートキーパーを、別々のサブネットまたはロケーションに配置可能
- フェールオーバーの遅延なし（代替ゲートキーパーはすでにエンドポイントを認識しているので、完全な登録プロセスを実行する必要はありません）
- クラスタ内のゲートキーパーは、状態情報を渡し、ロード バランシングを行う

図 8-8 では、Cisco Unified CallManager 分散型コール処理を行う 3 つのサイト、およびローカル クラスタで設定された 3 つの分散型ゲートキーパーを示しています。

図 8-8　ゲートキーパー クラスタリング

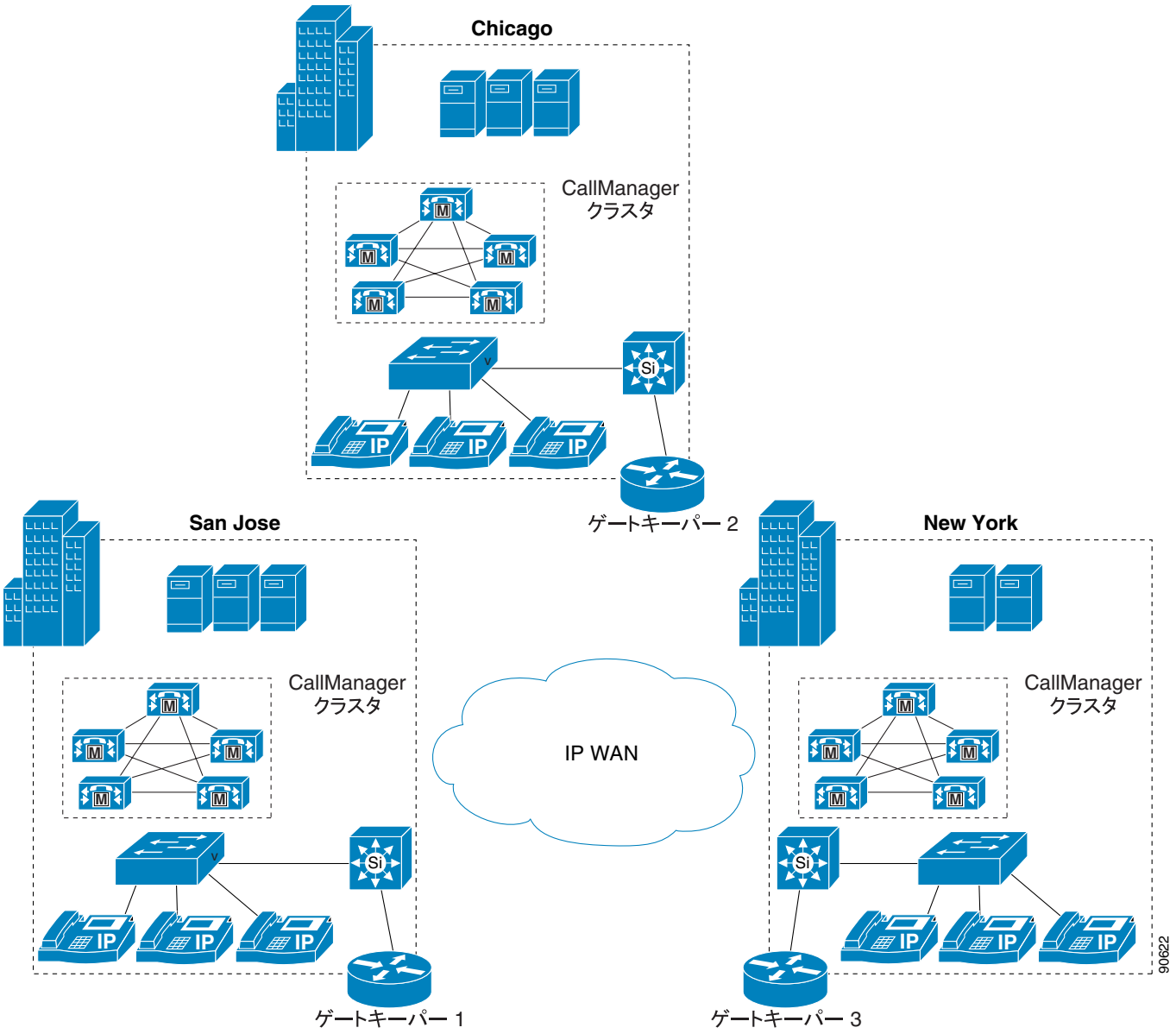


図 8-8 では、ゲートキーパー 2 はゲートキーパー 1 のバックアップ、ゲートキーパー 3 はゲートキーパー 2 のバックアップ、ゲートキーパー 1 はゲートキーパー 3 のバックアップです。

例 8-3 では、ゲートキーパー 1（SJC）の設定を示し、例 8-4 は、ゲートキーパー 2（CHC）の設定を示しています。ゲートキーパー 3（NYC）の設定は、他の 2 つの例を参照してください。

例 8-3　ゲートキーパー 1 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local SJC cisco.com 10.1.1.1
 zone local CHC_GK1 cisco.com
 zone local NYC_GK1 cisco.com
!
 zone cluster local SJC_Cluster SJC
  element SJC_GK2 10.1.2.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
 zone cluster local CHC_Cluster CHC_GK1
  element CHC 10.1.2.1 1719
  element CHC_GK3 10.1.3.1 1719
 !
 zone cluster local NYC_Cluster NYC_GK1
  element NYC 10.1.3.1 1719
  element NYC_GK2 10.1.2.1 1719
 !
 zone prefix SJC 40852.....
 zone prefix NYC_GK1 21251.....
 zone prefix CHC_GK1 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone SJC 192
 bandwidth interzone NYC_GK1 160
 bandwidth interzone CHC_GK1 160
 arq reject-unknown-prefix
 no shutdown
```

例 8-4　ゲートキーパー 2 のゲートキーパー クラスタリング設定

```
gatekeeper
 zone local CHC cisco.com 10.1.2.1
 zone local SJC_GK2 cisco.com
 zone local NYC_GK2 cisco.com
!
 zone cluster local CHC_Cluster CHC
  element CHC_GK3 10.1.3.1 1719
  element CHC_GK1 10.1.1.1 1719
!
 zone cluster local SJC_Cluster SJC_GK2
  element SJC  10.1.1.1 1719
  element SJC_GK3 10.1.3.1 1719
 !
  zone cluster local NYC_Cluster NYC_GK2
  element NYC_GK1 10.1.1.1 1719
  element NYC 10.1.3.1 1719
 !
 zone prefix SJC_GK2 40852.....
 zone prefix NYC_GK2 21251.....
 zone prefix CHC 72067.....
 gw-type-prefix 1#* default-technology
 load-balance cpu 80 memory 80
 bandwidth interzone CHC_Voice 160
 bandwidth interzone SJC_Voice2 192
 bandwidth interzone NYC_Voice3 160
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-3 と例 8-4 について説明します。

- Cisco Unified CallManager トランク登録をサポートするために、各 Cisco Unified CallManager クラスタにはローカル ゾーンが設定されます。
- ローカル ゾーンごとにクラスタが定義され、他のゲートキーパー上のバックアップ ゾーンはエレメントとしてリストされます。エレメントは、バックアップが使用される順にリストされます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **load-balance cpu 80 memory 80** コマンドは、CPU とメモリの使用率を制限します。ルータがどちらかの制限に達すると、新しい要求はすべて拒否され、使用率がしきい値以下に下がるまで、リスト内の最初のバックアップが使用されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドは、設定内容によっては機能しないことがあるためです。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

クラスタ内のすべてのゲートキーパーは、すべての Cisco Unified CallManager トランク登録を表示しています。ゲートキーパーをプライマリ リソースとして使用するトランクの場合、フラグ フィールドはブランクです。クラスタ内の別のゲートキーパーをプライマリ ゲートキーパーとして使用するトランクの場合、フラグ フィールドは A（代替）に設定されます。すべてのエンドポイントをプライマリまたは代替として登録すると、すべてのコールをローカル側で解決できるようになり、別のゲートキーパーにロケーション要求（LRQ）を送信する必要はありません。

例 8-5 では、ゲートキーパー 1（SJC）での **show gatekeeper endpoints** コマンドからの出力を示します。

例 8-5　ゲートキーパー エンドポイントの出力

```
                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name         Type        Flags
--------------- ----- --------------- ----- ---------         ----        -----
10.1.1.12       1307  10.1.1.12       1254  SJC               VOIP-GW
    H323-ID: SJC-to-GK-trunk_1
10.1.1.12       4422  10.1.1.12       4330  SJC               VOIP-GW
    H323-ID: SJC-to-GK-trunk_2
10.1.2.12       4587  10.1.2.12       4330  CHC_GK1           VOIP-GW     A
    H323-ID: CHC-to-GK-trunk_1
10.1.3.21       2249  10.1.3.21       1245  NYC_GK1           VOIP-GW     A
    H323-ID:  NYC-to-GK-trunk_1
Total number of active registrations = 4
```

ディレクトリ ゲートキーパーの冗長性

HSRP を使用するか、複数の同じディレクトリ ゲートキーパーを設定すると、ディレクトリ ゲートキーパーの冗長性を実装できます。同じゾーン プレフィックスを使用して、複数のリモート ゾーンをもつゲートキーパーを設定するとき、このゲートキーパーには、次のいずれかの方法が使用できます。

- 順次 LRQ（デフォルト）

  冗長リモート ゾーン（ゾーン プレフィックスが一致）にコストが割り当てられ、LRQ は、コスト値に基づいた順序で、一致するゾーンに送信されます。順次 LRQ を使用すると、一致するすべてのゲートキーパーに LRQ を送信しないので、WAN 帯域幅の節約になります。

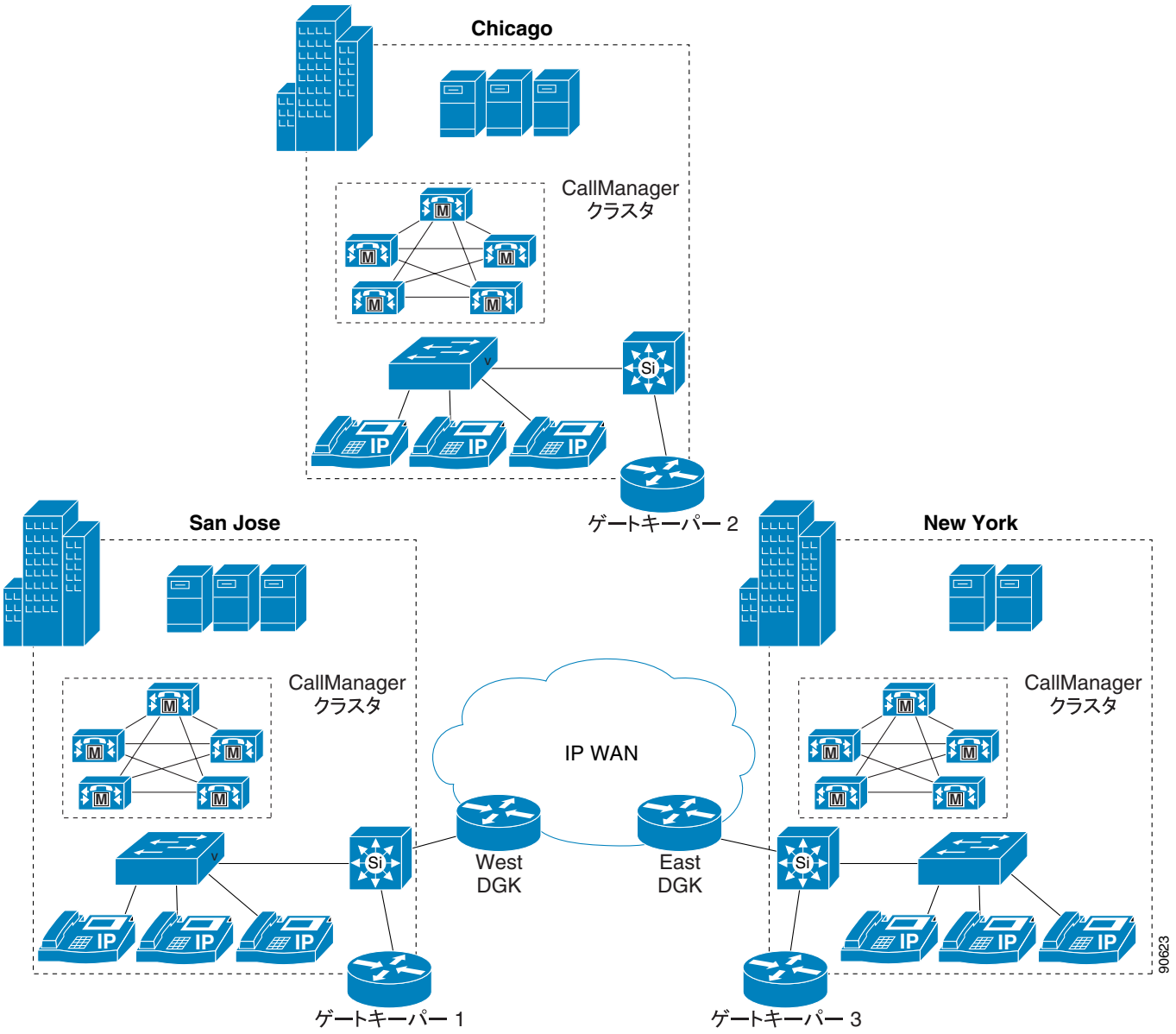
- LRQ ブラスト

  LRQ は、冗長ゾーン（ゾーン プレフィックスが一致）に同時に送信されます。ロケーション確認（LCF）で応答する最初のゲートキーパーが、使用されます。

順次 LRQ を使用して複数のアクティブ ディレクトリ ゲートキーパーを使用することをお勧めします。これによって、ディレクトリ ゲートキーパーを別々のロケーションに配置することができます。HSRP を使用するには、両方のディレクトリ ゲートキーパーを同じサブネットに置く必要があります。この場合常に 1 つのゲートキーパーしかアクティブにすることができません。

図 8-9 では、2 つのアクティブ ディレクトリ ゲートキーパーを備えた Cisco Unified CallManager 分散型コール処理環境を示しています。

図 8-9　冗長ディレクトリ ゲートキーパー



例 8-6 および例 8-7 では、図 8-9 の 2 つのディレクトリ ゲートキーパーの設定を示しています。

例 8-6　West ディレクトリ ゲートキーパーの設定

```
gatekeeper
 zone local DGKW customer.com 10.1.10.1
 zone remote SJC customer.com 10.1.1.1
 zone remote CHC customer.com 10.1.2.1
 zone remote NYC customer.com 10.1.3.1
 zone prefix SJC 408.......
 zone prefix CHC 720.......
 zone prefix NYC 212.......
 lrq forward-queries
 no shutdown
```

例 8-7　East ディレクトリ ゲートキーパーの設定

```
gatekeeper
 zone local DGKE customer.com 10.1.12.1
 zone remote SJC customer.com 10.1.1.1
 zone remote CHC customer.com 10.1.2.1
 zone remote NYC customer.com 10.1.3.1
 zone prefix SJC 408.......
 zone prefix CHC 720.......
 zone prefix NYC 212.......
 lrq forward-queries
 no shutdown
```

ここでは、例 8-6 と例 8-7 について説明します。

- 両方のディレクトリ ゲートキーパーはまったく同じように設定されます。
- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。ワイルドカード（*）をゾーン プレフィックスに使用すると設定を簡潔化できますが、ドット（.）を使用する方がきめ細かく設定できます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスは必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

（注） ディレクトリ ゲートキーパーは、アクティブ エンドポイント登録を含まず、いかなる帯域幅管理も行いません。

例 8-8、例 8-9、および例 8-10 では、図 8-9 のゲートキーパー 1 ～ 3 の設定を示しています。

例 8-8　ゲートキーパー 1（SJC）の設定

```
zone local SJC customer.com 10.1.1.1
 zone remote DGKW customer.com 10.1.10.1
 zone remote DGKE customer.com 10.1.12.1
 zone prefix SJC 408.......
 zone prefix DGKW ..........
 zone prefix DGKE ..........
 bandwidth remote 192
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-9　ゲートキーパー 2（CHC）の設定

```
gatekeeper
 zone local GK-CHC customer.com 10.1.2.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix CHC 720.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 8-10　ゲートキーパー 3（NYC）の設定

```
gatekeeper
 zone local NYC customer.com 10.1.3.1
 zone remote DGKE customer.com 10.1.12.1
 zone remote DGKW customer.com 10.1.10.1
 zone prefix NYC 212.......
 zone prefix DGKE ..........
 zone prefix DGKW ..........
 bandwidth remote 160
 gw-type-prefix 1# default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 8-8、例 8-9、および例 8-10 について説明します。

- Cisco Unified CallManager トランク登録をサポートするために、各 Cisco Unified CallManager クラスタにはローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、ローカル ゾーンと両方のリモート ゾーンにゾーン プレフィックスが設定されます。両方のディレクトリ ゲートキーパー プレフィックスは、10 個のドットです。一致するゾーン プレフィックスが設定されるとき、デフォルトで順次 LRQ が使用されます。ゲートキーパーは、コストが最低のディレクトリ ゲートキーパーに LRQ を送信します。応答がない場合、ゲートキーパーは、2 番目のディレクトリ ゲートキーパーに LRQ の送信を試みます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

Cisco Unified CallManager と CallManager Express の相互運用性

この項では、H.323 または SIP プロトコルを使用している Cisco Unified CallManager と Cisco Unified CallManager Express（CME。以前に Cisco IOS Telephony Services（ITS）と呼ばれていた製品）に関して、マルチサイト IP テレフォニー配置における相互運用性およびインターネットワーキングの要件について説明します。ここでは、Cisco Unified CallManager の制御する電話機と CME の制御する電話機との間での推奨する配置を中心に説明します。

Cisco CME 3.4 では、現時点でサポートされている Cisco IP SCCP Phone 7902、7905、7910、7912、7920、7935、7936、7940、7960、7970、7971、および Cisco IP Communicator に加えて、Cisco IP SIP Phone 7905、7912、7940、および 7960 を設定する機能が追加されています。CME を SIP 電話機で使用する場合は、WAN インターフェイスを SIP にする必要があります。CME SCCP 電話機は、H.323 または SIP の WAN インターフェイスでサポートされます。

すべてのコール シグナリングは、使用されるエンドポイントに関係なく、CME を通して送信されます。ただし、SCCP エンドポイントが同じ CME 上にある場合は、メディアが CME の周囲を流れることができるのに対して、SIP エンドポイントが同じ CME 上にある場合には、メディアは必ず CME を通って流れます。

次の各項では、Cisco Unified CallManager と Cisco Unified CallManager Express の相互運用を実現するためのガイドラインを示します。

- Cisco Unified CallManager および CME を SIP トランクで接続したマルチサイト IP テレフォニー配置（P.8-34）
- Cisco Unified CallManager と CME を H.323 トランクと IP-to-IP ゲートウェイで接続したマルチサイト IP テレフォニー配置（P.8-36）

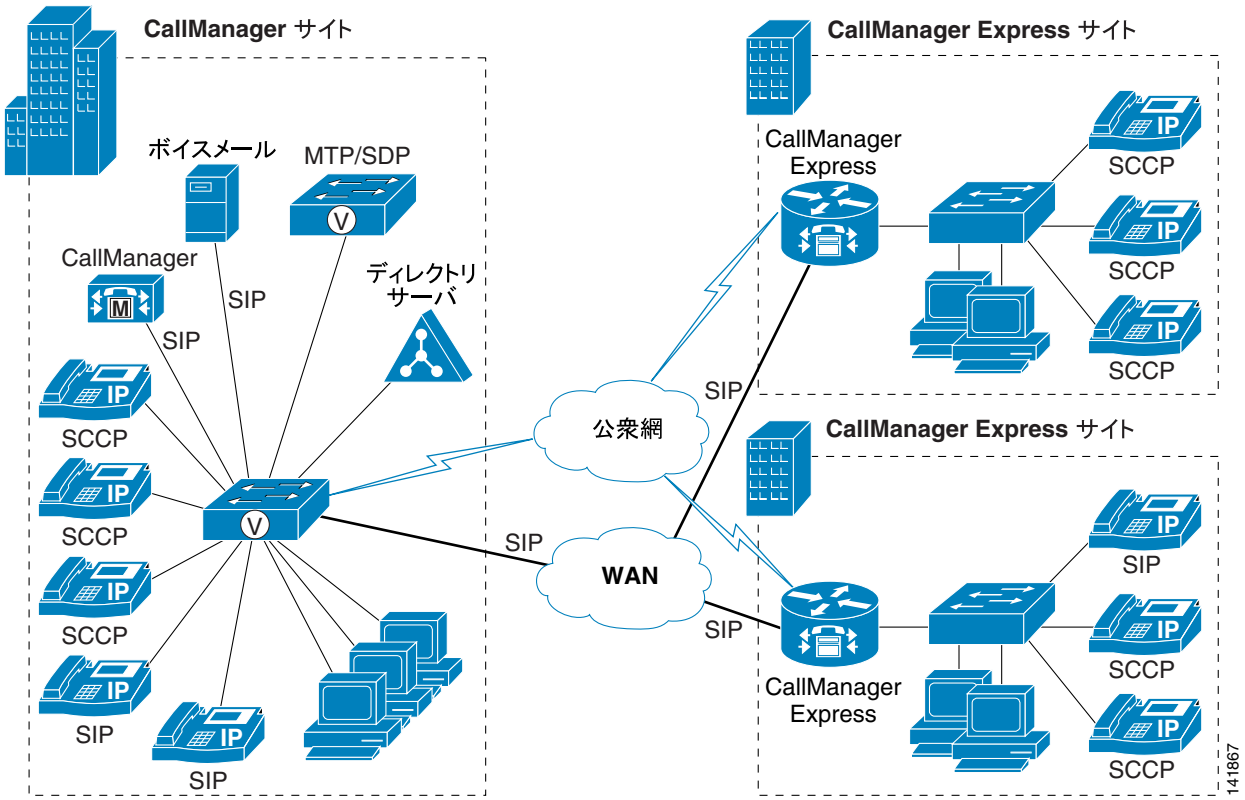
CME の詳細については、次の Web サイトで入手可能な Cisco Unified CallManager Express 製品マニュアルを参照してください。

http://www.cisco.com

Cisco Unified CallManager および CME を SIP トランクで接続したマルチサイト IP テレフォニー配置

Cisco Unified CallManager は、SIP インターフェイスを使用する Cisco Unified CallManager Express と直接通信することができます。図 8-10 では、SIP トランク WAN インターフェイスを使用して Cisco Unified CallManager が Cisco CME と直接にネットワーク接続されている IP テレフォニー配置を示しています。

図 8-10　Cisco Unified CallManager および CME を SIP トランクで接続したマルチサイト IP テレフォニー配置



ベスト プラクティス

図 8-10 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- **Replaces** ヘッダーを受け入れるように SIP トランク セキュリティ プロファイルを設定する。
- 作成した SIP トランク セキュリティ プロファイルを使用して SIP トランクを Cisco Unified CallManager 上に設定し、再ルーティング CSS も指定する。再ルーティング CSS は、どこで SIP ユーザ（転送者）が別のユーザ（被転送者）を第三者ユーザ（転送先）に振り向けることができるか、および SIP 3XX Redirection Response と Replaces を持つ INVITE を使用して SIP ユーザがどの機能を呼び出せるかを決定するために使用します。
- SIP トランクの場合、CME 上で SCCP エンドポイントを使用しているときに、メディア ターミネーション ポイント（MTP）を使用可能にする必要はない。ただし、CME 上に SIP エンドポイントがある場合は、メディア ターミネーション ポイントを Cisco Unified CallManager 上で使用して、SIP プロトコルで遅延オファー / アンサー交換の処理（Session Description Protocol なしの INVITE 受信）ができるようにする必要があります。

- Cisco Unified CallManager ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、CME に接続している SIP トランクにコールを送信する。
- Cisco Unified CallManager のデバイス プールとリージョンを使用して、サイト内では G.711 コーデックを設定し、リモートの CME サイトに対しては G.729 コーデックを設定する。
- CME の **voice services voip** で **allow-connections sip to sip** コマンドを設定して、SIP-to-SIP コール接続を許可する。
- SIP エンドポイントの場合は、**voice register global** で **mode cme** コマンドを設定し、CME の SIP 電話機ごとに **voice register pool** コマンドで **dtmf-relay rtp-nte** を設定する。
- SCCP エンドポイントの場合は、CME の **telephony-service** で **transfer-system full-consult** コマンドと **transfer-pattern .T** コマンドを設定する。
- CME の **session protocol sipv2** および **dtmf-relay sip-notify rtp-nte** により、SIP WAN インターフェイスの voip ダイヤル ピアを設定し、Cisco Unified CallManager を宛先としてコールを転送します。

(注) 複数の公衆網接続（Cisco Unified CallManager に 1 つと CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Cisco Unified CallManager エンドポイントと CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

例 8-11 に、この SIP 配置モデルを使用した CME の設定例を示します。

例 8-11　SIP での Cisco CME 3.4 の設定

```
voice service voip
    allow-connections sip to sip
    sip
    registrar server
dial-peer voice 1 voip       /* To Cisco Unified CallManager endpoints */
    destination-pattern xxxx
    session protocol sipv2
    session target ipv4:10.10.10.20
    session transport udp    /* tcp can be used here also */
    dtmf-relay rtp-nte
    codec g729r8             /* Voice class can also be used */
    no vad
voice register global
    mode cme
    source-address 10.10.10.21 port 5060
voice register pool 1
    id mac 0007.0E8B.5777
    type 7940
    number 1 dn 1
    codec g729r8      /* Voice class can also be used */
    dtmf-relay rtp-nte
telephony-service
 ip source-address 10.10.10.22 port 2000
 create cnf-files
 keepalive 45
 max-conferences 8 gain -6
 moh music-on-hold.au
 transfer-system full-consult /* full-blind can also be used */
 transfer-pattern .T
```

ここで示したガイドラインに従うと、Cisco Unified CallManager 電話および CME 電話間で基本的なコールを使用できるようになります。H323 の代わりに SIP トランク インターフェイスを使用することで、CME 上で SCCP エンドポイントのみを使用するときに、MTP は必要なくなります。SIP エンドポイントが CME 上で使用されている場合は、Cisco Unified CallManager 上に MTP を設定する必要があります。

Cisco Unified CallManager と CME を H.323 トランクと IP-to-IP ゲートウェイで接続したマルチサイト IP テレフォニー配置

IP-to-IP ゲートウェイは、Cisco Unified CallManager など、H.450 をサポートしないシステムのためにプロキシ（フロントエンド）を提供する独立ルータです。IP-to-IP ゲートウェイは、Cisco Unified CallManager と CME ルータの中間に配置できます。H.450 をサポートしないエンドポイントに転送または自動転送するコールを終端し、再発信するための H.323-to-H.323 コール接続を提供します。

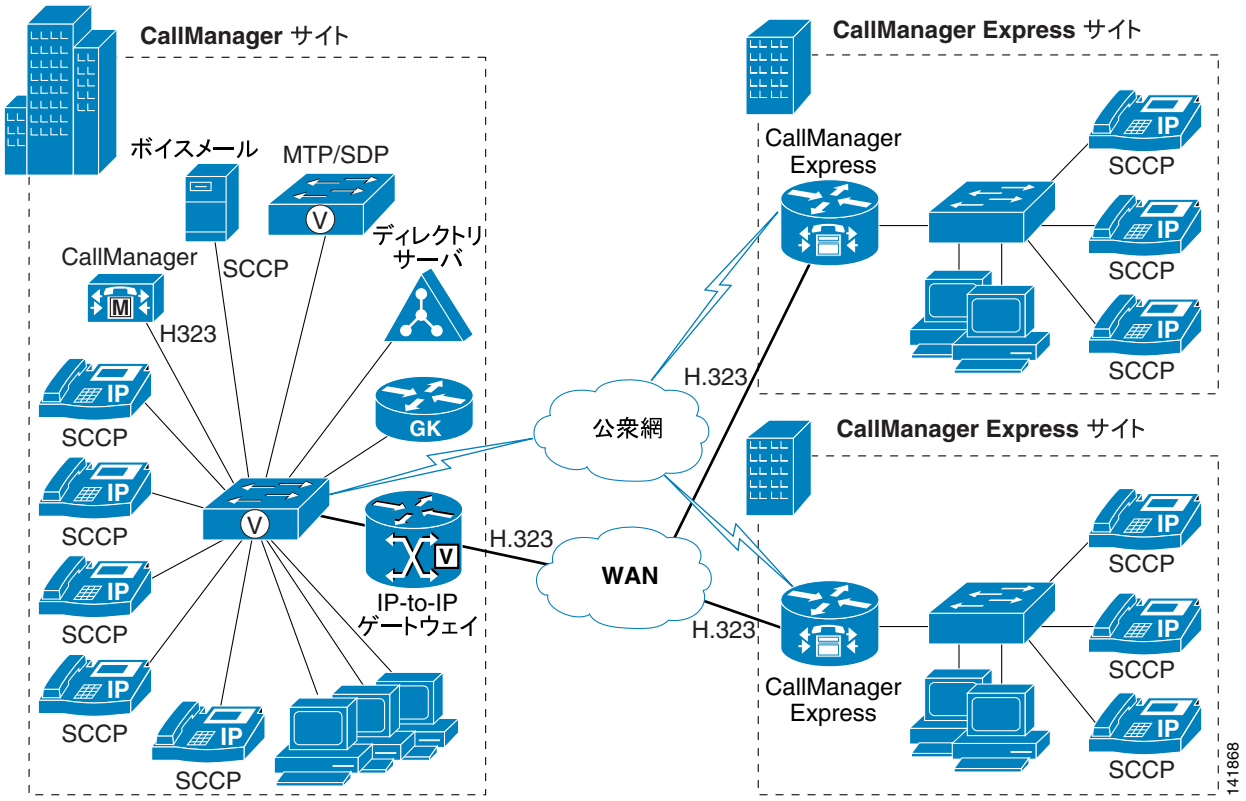
Cisco Unified CallManager Express は、IP-to-IP ゲートウェイなしで H.323 インターフェイスを使用して、Cisco Unified CallManager と直接統合することができます。ただし、Cisco Unified CallManager は H.450 仕様をサポートしていないため、Cisco Unified CallManager 電話から開始されたコール転送や自動転送などの補足サービスでは、Cisco Unified CallManager 電話がコールに関係しないときであっても、Cisco Unified CallManager を通した（場合によっては WAN 経由による）メディアのヘアピンが必要になります。IP-to-IP ゲートウェイは、このメディア ヘアピンが WAN 上で発生することを防止します。

また、IP-to-IP ゲートウェイは、Cisco Unified CallManager やリモート Cisco CME システム用の公衆網ゲートウェイとしても動作できます。この場合は、公衆網ゲートウェイを別に用意する必要がありません。

IP-to-IP ゲートウェイは、Cisco CME 3.4 と互換性があり、かつ H.450 をサポートしている Cisco IOS リリースを実行している必要があります。たとえば、IP VOICE 機能セットを備えた Cisco IOS Release 12.4(6)T 以降などです。

図 8-11 では、IP-to-IP ゲートウェイを通じて Cisco CME に接続されている Cisco Unified CallManager を使用した、IP テレフォニー配置を示しています。

図 8-11　Cisco Unified CallManager、CME、および IP-to-IP ゲートウェイで接続したマルチサイト IP テレフォニー配置



ベスト プラクティス

図 8-11 に示した配置モデルを使用する場合は、次のガイドラインに従い、ベスト プラクティスを参考にしてください。

- **Media Termination Point Required** をオンにし、**Wait For Far End H.245 Terminal Capability Set** をオフにして、ゲートキーパーが制御する H.225 トランクを Cisco Unified CallManager と IP-to-IP ゲートウェイ間に設定する。
- Cisco Unified CallManager で、サービス パラメータ **Send H225 user info message** を **H225 info for Call Progress Tone** に設定する。
- Cisco Unified CallManager ダイヤル プランの設定（ルート パターン、ルート リスト、およびルート グループ）を使用して、IP-to-IP ゲートウェイに接続している H.225 トランクにコールを送信する。
- ゲートキーパー上に、Cisco CME と IP-to-IP ゲートウェイを H.323 ゲートウェイとして登録する。
- H.450 が Empty Capability Set（ECS）シグナリング変換を実行するには、メディア ターミネーション ポイント（MTP）が必要である。MTP は、IP-to-IP ゲートウェイ上に設定して Cisco Unified CallManager に登録する必要があります。MTP によって、特にまれなケースとして、WAN 経由でメディアのヘアピンが起きることがあります。メディア ターミネーション ポイントの詳細については、P.6-1 の「メディア リソース」の章を参照してください。
- IP-to-IP ゲートウェイ上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 コール接続を許可する。リモート CME ルータについては、このコマンドを有効にする必要はありません。

（注） CME と Cisco Unified CallManager の間に H.323 トランクを使用する場合は、CME 上で **allow-connection h323 to h323** コマンドを設定して、H.323-to-H.323 ヘアピン コール接続を許可します。CME 3.1 からの Cisco Unified CallManager 自動検出機能を使用すると、Cisco Unified CallManager に接続されているインターフェイス上での H.450 ベースの通信が、すべて無効になります。Cisco Unified CallManager 電話と CME 電話間でコール転送または自動転送を確立するには、H.323-to-H.323 接続が必要です。

- IP-to-IP ゲートウェイ上で VoIP ダイヤル ピアを定義して、コールを Cisco Unified CallManager および CME のエンドポイントにルーティングする。
- CME 上で VoIP ダイヤル ピアを定義して、Cisco Unified CallManager エンドポイントを宛先とするコールを IP-to-IP ゲートウェイに転送する。
- コール転送や自動転送などの補足サービスでは、2 つのエンドポイントが同じ CME 支店ロケーションに存在する場合に、コールのメディア ヘアピンが発生する。

（注） 複数の公衆網接続（Cisco Unified CallManager に 1 つと CME に 1 つ）が存在する場合、公衆網エンドポイントに対する Cisco Unified CallManager エンドポイントと CME エンドポイント間の完全在席転送は失敗します。複数の公衆網接続を使用する場合にはブラインド転送の使用を推奨し、この設定は **telephony-service** で **transfer-system full-blind** として行います。

例 8-12 に、IP-to-IP ゲートウェイの設定例を示します。

例 8-12　IP-to-IP ゲートウェイの設定

```
voice service voip
    allow-connections h323 to h323
    supplementary-service h450.2
    supplementary-service h450.3
    supplementary-service h450.12
    h323
    emptycapability
    h225 id-passthru
    h225 connect-passthru
    h245 passthru tcsnonstd-passthru
dial-peer voice 1 voip        /* To Cisco Unified CallManager endpoints */
    destination-pattern xxxx
    session target ipv4:y.y.y.y
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
dial-peer voice 1 voip        /* To Cisco Unified CallManager endpoints */
    destination-pattern zzzz
    session target ras        /* "ras" if gatekeeper is used, otherwise "ipv4:a.b.c.d"
*/
    dtmf-relay h245-alphanumeric
    codec g729r8
    no vad
```

例 8-13 に、この H.323 配置モデルでの CME の設定例を示します。

例 8-13　H.323 での Cisco CME 3.4 の設定

```
voice service voip
    h323
interface FastEthernet0/1
    ip address 10.10.10.23 255.255.255.0
    h323-gateway voip interface
    h323-gateway voip id cme ipaddr 10.10.10.30 1719
dial-peer voice 1 voip       /* To Cisco Unified CallManager endpoints */
    destination-pattern xxxx
    session target ras
    session transport tcp
    codec g729r8             /* Voice class can also be used */
    no vad
telephony-service
 ip source-address 10.10.10.22 port 2000
 create cnf-files
 keepalive 45
 max-conferences 8 gain -6
 moh music-on-hold.au
 transfer-system full-blind /* Used with multiple PSTN connections */
 transfer-pattern .T
```

コール アドミッション制御

コール アドミッション制御機能は、IP WAN 経由で接続された複数のサイトで構成されるすべての IP テレフォニー システムに不可欠なコンポーネントです。コール アドミッション制御の機能と必要性をわかりやすく説明するために、図 9-1 の例について考えます。

図 9-1　　コール アドミッション制御が必要な理由

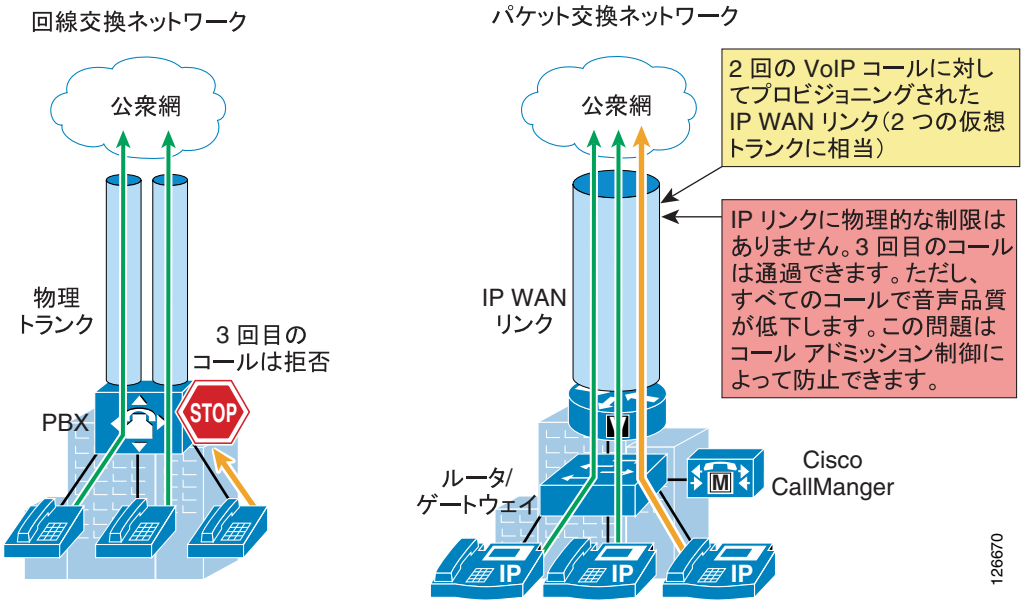


図 9-1 の左側で示すように、従来の TDM ベースの PBX は、回線交換ネットワークの一部として動作します。このネットワークでは、回線はコールがセットアップされるたびに確立されます。このため、レガシー PBX が公衆網または他の PBX に接続されている場合は、一定数の物理トランクを設定する必要があります。公衆網または他の PBX 宛てのコールをセットアップする必要があるとき、PBX は、使用可能なトランクの中からトランクを選択します。使用可能なトランクがない場合、コールは PBX によって拒否され、発信者にはネットワーク ビジー信号が聞こえます。

次に、図 9-1 の右側に示している IP テレフォニー システムについて考えます。このシステムは、パケット交換ネットワーク（IP ネットワーク）を基盤としているため、IP テレフォニー コールをセットアップするために回線を確立する必要はありません。サンプリング音声を含んでいる IP パケットが、他のタイプのデータ パケットとともに、IP ネットワーク経由でルーティングされるだけで

す。音声パケットは、QoS（Quality Of Service）を使用してデータ パケットと区別されますが、帯域幅リソースは、特に IP WAN リンクでは無限ではありません。このため、ネットワークの管理者が、一定量の「優先」帯域幅を各 IP WAN リンク上の音声トラフィック専用として割り当ててください。ただし、設定した帯域幅がすべて使用される状態になった場合は、IP テレフォニー システムで以後のコールを拒否して、IP WAN リンク上のプライオリティ キューのオーバーサブスクリプションを防止する必要があります。オーバーサブスクリプションが発生すると、すべての音声コールで品質が低下します。この機能はコール アドミッション制御と呼ばれ、IP WAN を利用したマルチサイト配置で良好な音声品質を保証するために不可欠なものです。

エンド ユーザ環境の満足度を維持するには、コール アドミッション制御機能を常にコール セットアップ段階で実行する必要があります。このようにすることで、ネットワーク リソースを使用できない場合に、エンド ユーザにメッセージを表示したり、異なるネットワーク（公衆網などの）を通じてコールを再ルーティングしたりすることができるようになります。

この章では、次の主要トピックについて説明します。

- ベスト プラクティスの概要（P.9-3）

  この項では、この章で説明する原理とメカニズムにすでに精通している読者向けに、コール アドミッション制御に関する主なベスト プラクティス、推奨事項、および注意事項の概要を示します。

- コール アドミッション制御の原理（P.9-4）

  この項では、IP ベースのテレフォニー システムにおけるコール アドミッション制御の 2 つの基本的な方法である、トポロジ対応とトポロジ非対応のコール アドミッション制御について説明します。

- コール アドミッション制御の要素（P.9-13）

  ここでは、Cisco Unified Communications システムのさまざまなコンポーネント、たとえば Cisco Unified CallManager ロケーション、Cisco IOS ゲートキーパー、RSVP、IP-to-IP ゲートウェイなどで使用できるコール アドミッション制御メカニズムについて説明します。

- コール アドミッション制御の設計（P.9-38）

  ここでは、上の項で説明したメカニズムを適用し、組み合せる方法について、IP WAN のトポロジ（単純なハブアンドスポーク、2 層ハブアンドスポーク、MPLS、またはその他のトポロジ）に基づいて、および採用する Cisco Unified CallManager 配置モデルに基づいて示します。

ベスト プラクティスの概要

ここでは、さまざまな Cisco Unified CallManager 配置でコール アドミッション制御を提供するためのベスト プラクティスについて、簡単に概要を示します。これらのベスト プラクティスについては、この章の他の部分で詳細に説明します。

次の推奨事項は、単一の Cisco Unified CallManager クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Cisco Unified CallManager 静的ロケーションを使用します。ハブ サイト デバイスは Hub_None ロケーションのままにします。
- デュアル リンクのない Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）トポロジでは、（中央サイトを含む）すべてのサイトのデバイスを 1 つのロケーションに割り当てて、Cisco Unified CallManager 静的ロケーションを使用します。
- その他のトポロジでは、Cisco Unified CallManager RSVP 対応ロケーションを使用します。サイト間のデフォルト RSVP ポリシーには、**Mandatory** または **Mandatory (video desired)** ポリシーをお勧めします。Cisco RSVP Agent 機能は、比較的小さなサイトでは IP WAN ルータに常駐している場合もあります。また、比較的大きなサイトではスタンドアロン プラットフォームで実行される場合もあります。

次の推奨事項は、複数の Cisco Unified CallManager クラスタによる配置に適用されます。

- デュアル リンクのない単純なハブアンドスポーク トポロジでは、Cisco Unified CallManager クラスタが存在するサイト間の Cisco IOS ゲートキーパー ゾーンを使用します。
- Cisco Unified CallManager クラスタが第 1 レベルおよび第 2 レベルのハブ サイトに配置された、デュアル リンクのない 2 層ハブアンドスポーク トポロジでは、第 1 レベルと第 2 レベルのハブ サイト間のリンクに Cisco IOS ゲートキーパー ゾーンを使用し、第 2 レベルのハブ サイトとスポーク サイト間のリンクには Cisco Unified CallManager 静的ロケーションを使用します。
- デュアル リンクのない MPLS トポロジでは、すべてのサイトを 1 つのロケーションに配置し、ゲートキーパー ゾーンなしで、Cisco Unified CallManager 静的ロケーションを使用します。MTP が必要な場合を除いて、クラスタ間トランクは Hub_None ロケーションのままにします。クラスタ間コール ルーティング用にはゲートキーパーを使用できますが、コール アドミッション制御では必要ありません。
- その他のトポロジと 3 つ以下のクラスタでは、RSVP 対応ロケーションおよび「リモート エージェント」方法を使用します。
- その他のトポロジと 3 つを超えるクラスタでは、各クラスタ内で RSVP 対応のロケーションを使用し、クラスタ間では RSVP 対応の IP-to-IP ゲートウェイを持つゲートキーパーを使用します。

コール アドミッション制御の原理

すでに述べたように、コール アドミッション制御は、IP ベースのテレフォニー システムのコール処理エージェントの機能です。したがって理論上は、IP ベースのテレフォニー システムと同じ数のコール アドミッション制御メカニズムが存在する可能性があります。しかし、ほとんどの既存のコール アドミッション制御メカニズムは、次の 2 つの主なカテゴリのいずれかになります。

- トポロジ非対応コール アドミッション制御：コール処理エージェント内の静的設定に基づくもの
- トポロジ対応コール アドミッション制御：使用可能なリソースに関するコール処理エージェントとネットワーク間の通信に基づくもの

以下この項では、トポロジ非対応コール アドミッション制御の原理とその制限について分析し、次にトポロジ対応コール アドミッション制御の原理を示します。

トポロジ非対応コール アドミッション制御

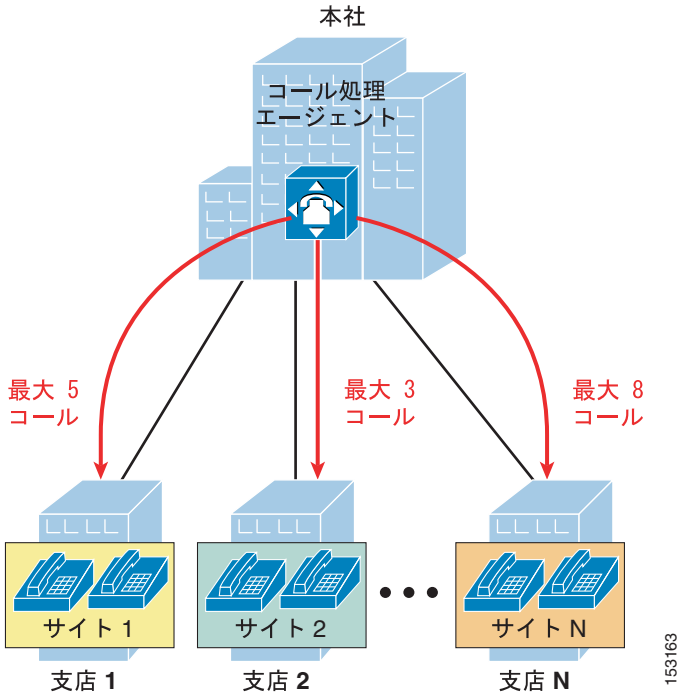
トポロジ非対応コール アドミッション制御とは、IP WAN で接続されたリモート サイトとの間の同時コール数を制限することを目的とし、コール処理エージェントまたは IP ベースの PBX 内の静的設定に基づくメカニズムです。

図 9-2 に示すように、このようなメカニズムのほとんどは、一般に企業 IP WAN に接続される地理上の支店に対応する、論理的な「サイト」エンティティの定義に依存しています。

各支店にあるすべてのデバイスを対応するサイト エンティティに割り当てた後に、管理者がそのサイトを宛先または発信元とするコールの許容最大数（または帯域幅の最大量）を設定するのが一般的です。

新しいコールの確立が必要になるたびに、コール処理エージェントは発信エンドポイントおよび終端エンドポイントが属するサイトをチェックし、（関係する両サイトのコール数または帯域幅の量に関して）コールに利用できるリソースがあるかどうか確認します。チェックが成功した場合、そのコールは確立され、両サイトのカウンタが減少します。チェックに失敗した場合、コール処理エージェントは事前に設定されたポリシーに基づいてコールの処理方法を決定できます。たとえば、発信者のデバイスにネットワーク ビジー信号を送信したり、公衆網接続を通じて再ルーティングを試行します。

図 9-2　トポロジ非対応コール アドミッション制御の原理



トポロジ非対応のコール アドミッション制御メカニズムは静的設定に依存しているため、一般に比較的単純な IP WAN トポロジのネットワークだけに配置できます。実際、このようなメカニズムのほとんどでは、図 9-3 に示すような単純なハブアンドスポーク トポロジまたは単純な MPLS ベースのトポロジ（MPLS サービスがサービス プロバイダーによって提供される場合）が必要です。

図 9-3　トポロジ非対応コール アドミッション制御に適したドメイン

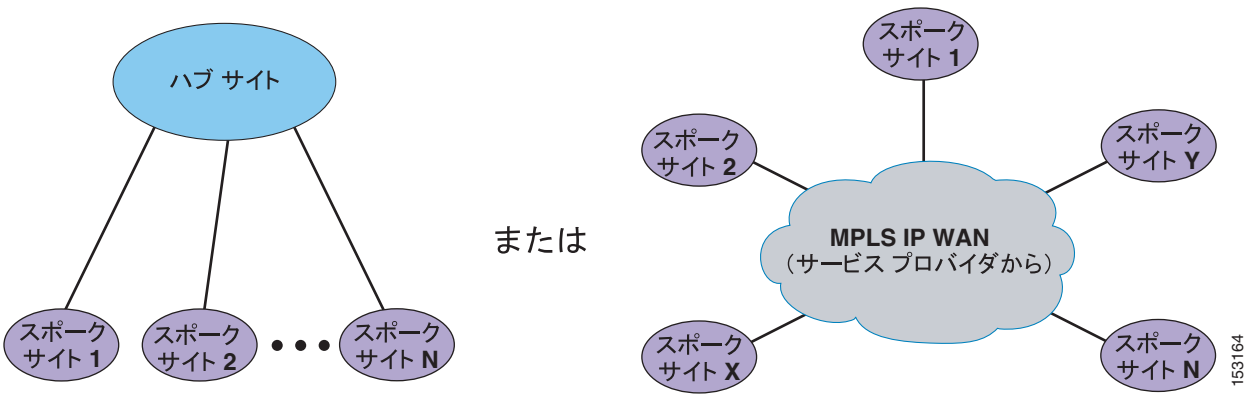


図 9-3 に示すようなハブアンドスポーク ネットワークまたは MPLS ベースのネットワークで、各スポーク サイトはコール処理エージェント内の「サイト」に割り当てられ、その「サイト」のコール数または帯域幅の量は、そのスポークを IP WAN に接続する IP WAN リンク上の音声またはビデオ（あるいはその両方）に利用可能な帯域幅と一致するように設定されます。

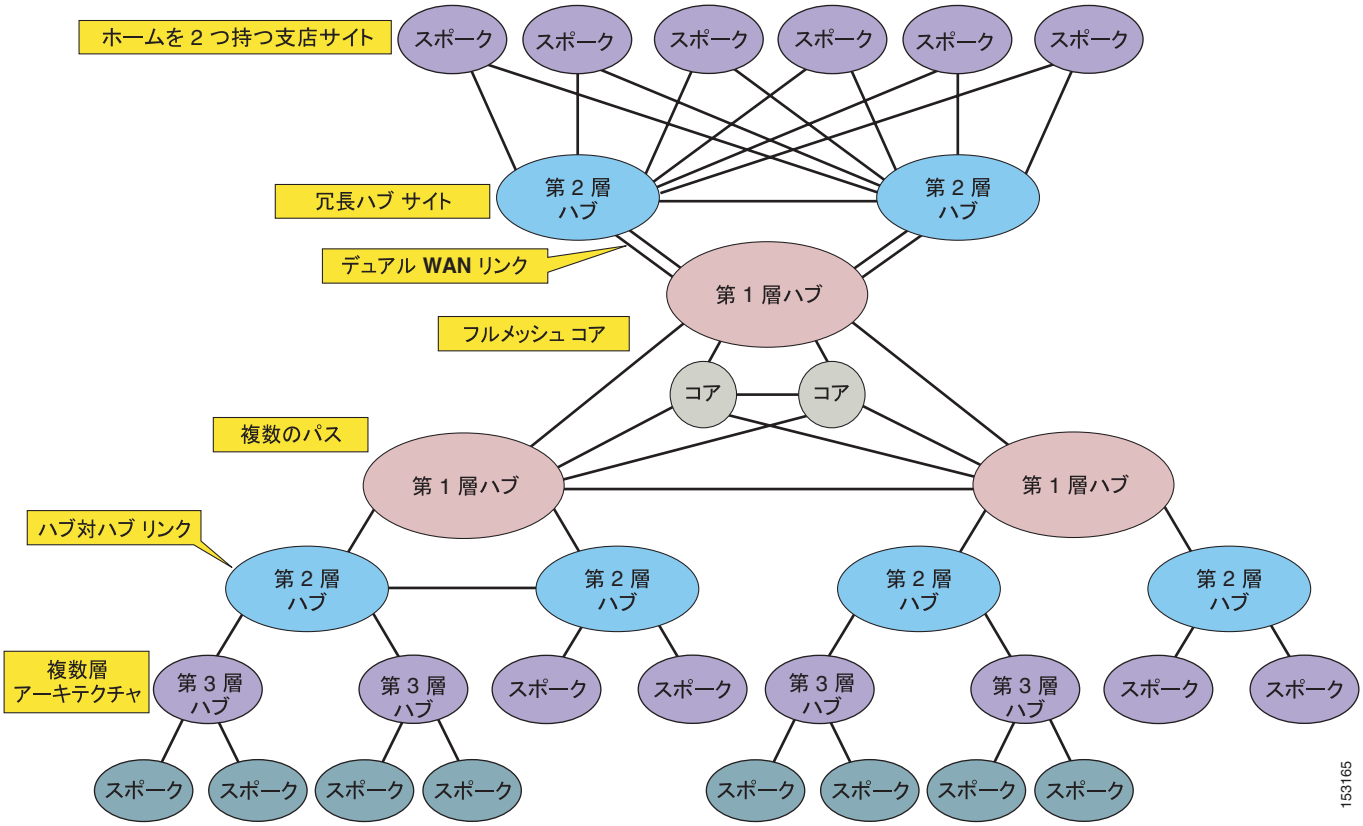
スポーク サイトからハーブ サイトへの冗長リンクと、2 つのスポーク サイトを直接接続するリンクがないことに注意してください。次の項では、トポロジ非対応コール アドミッション制御で、このようなリンクが問題を発生させる理由について説明します。

トポロジ非対応コール アドミッション制御の制限

現在の企業ネットワークでは、高可用性は共通の要件であり、そのために IP WAN ネットワーク接続に冗長性が求められることがあります。

代表的な企業ネットワークにおける IP WAN トポロジについて考えると、純粋なハブアンドスポーク トポロジの前提を複雑にする数多くの特性があることがわかります。図 9-4 は、このようなネットワーク特性のいくつかを 1 つの図にまとめたものです。すべての特性が一度に現れるのは大規模な企業ネットワークだけですが、多くの IP WAN ネットワークでも最低 1 つの特性が存在していることがよくあります。

図 9-4　代表的な企業ネットワークのトポロジ特性



P.9-38 の「コール アドミッション制御の設計」の項で説明するように、複雑なネットワーク トポロジにトポロジー非対応コール アドミッション制御メカニズムを適用できる場合がありますが、この方法を利用できる場合と、実現できる動作に関して制限があります。たとえば、冗長性がネットワーク要件となっている IP WAN を通じてハブ サイトに接続される支店サイトの単純なケースについて考えます。一般的に、冗長性は次のいずれかの方法で実現できます。

- IP WAN へのプライマリ リンクとバックアップ リンクを備えた 1 台のルータ
- ロード バランシング設定で 2 つのアクティブな WAN リンクを備えた 1 台のルータ
- それぞれが IP WAN に接続され、ロード バランシングされたルーティングを行う 2 つのルータ プラットフォーム

図 9-5 の例では、プライマリ リンクとバックアップ リンクを備えた 1 台のルータの場合と、2 つのアクティブなロード バランシング リンクを備えた 1 台のルータの場合に、トポロジ非対応コール アドミッション制御メカニズムを適用しようとしています（2 つのルータ プラットフォームの場合のコール アドミッション制御に対する影響は、後者の例と同じです）。

図 9-5　デュアル リンクが存在する場合のトポロジ非対応コール アドミッション制御

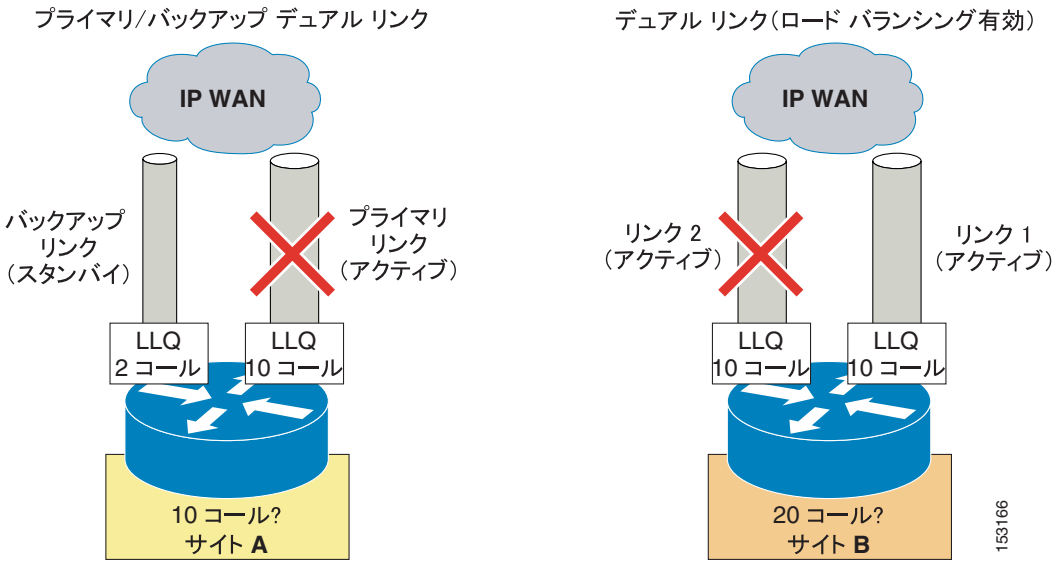


図 9-5 の最初の例で、支店 A は通常、最大 10 の同時コールが可能になるよう、Low Latency Queuing（LLQ; 低遅延キューイング）帯域幅がプロビジョニングされたプライマリ リンクを通じて、IP WAN に接続されます。このプライマリ リンクに障害が発生した場合、小さい方のバックアップ リンクがアクティブになり、IP WAN への接続を維持します。ただし、このバックアップ リンクの LLQ 帯域幅は、最大 2 つの同時コールだけが可能なようにプロビジョニングされています。

この支店にトポロジ非対応コール アドミッション制御メカニズムを配置するには、コール処理エージェントで「サイト」A を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。サイト A の最大値として 10 コールを使用する場合、プライマリ リンクの障害時にバックアップ リンクにオーバーランが発生し、すべてのアクティブなコールで音声の品質が低下する可能性があります。これに対して、最大値を 2 コールにした場合、プライマリ リンクがアクティブなときは、残りの 8 コールに対してプロビジョニングされた帯域幅を使用できません。

次に、IP WAN に接続する 2 つのアクティブなリンクを備えた支店 B について考えます。各リンクは、最大 10 の同時コールが可能なようにプロビジョニングされ、ルーティング プロトコルは各リンク間のロード バランシングを自動的に実行します。この支店にトポロジ非対応コール アドミッション制御メカニズムを配置する場合、コール処理エージェントで「サイト」B を定義し、一定のコール数（または帯域幅の量）を設定する必要があります。支店 A の場合と同様に、2 つのリンクの容量を増強し、サイト B の最大値として 20 コールを使用する場合、一方のリンクの障害時に、もう一方のリンクで LLQ のオーバーランが発生する可能性があります。たとえば、リンク #2 に障害が発生した場合、サイト B を宛先または発信元とする 20 の同時コールが引き続き可能です。これらのコールは、すべてリンク #1 を通じてルーティングされるようになるため、オーバーランが発生し、すべてのコールで音声品質が低下します。これに対して、最大 10 の同時コールでサイト B を設定した場合、（両方のリンクが動作している）通常の条件では、使用可能な LLQ 帯域幅が十分に活用されなくなります。

上記の 2 つの単純な例は、実際の企業ネットワークでの IP WAN 帯域幅のプロビジョニングが非常に複雑で、コール処理エージェント内の静的に設定されたエントリにまとめられない場合があることを示しています。このようなネットワークでトポロジ非対応コール アドミッション制御を配置すると、管理者は推測をしたり、回避策を取ったり、最適ではないネットワーク リソースの使用を許容したりする必要があります。

単純なハブアンドスポークに従わないネットワーク トポロジが存在する場合にコール アドミッション制御を提供する最適な方法は、次の項で説明するようにトポロジ対応コール アドミッション制御を実装することです。

(注)　一部の IP テレフォニー システムは、ネットワークで観察された輻輳に基づくフィードバック メカニズムで、従来のトポロジ非対応コール アドミッション制御を拡張します。これにより、音声品質が低下した場合、コールが強制的に公衆網経由になります。コール処理エージェントはコールの確立後に実行されることと、輻輳が発生している正確な場所を認識しないという理由から、この方法はまだ真のトポロジ対応コール アドミッション制御と同等ではありません。この章の最初に述べたように、効果的に運用するには、コールをセットアップする前にコール アドミッション制御を実行する必要があります。

トポロジ対応コール アドミッション制御

トポロジ対応コール アドミッション制御とは、IP WAN リンクを通じた同時コール数を制限することを目的とするメカニズムであり、任意のネットワーク トポロジに適用でき、またトポロジの変更にも動的に適応できます。

このような目的を達成するには、トポロジ対応コール アドミッション制御は、コール処理エージェント（または IP ベースの PBX）とネットワーク間のネットワーク リソースの可用性に関するリアルタイム通信を利用する必要があります。ネットワークは分散エンティティであるため、リアルタイムの通信にはシグナリング プロトコルが必要です。

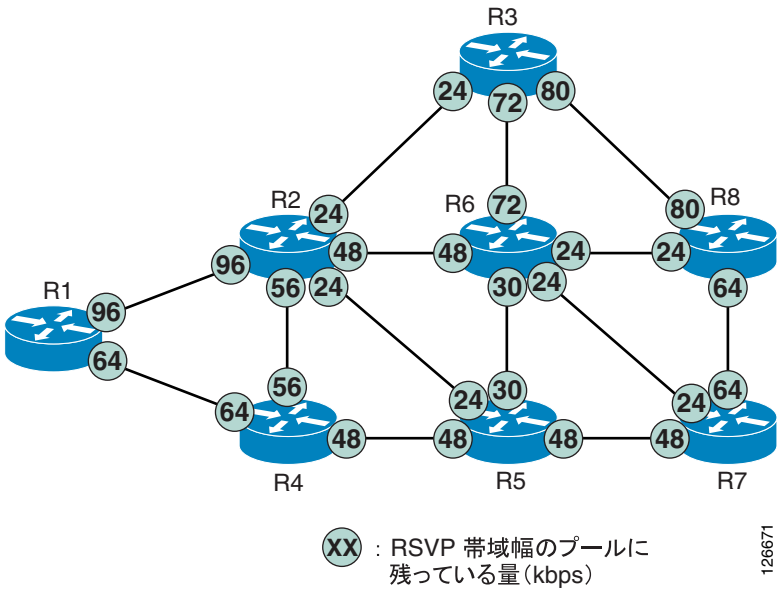
Resource Reservation Protocol（RSVP; リソース予約プロトコル）は、アプリケーションが IP ネットワークを通じて動的に帯域幅を予約できるようにするための、最初の重要な業界標準シグナリング プロトコルです。RSVP を使用すると、アプリケーションはネットワークを通じたデータ フロー（音声コールなど）のために一定の帯域幅を要求し、実際のリソースの可用性に基づいて予約結果の通知を受け取ることができます。

音声コールまたはビデオ コールのためのコール アドミッション制御の特定のケースで、IP ベースの PBX は、2 つのリモート サイト間でコール セットアップ プロセスを RSVP 予約と同期し、予約の結果に基づいてルーティングの決定を行います。分散型ネットワークに対応し、動的に機能する性質を持っているため、RSVP はあらゆるネットワーク トポロジにわたって帯域幅を予約できます。つまり、本格的なトポロジ対応コール アドミッション制御メカニズムを提供します。

RSVP がネットワークで帯域幅予約を実行する方法の基本的な原理を理解するために、図 9-6 に示す簡単な例について考えます。この例では、メッセージ交換とプロトコルの動作自体については説明しません。機能によってもたらされる結果を中心に説明します。RSVP メッセージ交換の詳細については、P.3-38 の「RSVP の原理」を参照してください。

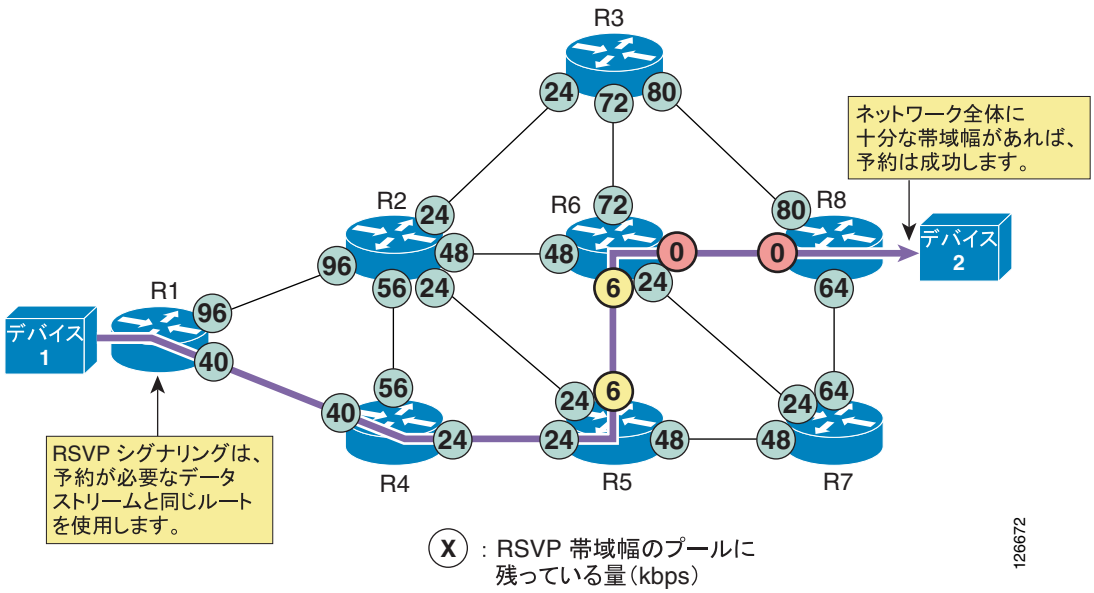
図 9-6 に示すネットワークの各ルータ インターフェイスで、RSVP が有効になっているとします。円で囲まれた数値は、各インターフェイス上に残っている使用可能な RSVP 帯域幅の量を表しています。

図 9-6　RSVP の原理を示すためのサンプル ネットワーク



ここで、RSVP 対応のアプリケーションが、2 つのデバイス間でのデータ ストリーム用に一定の帯域幅を予約するとします。このシナリオを図 9-7 に示します。この図では、デバイス 1 からデバイス 2 への個々のデータ ストリームで、24 Kbps の帯域幅を要求することを示しています。

図 9-7　予約が成功する RSVP シグナリング

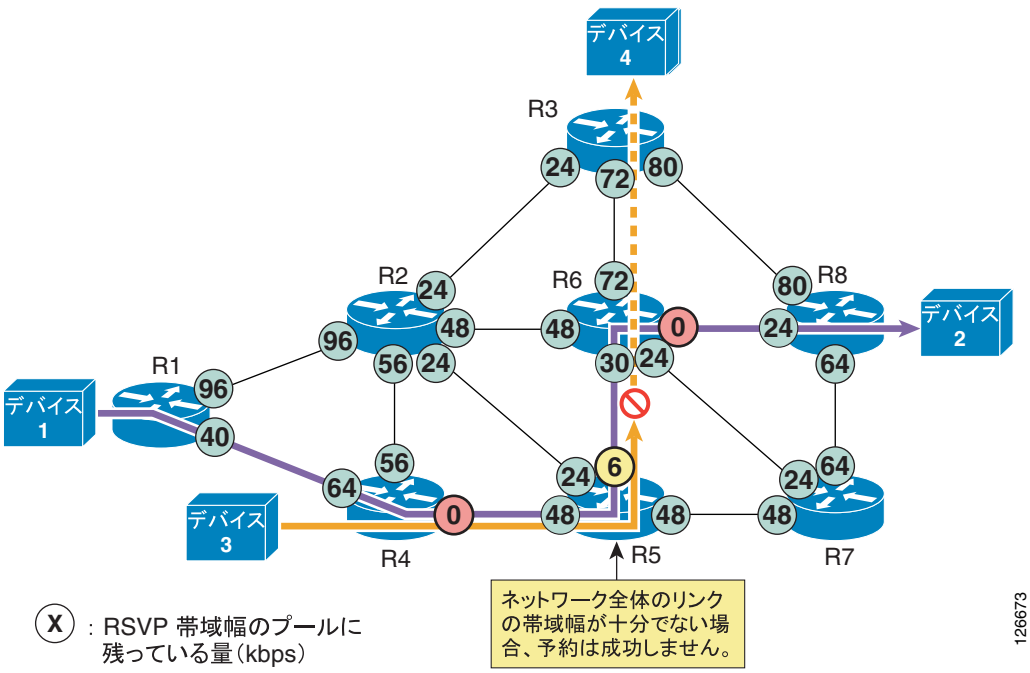


ここでは、図 9-7 について説明します。

- RSVP は、自身ではルーティングを実行しません。代わりに、下層で機能しているルーティング プロトコルを使用して、予約要求の宛先を決定します。トポロジの変更に対応するためにルーティングのパスが変化すると、RSVP は、自身の予約を予約が存在する新しいパスに合せて調整します。
- RSVP プロトコルは、デバイス 1 からデバイス 2 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 9-7 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- 使用可能な帯域幅がすべての発信側インターフェイスで十分にあり、この新しいデータ　ストリームを受け付けることができる場合は、予約が成功し、アプリケーションに通知されます。
- RSVP 予約は単方向です。この例では、予約はデバイス 1 からデバイス 2 に向かって確立され、逆方向については確立されません。音声会議やビデオ会議などの双方向アプリケーションがある場合は、各方向について 1 つずつ、2 つの予約を確立する必要があります。
- RSVP は、RSVP をサポートしないルータ ノードでは透過的に動作します。RSVP に対応しないルータがパスに存在していても、それらのルータは単に RSVP メッセージを無視して、他の IP パケットと同様に渡すだけであり、予約を確立することは可能です（プロトコルのメッセージと動作の詳細については、P.3-38 の「RSVP の原理」を参照してください）。ただし、エンドツーエンドでの QoS を確保するには、この RSVP 非対応のルータが制御するリンク上で、帯域幅の輻輳が発生しないようにする必要があります。

デバイス 1 とデバイス 2 の間で予約が正常に確立された後に、別のアプリケーションがデバイス 3 とデバイス 4 の間で 24 Kbps の予約を要求したとします（図 9-8 を参照）。

図 9-8　予約が成功しない RSVP シグナリング



ここでは、図 9-8 について説明します。

- RSVP プロトコルは、デバイス 3 からデバイス 4 へのパスにあるすべての RSVP 対応ルータ上で、使用可能な帯域幅リソースを確認することによって、エンドツーエンドの予約を確立しようとします。図 9-8 に示すように、RSVP メッセージがネットワークを進んでいくとき、発信側ルータ インターフェイスでは、使用可能な RSVP 帯域幅が 24 Kbps ずつ減分されます。
- この例では、R6 に対する R5 の発信側インターフェイス上に、この新しいデータ ストリームを受け付けるための使用可能な帯域幅が十分にありません。このため、予約は失敗し、アプリケーションに通知されます。パスに含まれている各発信側インターフェイス上の使用可能な RSVP 帯域幅は、以前の値に戻されます。
- 次にどのように処理するかは、アプリケーションが決定します。データの転送を放棄することも、何らかの方法で QoS 保証のないベストエフォート型トラフィックとして送信することもできます。

ここで、前の項で紹介した二重接続される支店 A および B の例に、RSVP に基づくトポロジ対応コール アドミッション制御方法を適用できます。

図 9-9 に示すように、支店 A には 10 コール用にプロビジョニングされた LLQ を備えるプライマリ リンクと、2 つのコールだけを許容するバックアップ リンクがあります。この方法で RSVP は、RSVP 帯域幅が LLQ 帯域幅と一致するように、両方のルータ インターフェイスで設定されます。支店 A は、他の支店を宛先または発信元とするすべてのコールの RSVP 予約を要求するために、コール処理エージェント内でも設定されます。これで、コールは、ルーティング プロトコルによって決定されるパスに自動的に従う RSVP 予約の結果に基づいて、許可または拒否されるようになります。通常の条件下では（プライマリ リンクがアクティブな場合）、最大 10 コールが許容されます。プライマリ リンクの障害時には、最大 2 コールだけが許容されます。

ポリシーは、一般にコール アドミッション制御に障害が発生した場合の動作を決定するために、コール処理エージェント内で設定できます。たとえば、コールを拒否したり、公衆網を通じて再ルーティングしたり、異なる DSCP マーキングでのベストエフォート コールとして IP WAN を通じて送信したりすることができます。

図 9-9　デュアル リンクのトポロジ対応コール アドミッション制御

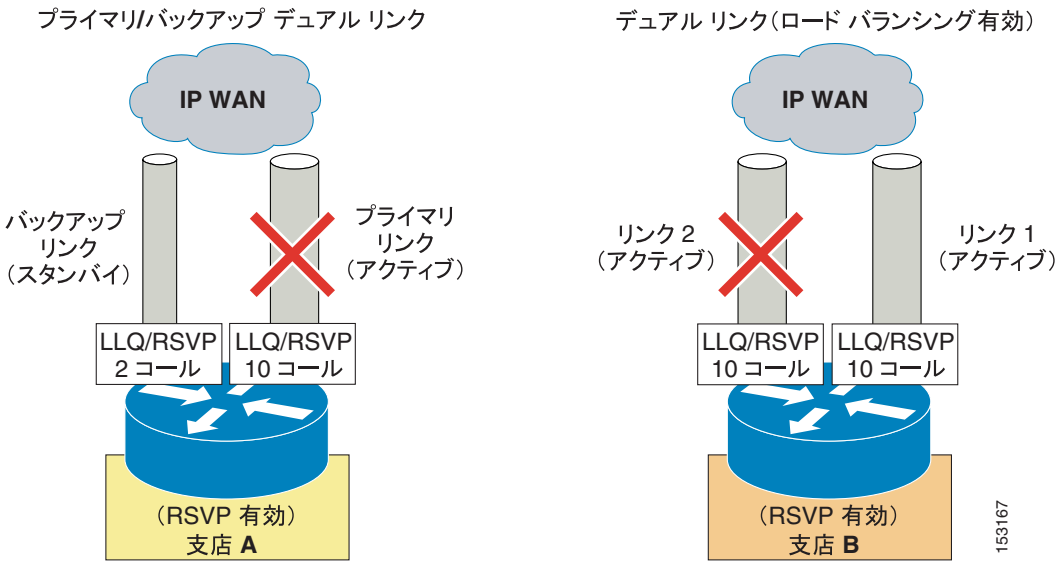


図 9-9 の右側に示すように、2 つのロード バランシング リンクを通じて IP WAN に接続される支店 B にも、同様の考慮事項が該当します。RSVP は、LLQ 設定と一致する帯域幅の値（この場合は、10 コールに対して十分な帯域幅）で、2 つのルータ インターフェイスのそれぞれで有効になります。支店 B は、他の支店との間のコール用に RSVP 予約を要求するため、コール処理エージェント内でも設定されます。このときも、コールはルーティング プロトコルが決定するパスに沿って、使用可能な実際の帯域幅に基づいて許可または拒否されるようになります。したがって、2 つのリンクを通じた完全に均等なロード バランシングの場合、（両方のリンクが動作している）通常の条件下で最大 20 コールを許容できます。2 つのリンクのいずれかに障害が発生した場合は、最大 10 コールだけが許容されます。

10 を超えるコールがアクティブなときに 2 つのリンクのいずれかに障害が発生した場合、一部のコールは新しいパスでの予約の再確立に失敗します。この時点で、コール処理エージェントは通知を受け、設定されたポリシーに基づいて対応することができます（追加のコールをドロップしたり、ベストエフォート コールとして再マーキングします）。

要するに、トポロジ対応コール アドミッション制御によって、管理者は任意のネットワーク トポロジでコール品質を保護し、トポロジの変更に自動的に適応し、すべての状況の下でネットワーク リソースを最適に使用することができます。

MPLS ネットワークの特別な考慮事項

コール アドミッション制御の点から見ると、ネットワークの「ハブ」での RSVP のサポートに関して、MPLS に基づくネットワークは従来のレイヤ 2 WAN サービスに基づくネットワークとは異なっています。従来のレイヤ 2 WAN は、ほとんどの場合、RSVP への参加を有効にできる企業管理のルータから構成されます。MPLS ネットワークではネットワーク全体（クラウド）が「ハブ サイト」であるため、RSVP を有効にするための企業管理のハブ ロケーションは存在しません（詳細については、P.9-46 の「単純な MPLS トポロジ」を参照してください）。したがって、MPLS 環境でトポロジ対応コール アドミッション制御を提供するには、RSVP のサポート用にネットワークの Customer Edge（CE）デバイスを設定する必要があります。

RSVP は CE で有効にする必要があるため、この機器の制御は重要です。この機器が企業で管理されていない場合、サービス プロバイダーに問い合せて、WAN インターフェイスで RSVP が有効になっているかどうか、およびその実装で RSVP アプリケーション ID などの高度な機能がサポートされるかどうかを確認する必要があります。

RSVP メッセージは、RSVP 非対応 MPLS クラウドを透過的に通過するため、エンドツーエンドの RSVP 機能で問題は生じません。CE WAN インターフェイスで RSVP を設定すると、そのプライオリティ キューにオーバーランが発生しなくなります。RSVP 予約は単方向であるため、RSVP が MPLS クラウドで有効になっていない場合、Provider Edge（PE）ルータでプライオリティ キューを保護するには、次の規則に従う必要があります。

- メディア ストリームを両方向で同じサイズにする。
- メディアを対称的にルーティングする。

MPLS ネットワークがこれらの規則に従っていない場合は、RSVP を実装する前にシスコのアカウント チームにお問い合せください。

コール アドミッション制御の要素

Cisco Unified Communications システムには、コール アドミッション制御機能を実行する複数のメカニズムがあります。この項では、次のカテゴリに従って、すべてのメカニズムの設計と設定のガイドラインについて説明します。

- トポロジ非対応メカニズム
  - Cisco Unified CallManager の静的ロケーション（P.9-13）
  - Cisco IOS ゲートキーパー ゾーン（P.9-16）
- トポロジ対応メカニズム
  - Cisco Unified CallManager の RSVP 対応ロケーション（P.9-18）
  - RSVP 機能のある Cisco IOS Gatekeeper および IP-to-IP ゲートウェイ（P.9-30）

(注) Cisco Unified CallManager 5.0 では、以前のリリースですでに存在していた「ロケーション」の概念を拡張することによって、トポロジ対応コール アドミッション制御が導入されています。したがって、このマニュアルでは以前のトポロジ非対応メカニズムを「静的ロケーション」と呼び、新しいトポロジ対応メカニズムを「RSVP 対応ロケーション」と呼ぶことにします。

Cisco Unified CallManager の静的ロケーション

Cisco Unified CallManager では、集中型コール処理配置において、コール アドミッション制御を実装するために、「静的ロケーション」と呼ばれている単純なメカニズムを取り入れています。Cisco Unified CallManager でデバイスを設定するときは、そのデバイスをロケーションに割り当てることができます。各ロケーションとの間のコールに対しては、特定の帯域幅が割り当てられます。Cisco Unified CallManager で設定するロケーションは、仮想ロケーションであり、実際の物理ロケーションではありません。Cisco Unified CallManager は、デバイスの物理的なロケーションを認識しません。このため、デバイスをある物理ロケーションから別のロケーションに移動する場合は、システム管理者がロケーション設定を手動でアップデートして、Cisco Unified CallManager がそのデバイスの帯域幅割り当てを正しく計算できるようにする必要があります。各デバイスは、デフォルトでは Hub_None ロケーションに配置されます。ロケーション Hub_None は、デフォルトで設定される特別なロケーションで、無制限の音声およびビデオの帯域幅が割り当てられます。ロケーション Hub_None は削除できません。支店ロケーションにあるデバイスが Hub_None ロケーションに設定されている場合、その支店デバイスが宛先または発信元となっている電話コールはすべて、コール アドミッション制御の対象となりません。

Cisco Unified CallManager では、各ロケーションに対して音声およびビデオの帯域幅プールを定義できます。ロケーションの音声帯域幅とビデオ帯域幅が **Unlimited** に設定されている場合、そのロケーションでは帯域幅を無限に使用できるため、そのロケーションが宛先または発信元となる音声コールとビデオ コールは、Cisco Unified CallManager ではすべて許可されます。帯域幅の値が有限のキロビット / 秒（Kbps）に設定されている場合は、アクティブになっているすべてのコールで使用されている合計帯域幅が、その設定値以下になっている場合に限り、Cisco Unified CallManager は、そのロケーションで入出力されるコールを許可します。ロケーションのビデオ帯域幅を **None** に設定した場合、このロケーションが宛先または発信元となるすべてのビデオ コールは拒否されます。ただし、このロケーションの内部でやり取りされるビデオ コールには影響しません。

ビデオ コールの場合、ビデオ ロケーションの帯域幅については、コールのビデオ部分と音声部分の両方を考慮に入れる必要があります。したがって、ビデオ コールの場合、帯域幅が音声帯域幅プールから差し引かれることは一切ありません。

ロケーションでメンバーシップを指定できるデバイスには、次のものがあります。

- IP Phone
- CTI ポート
- H.323 クライアント
- CTI ルート ポイント
- コンファレンス ブリッジ
- Music On Hold（MoH）サーバ
- ゲートウェイ
- トランク

静的ロケーションのコール アドミッション制御メカニズムでは、通話中のコール タイプ変更も考慮に入れる必要があります。たとえば、サイト間でビデオ コールを確立する場合、Cisco Unified CallManager は、それぞれのロケーションから適切なビデオ帯域幅を差し引きます。このビデオ コールが、ビデオ非対応のデバイスに転送する過程で音声専用コールに変更された場合、Cisco Unified CallManager は割り当てた帯域幅をビデオ プールに戻し、適切な帯域幅を音声プールから割り当てます。音声からビデオに変更されるコールについては、これとは逆の帯域幅割り当て変更が発生します。

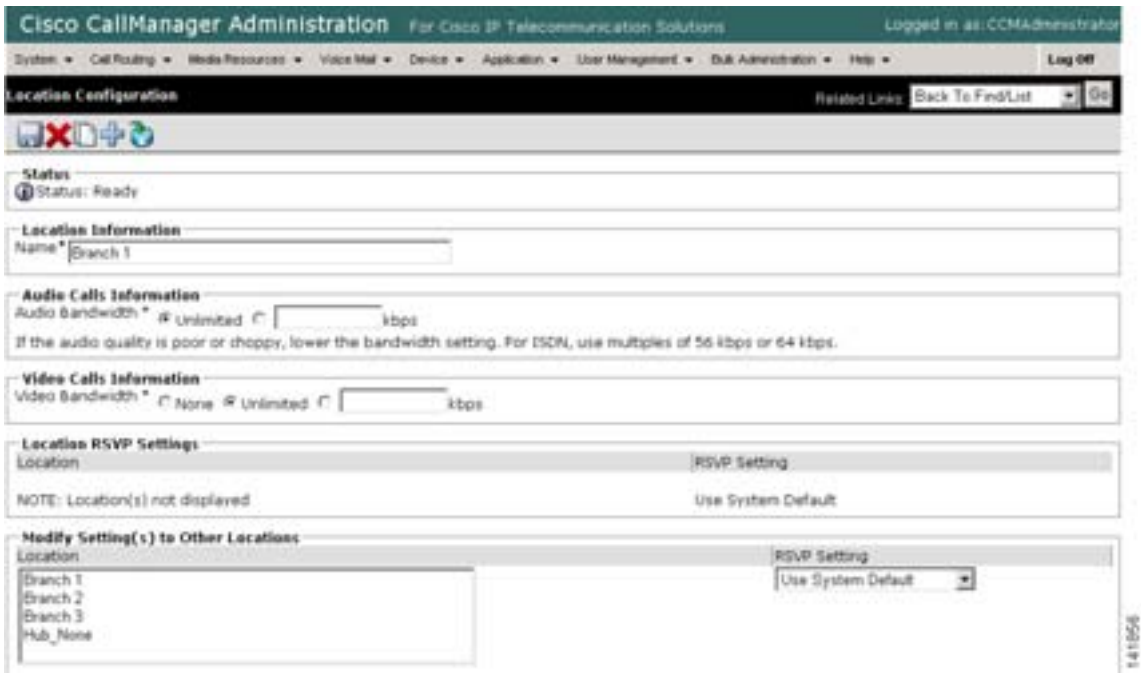
表 9-1 に、さまざまなコールのタイプ（ビットレート）において静的ロケーション アルゴリズムが要求する帯域幅を示します。音声コールでは、Cisco Unified CallManager は、メディア ビット レートにレイヤ 3 オーバーヘッドを加えて計算します。たとえば、G.711 音声コールは、ロケーションの音声帯域幅プールから割り当てられた 80 kbps を消費します。ビデオ コールでは、Cisco Unified CallManager は、音声ストリームとビデオ ストリームの両方に対して、メディア ビット レートだけを計算します。たとえば、384 kbps の速度のビデオ コールに対して、Cisco Unified CallManager はビデオ帯域幅プールから 384 kbps を割り当てます。

表 9-1　静的ロケーション アルゴリズムが要求する帯域幅

コールのタイプ（ビットレート）	静的ロケーションの帯域幅の値
G.711 音声コール（64 Kbps）	80 kbps
G.729 音声コール（8 Kbps）	24 kbps
128 Kbps ビデオ コール	128 kbps
384 Kbps ビデオ コール	384 kbps
512 Kbps ビデオ コール	512 kbps
768 Kbps ビデオ コール	768 kbps

図 9-10 では、使用可能な音声帯域幅 256 Kbps およびビデオ帯域幅 384 Kbps を指定した、ロケーション Branch 1 の設定を示しています。Branch 1 は、最高 3 つの G.711 音声コール（コールごとに 80 Kbps）、または 10 個の G.729 音声コール（コールごとに 24 Kbps）、または両方のコールの組み合せ（256 Kbps を超えないこと）をサポートできます。このロケーションでは、使用されているビデオ コーデックおよび音声コーデックに応じて、さまざまな数のビデオ コールをサポートすることもできます。たとえば、384 kbps の帯域幅を要求する 1 つのビデオ コール、またはそれぞれ 128 kbps の帯域幅を要求する 3 つのビデオ コールをサポートできます。

図 9-10　Cisco Unified CallManager におけるロケーションの定義



コール アドミッション制御は、同じロケーション内のデバイス間のコールには適用されません。

あるロケーションから他のロケーションにコールが発信されると、Cisco Unified CallManager は、両方のロケーションから適切な帯域幅を差し引きます。たとえば、2 つのロケーション間の G.729 コールによって、Cisco Unified CallManager は、両方のロケーションで使用可能な帯域幅から 24 kbps を差し引きます。コールが完了すると、Cisco Unified CallManager は、帯域幅を差し引かれたロケーションに帯域幅を戻します。いずれかの支店ロケーションで十分な帯域幅がない場合、コールは Cisco Unified CallManager によって拒否され、発信者はネットワーク ビジー トーンを受け取ります。発信側デバイスが、ディスプレイを備えた IP Phone である場合、そのデバイスには、「Not Enough Bandwidth」というメッセージも表示されます。

サイト間コールがコール アドミッション制御によって拒否された場合、Cisco Unified CallManager は Automated Alternate Routing（AAR）機能を使用して、公衆網接続を通じて宛先にコールを自動的に再ルーティングできます。AAR 機能の詳細については、P.10-28 の「Automated Alternate Routing」を参照してください。

（注） AAR が呼び出されるのは、帯域幅が不足しているために、ロケーション ベースのコール アドミッション制御によってコールが拒否される場合だけです。IP WAN が使用不可の場合や、接続に関するその他の問題によって着信側デバイスが Cisco Unified CallManager に登録されない状態になった場合には、AAR は呼び出されません。このような場合、コールは着信側デバイスの Call Forward No Answer フィールドで指定されている宛先に転送されます。

Cisco IOS ゲートキーパー ゾーン

Cisco IOS ゲートキーパーは、Cisco Unified CallManager、Cisco Unified CallManager Express、レガシー PBX に接続されている H.323 ゲートウェイなどのデバイス間で、コール ルーティングとコール アドミッション制御を提供できます。H.323 Registration Admission Status（RAS）プロトコルを使用してこれらのデバイスと通信し、コールをネットワークにルーティングします。

ゲートキーパーのコール アドミッション制御は、ポリシーベースの方式であり、使用可能なリソースの静的設定を必要とします。ゲートキーパーは、ネットワーク トポロジを認識しないので、単純なハブアンドスポーク トポロジに制限されます。トポロジの詳細な例については、P.9-38 の「コール アドミッション制御の設計」の項を参照してください。

Cisco 2600、2800、3600、3700、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール アドミッション制御の面を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、P.8-22 の「ゲートキーパーの設計上の考慮事項」を参照してください。コール ルーティングに関する考慮事項については、P.10-42 の「ゲートキーパーを使用する Cisco IOS でのコール ルーティング」を参照してください。

Cisco IOS ゲートキーパーのコール アドミッション制御機能は、ゲートキーパーの「ゾーン」の概念に基づいています。ゾーンは、エンドポイント、ゲートウェイ、マルチポイント コントロール ユニット（MCU）などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。ローカル ゾーンは、当該のゲートキーパーがアクティブに処理しているゾーンです。つまり、このゾーンに割り当てられている H.323 デバイスは、すべて当該ゲートキーパーに登録されます。

複数のゲートキーパーを同一ネットワークに配置している場合、ゾーンがローカル ゾーンとして設定されるのは、1 つのゲートキーパー上のみです。他のゲートキーパーでは、このゾーンはリモート ゾーンとして設定されます。この設定によって、あるゾーンが宛先になっているコールを、そのゾーンを「所有」しているゲートキーパー（つまり、そのゾーンがローカル ゾーンとして設定されているゲートキーパー）に転送するようにゲートキーパーに指示しています。

ゲートキーパーで許可されるコールの数を管理する、つまりコール アドミッション制御機能を利用するには、**bandwidth** コマンドを使用します。このコマンドにはいくつかのオプションがありますが、この機能と密接に関連するのは次のオプションです。

- **interzone** オプションによって、特定のローカル ゾーンで送受信されるすべてのコールの帯域幅の量を制御します。
- **total** オプションによって、特定のローカル ゾーンを宛先または発信元とするすべてのコール、そのローカル ゾーン内のすべてのコールの帯域幅の量を制御します。
- **session** オプションによって、特定のローカル ゾーンのコール 1 件あたりの帯域幅の量を制御します。
- **remote** オプションによって、すべてのリモート ゾーンで送受信される帯域幅の総量を制御します。

すべてのアクティブなコールに対してゲートキーパーによって差し引かれる帯域幅の値は、レイヤ 2、IP、および RTP のオーバーヘッドを除いた、コールのビットレートの倍です。たとえば、64 Kbps を使用する G.711 音声コールは、ゲートキーパーでは 128 Kbps と認識され、384 Kbps のビデオ コールは 768 Kbps と認識されます。表 9-2 に、一般に利用されているいくつかのコールビットレートにおいて、ゲートキーパーが使用する帯域幅の値を示します。

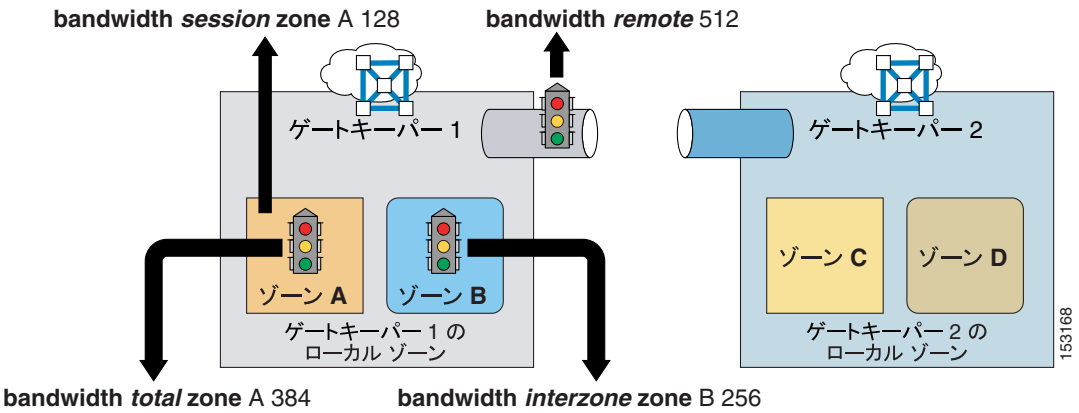
表 9-2　さまざまなコールビットレートにおけるゲートキーパーの帯域幅設定

コールのビットレート	ゲートキーパーの帯域幅の値
G.711 音声コール（64 Kbps）	128 kbps
G.729 音声コール（8 Kbps）	16 kbps
128 Kbps ビデオ コール	256 kbps
384 Kbps ビデオ コール	768 kbps
512 Kbps ビデオ コール	1024 kbps
768 Kbps ビデオ コール	1536 kbps

（注） コール ARQ（アドミッション要求）に対する帯域幅計算には、RTP ヘッダー圧縮（cRTP）やその他のトランスポートのオーバーヘッドは含まれません。インターフェイス キューのプロビジョニング方法の詳細については、P.3-48 の「帯域幅のプロビジョニング」を参照してください。

実際のネットワークでの **bandwidth** コマンドの利用方法を深く理解するために、図 9-11 に示す例について考えます。

図 9-11　Cisco IOS ゲートキーパーの bandwidth コマンドの例



すべてのコールが G.711 コーデックを使用する音声専用コールであるとすると、図 9-11 に示す設定コマンドについて、次のことがいえます。

- 1　回のコールに対してゾーン　A　で任意のデバイスによって要求される帯域幅の最大量は、128 kbps です。つまり、64 kbps よりも高いビットレートのコーデックを使おうとするコールは拒否されます。
- ゾーン A のデバイスに関係するすべてのコール（ゾーン内、またはその他のゾーンとの間）で使用される帯域幅の最大量は、384 kbps です。つまり、ゾーン A のデバイスに関係する最大 3 つのアクティブなコールが存在できます。
- ゾーン　B　のデバイスとその他のゾーンのデバイス間のすべてのコールによって使用される帯域幅の最大量は、256 kbps です。つまり、ゾーン B のデバイスと、ゾーン A、C、および D のデバイスの間には、最大 2 つのアクティブなコールが存在できます。
- ゲートキーパー GK 1 で登録されたデバイスと、その他のゲートキーパーで登録されたデバイスとの間のすべてのコールで使用される帯域幅の最大量は、512 kbps です。つまり、ゾーン A およびゾーン B のデバイスと、ゾーン C および ゾーン D のデバイスの間には、最大 4 つのアクティブなコールが存在できます。

Cisco Unified CallManager の RSVP 対応ロケーション

Cisco Unified CallManager Release 5.0 では、リソース予約プロトコル（RSVP）に基づくトポロジ対応コール アドミッション制御メカニズムが導入されました。このプロトコルは、すべてのネットワーク トポロジに適用可能で、従来のハブアンドスポーク トポロジの制限を緩和します。Cisco RSVP Agent は Cisco IOS の機能であり、Cisco Unified CallManager が RSVP ベースのコール アドミッション制御を実行できるようにするものです。Cisco RSVP Agent 機能は、Cisco IOS Release 12.4（6）T で導入され、Cisco 2600XM、2691、3700 シリーズ、2800 シリーズ、および 3800 シリーズの Integrated Services Routers プラットフォームで使用できます。

Cisco RSVP Agent は、Cisco Unified CallManager で、メディア ターミネーション ポイント（MTP）または RSVP をサポートするトランスコーダ デバイスのいずれかとして登録されます。エンドポイント デバイスが帯域幅の予約を必要としてコールを行う場合、Cisco Unified CallManager は、帯域幅を予約するためのエンドポイントに対するプロキシとして機能する Cisco RSVP Agent を呼び出します。

図 9-12 は、Cisco Unified CallManager とさまざまなその他のデバイス間で使用されるシグナリング プロトコルと、特定のロケーションで WAN を通じたコールのために関連付けられる RTP ストリームを示しています。WAN を通じたすべてのコールで、Cisco Unified CallManager は、ローカル Cisco RSVP Agent にメディア ストリームを送信するようエンドポイント デバイスに指示します。このローカル Cisco RSVP Agent は、リモート ロケーションにある Cisco RSVP Agent への RSVP 予約と同期された別のコール レッグを発信します。図 9-12 は、次のシグナリング プロトコルを示しています。

- Skinny Client Control Protocol（SCCP）による Cisco Unified CallManager への Cisco RSVP Agent の登録
- SCCP または Session Initiation Protocol（SIP）による Cisco Unified CallManager への IP Phone の登録
- Media Gateway Control Protocol（MGCP）、SIP、または H.323 プロトコルによる Cisco Unified CallManager への公衆網ゲートウェイの登録

図 9-12　RSVP をサポートするロケーションのプロトコル フロー

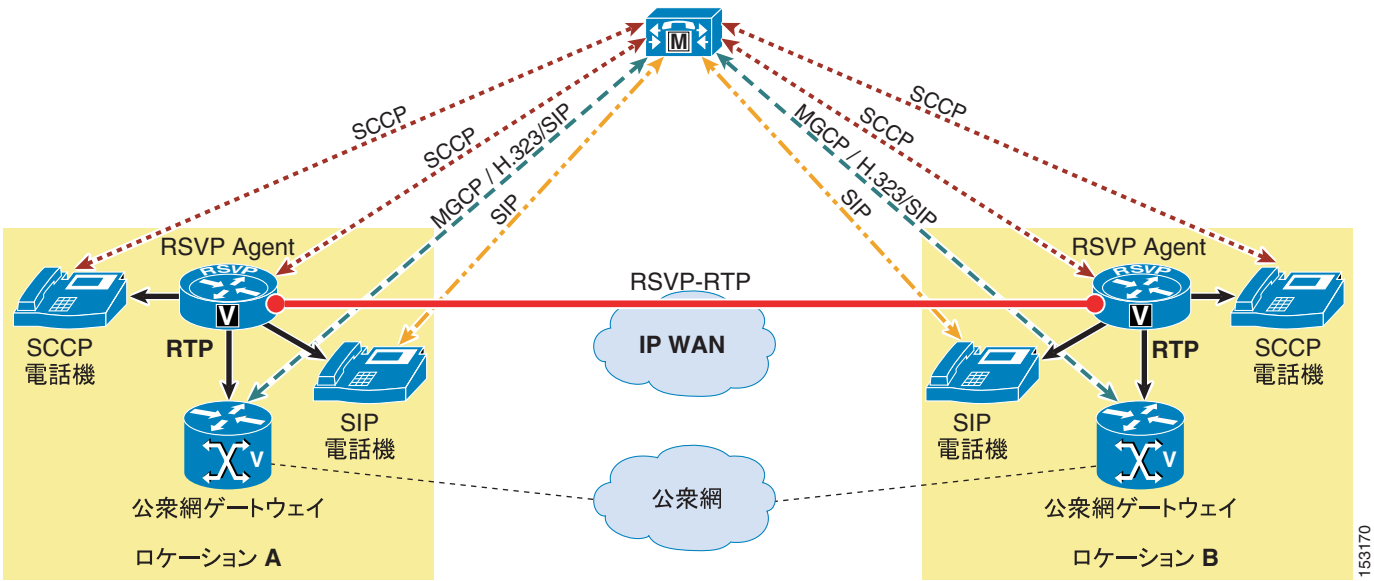
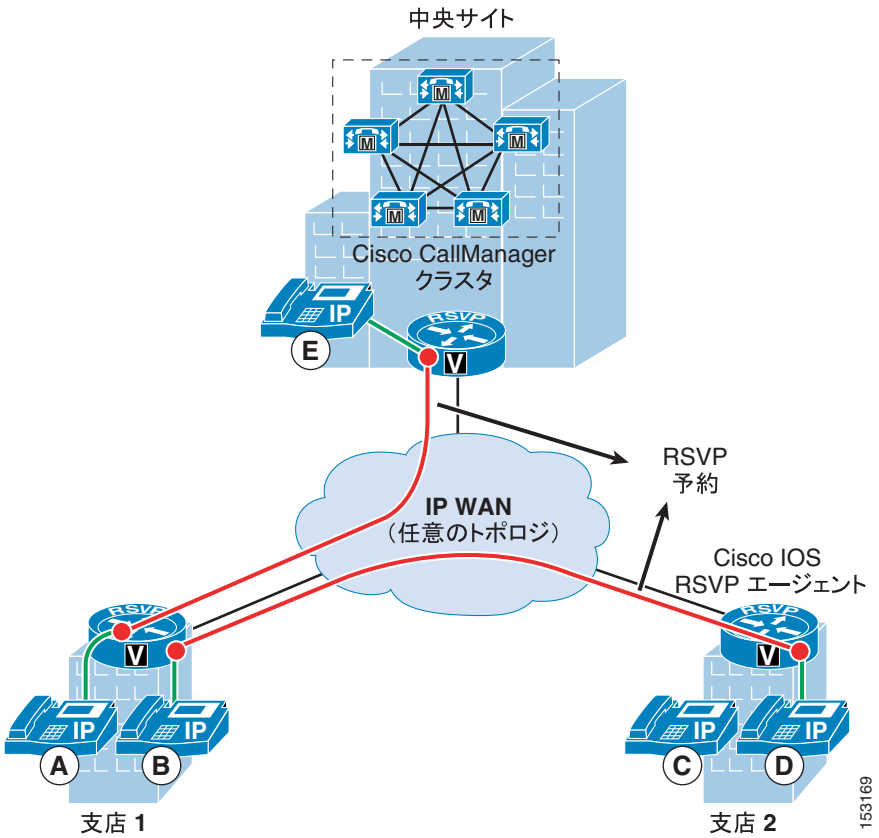


図 9-13 は、Cisco Unified CallManager クラスタ内の代表的な Cisco RSVP Agent 配置を示しています。これには、中央サイト、支店 1、および支店 2 の 3 つのロケーションが含まれます。3 つのロケーションを接続する IP WAN は、任意のトポロジ タイプにすることができ、ハブアンドスポーク トポロジに制限されません。メディア パスで RSVP 予約を必要とする 2 つのロケーション間のコールに対して、Cisco RSVP Agent のペアが、Cisco Unified CallManager から動的に呼び出されます。Cisco RSVP Agent は、Cisco RSVP Agent と同じロケーションにある IP Phone の RSVP 予約を行うためにプロキシとして動作します。たとえば、支店 1 の電話機 A が中央サイトの電話機 E をコールする場合、RSVP 予約が、支店 1 ロケーションと中央サイト ロケーションの Cisco RSVP Agent 間で確立されます（図 9-13 の赤線）。

このコールのメディア ストリームに対しては、3 つのコール レッグがあります。第 1 のコール レッグは電話機 A と支店 1 の Cisco RSVP Agent との間、第 2 のコール レッグは支店 1 と中央サイトの Cisco RSVP Agent との間、第 3 のコール レッグは中央サイトの Cisco RSVP Agent と電話機 E との間です。同様に、支店 1 の電話機 B が、支店 2 の電話機 D をコールした場合、RSVP 予約が支店 1 と支店 2 の Cisco RSVP Agent 間で確立されます。この場合、2 つの支店ロケーション間のコールのメディア ストリームは、中央サイト経由で送信されません。静的ロケーションに基づき、コール アドミッション制御を使用して、従来のハブアンドスポーク トポロジを通じて行われるコールとは異なっています。

（注） RSVP 対応ロケーションおよび Cisco RSVP Agent を使用すると任意の WAN トポロジがサポートされますが、これらはロケーションに対するデバイスの静的な割り当てに基づいています。つまり、ある物理的なサイトから別のサイトにデバイスを移動するたびに、Cisco Unified CallManager の設定を更新する必要があります。

図 9-13　Cisco RSVP Agent の概念



Cisco RSVP Agent のプロビジョニング

Cisco RSVP Agent 機能には、Cisco IOS Release 12.4（6）T および Cisco Unified Survivable Remote Site Telephony ライセンス、または Cisco Multiservice IP-to-IP Gateway ライセンス付きの Integrated Voice and Video Services イメージが必要です。同時コール（セッションとも呼ばれる）に対するその容量は、次の要因によって変化します。

- ソフトウェアベースの MTP 機能では、ルータ プラットフォームおよび相対的な CPU 負荷によってセッション容量が決まる（表 9-3 を参照）。
- ハードウェアベースの MTP およびトランスコーダの機能では、使用可能な DSP の数によってセッション容量が制限される（DSP のサイズ選定の考慮事項については、P.6-1 の「メディア リソース」を参照してください）。

ソフトウェアベースの MTP 機能に関して、表 9-3 は、Cisco RSVP Agent 専用のルータおよび 75% の CPU 利用率を基準としたセッション容量のガイドラインを示しています。これらの数値は、Cisco IOS Release 12.4（6）T に適用されるもので、大まかなガイドラインとみなす必要があります。特定のサービス、設定、トラフィック パターン、ネットワーク トポロジ、ルーティング テーブル、およびその他の要因の異なる組み合せは、特定の配置のパフォーマンスに著しい影響を与え、サポートされる同時セッション数が減少することがあります。実稼働環境でマルチサービス ルータを配置する前に、慎重に計画および検証試験を行うことをお勧めします。

表 9-3　ソフトウェアベースの MTP 機能を備えた Cisco RSVP Agent のセッション容量

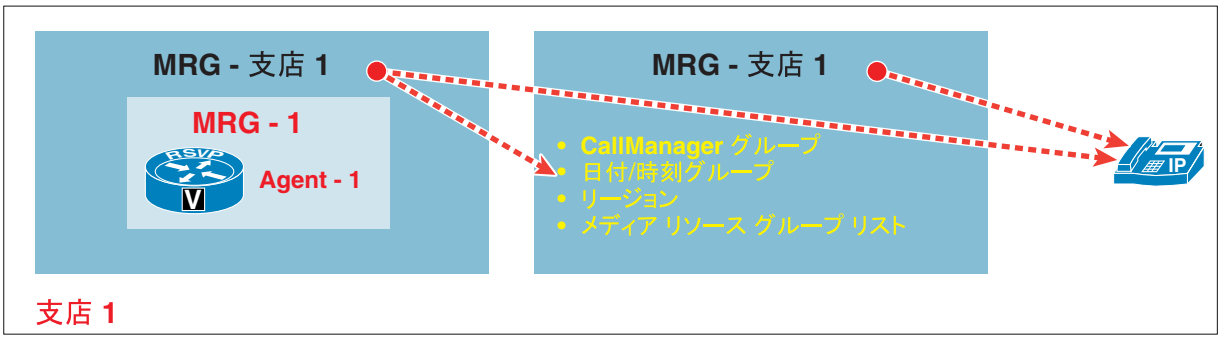
Cisco RSVP Agent プラットフォーム	サポートされるセッション数
2611XM	40
2621XM	50
2651XM	65
2691	150
2801	130
2811	180
2821	240
2851	300
3725	250
3745	320
3825	400
3845	536

（注） Cisco RSVP Agent が Cisco Unified Survivable Remote Site Telephony ライセンスで配置される場合、サポートされるセッション数は（表 9-3 に示すように）ルータのパフォーマンスとライセンス権で決まります。Cisco RSVP Agent が Cisco Multiservice IP-to-IP Gateway ライセンスで配置される場合、サポートされるセッション数はルータのパフォーマンスだけで決まります。

Cisco RSVP Agent は、デバイス プール、メディア リソース グループ（MRG）、およびメディア リソース グループ リスト（MRGL）の設定の組み合せでエンドポイント デバイスに関連付けることができます。Cisco RSVP Agent は MRG に含めることができ、MRG は MRGL の要素になることができます。MRGL は、直接またはデバイス プールを通じてエンドポイント デバイスに割り当てることができます。図 9-14 に示すように、MRGL- 支店 1 は、直接または Device Pool-Branch 1 から IP Phone に関連付けることができます。一般に、エンドポイント デバイスがメディア リソースの一意

のセットを要求する場合は、エンドポイント デバイス MRGL を直接割り当てます。それ以外の場合は、エンドポイント デバイスが配置されているデバイス プールに MRGL を割り当てます。

図 9-14　IP Phone への MRGL の割り当て



Cisco Unified CallManager は、MTP、トランスコーダ、会議リソース、および Annunciator など、その他の従来のメディア リソースを割り当てるのと同じ方法で、Cisco RSVP Agent を割り当てます。

他の従来のメディア リソースと同じ MRG で、Cisco RSVP Agent を設定しないようにしてください。設定すると、コールが RSVP に関係しない場合であっても、MTP デバイスを必要とするコールに Cisco RSVP Agent が割り当てられます。

図 9-15 は、Cisco RSVP Agent ロード バランシングが MRG および MRGL 設定によって実装される様子を示しています。同じ MRG 内のすべての Cisco RSVP Agent に対して、Cisco Unified CallManager は、ラウンドロビン方式で Cisco RSVP Agent に対してロード バランシングおよび割り当てを行います。

図 9-15　Cisco RSVP Agent のロード バランシング

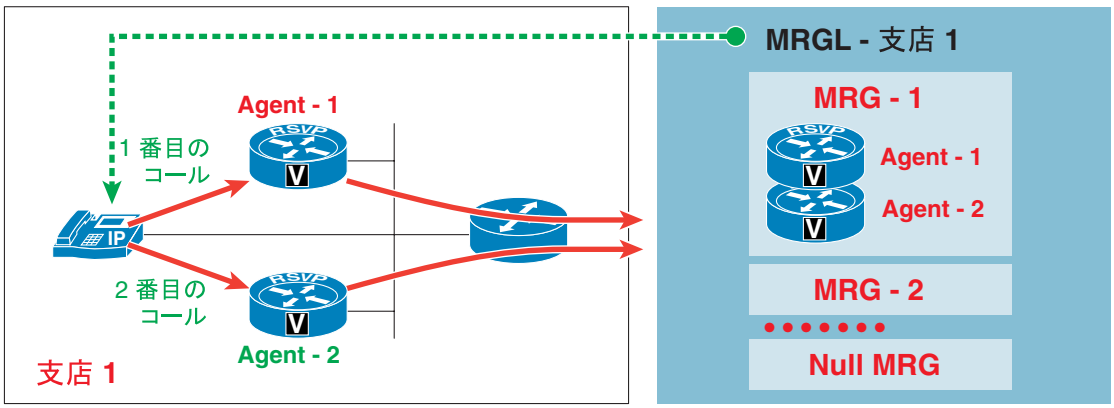


図 9-15 に示すように、MRG-1 の両方の Cisco RSVP Agent が使用可能な場合、最初のコールに対して Agent-1 が選択され、2 番目のコールに対して Agent-2 が選択されます。MRG-1 でいずれの Cisco RSVP Agent も使用できない場合、Cisco Unified CallManager はコールに適した Cisco RSVP Agent が見つかるまで、MRG-2、MRG-3、および残りの MRG の検索を試行します。MRG に明示的に含まれていない Cisco RSVP Agent は、デフォルトで Null MRG に含まれています。Null MRG は常に

MRGL 設定の最後の MRG として黙示的に含まれていますが、Cisco Unified CallManager Administration には表示されません。Null MRG の Cisco RSVP Agent は、Cisco Unified CallManager クラスタの任意のエンドポイント デバイスからアクセスできます。したがって、常に MRG で Cisco RSVP Agent を設定することをお勧めします。Cisco Unified CallManager のメディア リソース割り当てプロセスおよび関連するベスト プラクティスの詳細については、P.6-1 の「メディア リソース」を参照してください。

Cisco RSVP Agent の登録

Cisco RSVP Agent は、RSVP をサポートする MTP またはトランスコーダ デバイスとして、Cisco Unified CallManager に登録されます。Cisco RSVP Agent は、MTP デバイスとして登録する場合、トランスコーディング機能をサポートしません。トランスコーディング機能をサポートするには、Cisco RSVP Agent をトランスコーダ デバイスとして Cisco Unified CallManager に登録する必要があります。

登録のスイッチオーバーとスイッチバック

プライマリ Cisco Unified CallManager に障害が発生した場合、Cisco RSVP Agent はセカンダリ Cisco Unified CallManager にスイッチオーバーします。プライマリ Cisco Unified CallManager が障害から回復すると、Cisco RSVP Agent はプライマリ Cisco Unified CallManager に登録をスイッチバックします。Cisco RSVP Agent 登録のスイッチオーバーとスイッチバックを設定するには、次のコマンドを使用します。

```
sccp ccm group
 switchover method immediate
 switchback method guard timeout 7200
!
gateway
  timer receive-rtp 180
```

- **switchover method immediate** は、プライマリ Cisco Unified CallManager サーバの障害が検出されたら、すぐにセカンダリ Cisco Unified CallManager サーバに登録をスイッチオーバーすることを指定します。使用可能な DSP リソースは、スイッチオーバーが完了するとすぐに、新しいコールで利用できるようになります。
- **switchback method guard timeout 7200** コマンドは、プライマリ Cisco Unified CallManager が障害から回復した後の登録のスイッチバック メカニズムを指定します。このコマンドを設定すると、Cisco RSVP Agent は最後のアクティブなコールの切断後に、プライマリ Cisco Unified CallManager への登録の正常なスイッチバックを開始します。保護タイマーの期限内に登録の正常なスイッチバックが開始されない場合、Cisco RSVP Agent は即時のスイッチバック メカニズムを使用してすぐに Cisco Unified CallManager に登録します。保護タイマーのデフォルト値は 7200 秒で、60 ～ 172800 秒の範囲で静的に設定できます。
- ゲートウェイ設定モードでの **timer receiver-rtp** コマンドは、RSVP 予約のための RTP クリーンアップ タイマーを定義します。障害が発生した場合、既存のコール用の RSVP 予約は、RTP クリーンアップ タイマーの期限が切れるまで有効です。このタイマーのデフォルト値は、1200 秒です。このタイマーは可能な最小値である 180 秒に設定することをお勧めします。

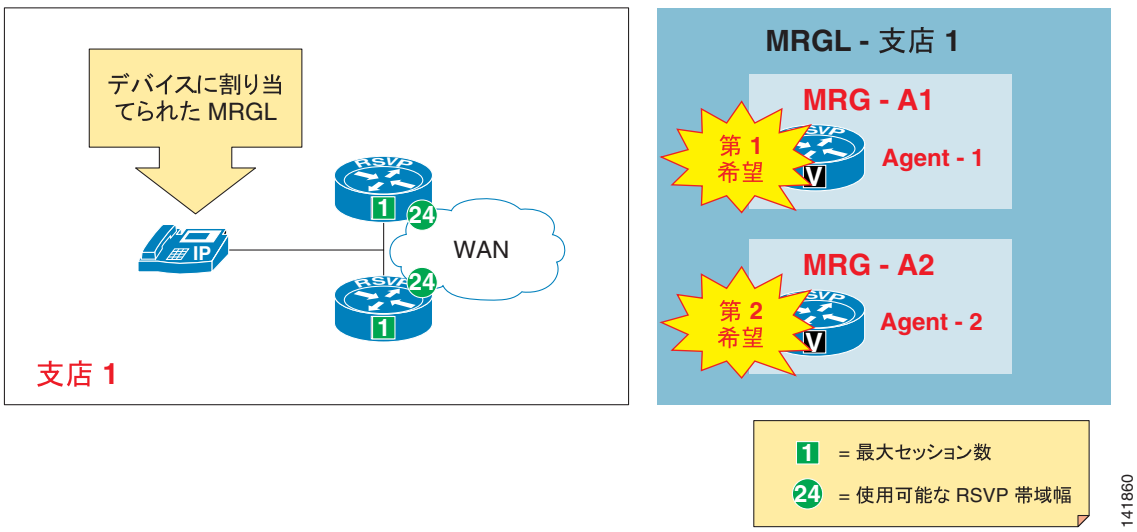
最大セッション サポート

Cisco RSVP Agent は、Cisco RSVP Agent ルータに搭載されるソフトウェアベースのリソース（CPU）とハードウェアベースのリソース（DSP）に基づく、コールまたはセッションの最大数をサポートしています。**dspfarm profile** 設定モードの **maximum sessions** コマンドは、Cisco RSVP Agent が処理できるコールの最大数を指定します。Cisco RSVP Agent は、この設定に基づいてセッション容量を Cisco Unified CallManager に通知します。セッションの最大数は、コールが Cisco RSVP Agent を通過するごとに 1 つずつ減少します。カウンタが 0 になると、Cisco RSVP Agent には使用可能なリソースがないと見なされ、Cisco Unified CallManager はそれ以降のコールでその Cisco RSVP Agent をスキップします。

図 9-16 は、2 つの Cisco RSVP Agent がある支店サイトを示しています。Cisco RSVP Agent は WAN ルータと共存し、Cisco RSVP Agent の冗長性は、同じ MRGL の別の MRG に 2 つの Cisco RSVP Agent を割り当てることによって実現されます。MRG-1 の Agent-1 が使用できないか、セッション容量を超えている場合、Cisco Unified CallManager は支店 1 を宛先または発信元とする RSVP コールのために、MRG-2 に Agent-2 を割り当てようとします。Agent-1 の容量に達したときに Agent-2 が選択されるようにするには、Cisco RSVP Agent の WAN インターフェイスで設定する **ip rsvp bandwidth** でサポートされるコール数と正確に一致するセッションの最大数を設定することをお勧めします。この例では、両方の Cisco RSVP Agent を **maximum sessions 1** に設定する必要があります。この推奨事項は、WAN を経由するすべてのコールが同じタイプのコーデックを使用し、WAN 経由のコール数を正確に計算できることを前提としています。このコール数は、使用可能な RSVP 帯域幅をコールごとに必要な帯域幅で割ることによって計算します。

（注） セッションの最大数が **ip rsvp bandwidth** 設定でサポートされるコール数よりも大きい場合でも、Cisco Unified CallManager はそのコールを Cisco RSVP Agent に送りますが、使用可能な帯域幅がないため RSVP 予約は失敗します。Cisco Unified CallManager は、コール アドミッション制御失敗の通常の処理に従います（コールを拒否するか、AAR 機能を呼び出します）。

図 9-16　Cisco RSVP Agent での最大セッションの設定



パススルー コーデック

パススルー コーデックを使用すると、Cisco IOS Enhanced MTP デバイスは、ストリームのメディア エンコーディングを認識していなくても、エンドポイントから受信した RTP メディア ストリームを終端することができます。つまり、メディア ストリームの UDP パケットは、デコードされずに MTP を通過します。この方法により、MTP は、Cisco Unified CallManager で定義されるすべての音声、ビデオ、およびデータのコーデックをサポートできます。MTP はメディア ストリームをデコードしないため、パススルー コーデックは暗号化（SRTP）メディア ストリームでも使用できます。実際にビデオおよび SRTP メディア ストリームが MTP を使用するには、パススルー コーデックをサポートする必要があります。パススルー コーデックで設定した場合、Cisco RSVP Agent はパケットの IP/UDP ヘッダーのソース IP アドレスを独自の IP アドレスで置き換えて、パケットを通過させます。

Cisco RSVP Agent は、次のすべての条件が満たされる場合にだけ、パススルー コーデックを使用します。

- コールに関与する 2 つのエンドポイント デバイスの音声コーデック能力が一致し、リージョン設定により同一のコーデックの使用がコールに対して許可されている。つまり、コールにトランスコーダ デバイスを挿入する必要はありません。
- **MTP Required** が、いずれのエンドポイント デバイスに対しても設定されていない。
- すべての中間リソース デバイスが、パススルー コーデックをサポートしている。

（注） Cisco RSVP Agent が MTP デバイスとして登録され、トランスコーダ デバイスをコールに挿入する必要がある場合、Cisco RSVP Agent の dspfarm MTP プロファイルで設定されるコーデックは、Cisco Unified CallManager Administration で設定されるリージョン間コーデックと一致している必要があります。たとえば、G.729 コーデックが Cisco Unified CallManager Administration で設定されるリージョン間コーデックの場合は、dspfarm MTP プロファイルでも G.729 コーデックを設定する必要があります。

次の例は、Cisco 2800 IOS プラットフォーム上の Cisco RSVP Agent 設定を示しています。

```
interface Loopback0
 ip address 10.11.1.100 255.255.255.255
!
sccp local Loopback0
sccp ccm 20.11.1.50 identifier 1 priority 1 version 5.0.1
sccp ccm 20.11.1.51 identifier 2 priority 2 version 5.0.1
sccp
!
sccp ccm group 1
 associate ccm 1 priority 1
 associate ccm 2 priority 2
 associate profile 1 register RSVPAgent
 switchover method immediate
 switchback method guard timeout 7200
!
dspfarm profile 1 mtp
 codec pass-through
 codec g729ar8
 rsvp
 maximum sessions software 100
 associate application SCCP
```

RSVP ポリシー

Cisco Unified CallManager は、ロケーション ペアごとに異なる RSVP ポリシーを適用できます。RSVP ポリシーは、Cisco Unified CallManager Administration で設定できます。RSVP ポリシーでは、RSVP 予約試行が失敗した場合に、Cisco Unified CallManager がコールを許可するかどうかが定義されます。次の RSVP ポリシー設定は、任意の 2 つのロケーション間で設定できます。

- No Reservation

  RSVP 予約試行は行われず、静的ロケーション コール アドミッション制御だけが、Cisco Unified CallManager で実行されます。

- Mandatory

  Cisco Unified CallManager は、音声ストリームに対する（コールがビデオ コールの場合はビデオ ストリームに対する）RSVP 予約が成功するまで、終端エンドポイント デバイスを呼び出しません。

- Mandatory (Video Desired)

  ビデオ ストリームの予約はできないが、音声ストリームの予約に成功した場合、ビデオ コールは音声専用コールとして処理できます。

- Optional (Video Desired)

  音声ストリームとビデオ ストリームの両方に対して予約が得られなかった場合、コールはベストエフォートの音声専用コールとして処理できます。Cisco RSVP Agent は、ベストエフォートとしてメディア パケットを再マーキングします。

- Use System Default

  ロケーション ペアの RSVP ポリシーが、クラスタ全体の RSVP ポリシーと一致します。デフォルトのクラスタ全体の RSVP ポリシーは、No Reservation です。Cisco Unified CallManager Administration でデフォルトの RSVP ポリシーを変更するには、**System** > **Service Parameters** > **Cisco Unified CallManager Service** >**Default Inter-location RSVP Policy** を選択します。

（注） Optional (video desired) ポリシーでは、RSVP 予約が失敗しただけでなく、Cisco RSVP Agent も使用できない場合にだけ、IP WAN コールをベストエフォートとして処理できます。この場合、Cisco Unified CallManager は、ベストエフォートとしてトラフィックを再マーキングするように SCCP デバイスおよび MGCP デバイスに指示します。しかし、H.323 デバイスと SIP デバイスではこの再マーキングを行うことができないため、デフォルトの QoS マーキングでトラフィックの送信が続けられます。後者の場合にプライオリティ キューのオーバーサブスクリプションを防ぐため、IP WAN ルータで Access Control List（ACL; アクセス コントロール リスト）を設定し、ソース IP アドレスが Cisco RSVP Agent のアドレスの場合に、DSCP EF または AF41 とマークされたパケットだけを許可することをお勧めします。

図 9-17 では、クラスタ全体の RSVP パラメータのデフォルト設定と推奨設定の両方を示しています。RSVP ポリシーは、**Mandatory** または **Mandatory (Video Desired)** に設定することをお勧めします。これらの設定では、帯域幅の予約とコールの音声品質が保証されます。クラスタ全体の RSVP ポリシーを設定するための最も効率的な方法としては、Cisco CallManager Service Service Parameter Configuration のクラスタ全体の RSVP パラメータに **Default Inter-location RSVP Policy** を設定し、ロケーション設定の RSVP 設定を **Use System Default** のままにします。

図 9-17　クラスタ全体の RSVP パラメータの設定

クラスタ全体の RSVP パラメータ設定には、**Mandatory RSVP mid call error handle option** という名前のサービス パラメータがあります。RSVP ポリシーを **Mandatory** または **Mandatory (Video Desired)** に設定した場合、このパラメータは Cisco Unified CallManager がコール中の RSVP 予約試行の失敗に基づいて既存の RSVP を処理する方法を指定します。コール中の RSVP 予約試行は、WAN の障害後にネットワークのコンバージェンスや、既存の音声専用コールがビデオ コールになることなどでトリガーされることがあります。ネットワークのコンバージェンスでは、Cisco RSVP Agent は、新たにコンバージされたパスを通じてメディア ストリームの送信が開始されるだけでなく、新しいパスを通じて新しい RSVP 予約も試行されます。

Mandatory RSVP mid call error handle option のデフォルト設定は、**Call Becomes Best Effort** です。デフォルト オプションの設定では、Cisco Unified CallManager はコール中の RSVP 予約試行が失敗しても既存のコールを保持しますが、RTP ストリームはベストエフォートとしてマークされます（DSCP 0）。このパラメータは、**Call Fails Following Retry Counter Exceeded** オプション付きで設定することをお勧めします。このオプションを設定すると、Cisco Unified CallManager は RSVP 予約試行が一定の試行回数を超えて失敗し続けた場合に、コールを切断します。再試行カウンタのデフォルト値は 1 です。これは **RSVP Mandatory mid-call retry counter** サービス パラメータで定義され、**RSVP retry timer** のデフォルト値は 60 秒です。再試行カウンタと再試行タイマーの両方のサービス パラメータを、デフォルト値で設定することをお勧めします。両方のパラメータをデフォルト値に設定すると、Cisco Unified CallManager はコール中の RSVP 再試行が失敗した場合に、60 秒待機してからそのコールを切断します。この 60 秒間は、RSVP 予約が存在せず、RTP ストリームはベストエフォートとしてマーキングされるため、音声品質が低下することがあります。

静的ロケーションから RSVP コール アドミッション制御への移行

この項の例では、従来の静的ロケーション コール アドミッション制御から RSVP ベースのコール アドミッション制御メカニズムに移行するためのベスト プラクティスを示します。

図 9-18 では、静的ロケーション コール アドミッション制御メカニズムによるコール処理の集中型配置を示しています。Hub_None ロケーションや 3 箇所の支店など、Cisco Unified CallManager クラスタには 4 つのロケーションがあります。説明を簡単にするために、この例で使用する帯域幅は音声ストリームの帯域幅だけを示しています。表 9-4 と表 9-5 は、256 kbps の帯域幅で静的にプロビジョニングされるすべての支店ロケーションと、**Unlimited** の帯域幅でプロビジョニングされる Hub_None ロケーションを示しています。ロケーションの任意のペア間の RSVP 設定は **Use System Default** で設定され、クラスタ全体の RSVP 設定はデフォルト値 **No Reservation** で設定されます。

図 9-18　静的ロケーションでのコール アドミッション制御の設定

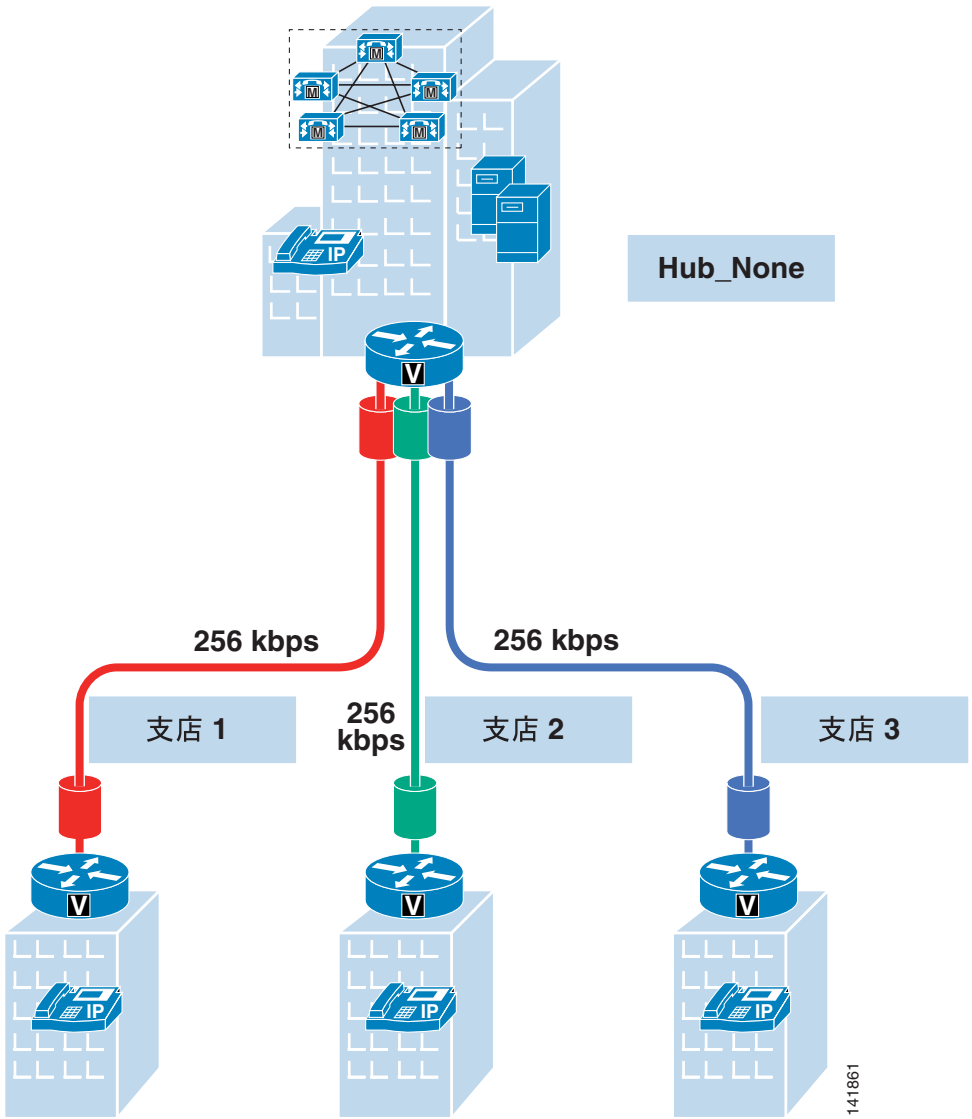


表 9-4　図 9-18 の例でのロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	256 kbps
支店 2	256 kbps
支店 3	256 kbps

表 9-5　図 9-18 の例での RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	No Reservation

RSVP ベースのコール アドミッション制御に移行するには、ロケーションを一度に 1 つずつ移行することをお勧めします。たとえば、支店 1 が最初に移行するロケーションの場合は、次の手順に従います。

- 支店 1 ロケーションで Cisco RSVP Agent を設定し、支店 1 の MRG および MRGL に割り当てて、支店 1 の IP Phone に関連付けます。
- Hub_None ロケーションで別の Cisco RSVP Agent を設定し、Hub_None ロケーションを含む残りの 3 つのロケーションのすべての IP Phone に関連付けられた MRG および MRGL に、Cisco RSVP Agent を含めます。Cisco RSVP Agent を、Null MRG または支店 1 MRG に含めないでください。含めると、支店 1 の IP Phone が Hub_None ロケーションで Cisco RSVP Agent を使用して、RSVP 予約を行う可能性があります。
- 支店 1 の帯域幅を **Unlimited** に設定します。
- 支店 1 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。たとえば、支店 1 と支店 2 の IP Phone 間のコールに対して、音声ストリームは Hub_None ロケーションを通じたヘアピンのままになります。支店 1 ロケーションと Hub_None ロケーション間の最初のコール レッグに対して、RSVP 予約は、支店 1 と Hub_None の Cisco RSVP Agent 間に行われます。Hub_None ロケーションと支店 2 ロケーション間の 2 番目のコール レッグに対して、Cisco Unified CallManager は、支店 2 ロケーションの帯域幅の可用性をチェックすることにより、静的ロケーションに基づくコール アドミッション制御を実行します。

表9-6 と表9-7 は、支店 1 での移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。

表 9-6　支店 1 への移行後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	256 kbps
支店 3	256 kbps

表 9-7　支店 1 への移行後の RSVP ポリシー

ロケーション ペア		ポリシー
支店 1	任意	Mandatory
その他すべてのロケーション	その他すべてのロケーション	No Reservation

表 9-8 と表 9-9 は、クラスタ全体の移行後のロケーションの帯域幅と RSVP ポリシー設定を示しています。クラスタ全体の移行が完了すると、サイト間のコールでは 2 つの Cisco RSVP Agent 間で RSVP 予約を直接行う必要があり、音声ストリームは帯域幅予約パスを通じて転送されます。

次の手順を使用すると、支店 2 および支店 3 を RSVP コール アドミッション制御に移行できます。

- 支店 2 ロケーションで Cisco RSVP Agent を設定し、支店 2 の IP Phone に関連付けられた支店 2 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 2 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 2 の MRG から削除してください。
- 支店 2 の帯域幅を **Unlimited** に設定します。
- 支店 2 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。
- 支店 3 ロケーションで Cisco RSVP Agent を設定し、支店 3 の IP Phone に関連付けられた支店 3 の MRG および MRGL に割り当てます。Hub_None ロケーションの Cisco RSVP Agent が支店 3 の IP Phone からアクセスされなくなるように、Hub_None ロケーションの Cisco RSVP Agent を支店 3 の MRG から削除してください。
- 支店 3 の帯域幅を **Unlimited** に設定します。

- 支店 3 とその他の任意のロケーション間の RSVP 設定を **Mandatory** に設定します。

表 9-8　移行の完了後のロケーションと帯域幅の設定

ロケーション名	帯域幅
Hub_None	Unlimited
支店 1	Unlimited
支店 2	Unlimited
支店 3	Unlimited

表 9-9　移行完了後の RSVP ポリシー

ロケーション ペア		ポリシー
任意	任意	Mandatory

RSVP アプリケーション ID

RSVP アプリケーション ID は、Cisco Unified CallManager が音声トラフィックとビデオ トラフィックの両方に識別子を追加できるようにするメカニズムです。これにより、Cisco RSVP Agent は、受け取った識別子に基づいていずれかのトラフィックに個別の帯域幅制限を設定できます。ネットワークに RSVP アプリケーション ID を配置するには、Cisco RSVP Agent ルータおよび Cisco Unified CallManager Release 5.0 で、Cisco IOS Release 12.4（6）T 以降を使用する必要があります。RSVP アプリケーション ID 文字列は、クラスタ全体の RSVP パラメータ設定の 2 つのサービス パラメータ（**RSVP Audio Application ID** と **RSVP Video Application ID**）で設定できます。

Cisco Unified CallManager は SCCP を使用して、RSVP アプリケーション ID を Cisco RSVP Agent に伝達します。Cisco RSVP Agent も、RSVP シグナリング メッセージ（RSVP Path メッセージや Resv メッセージなど）に RSVP アプリケーション ID を挿入し、ダウンストリームまたはアップストリームの RSVP ルータにこれらのメッセージを送信します。

RSVP アプリケーション ID は、静的ロケーション モデルとは異なるモデルを使用して、音声トラフィックおよびビデオ トラフィックの帯域幅を分離します。静的ロケーションでは、ビデオ コールの音声ストリームとビデオ ストリームはどちらもビデオ帯域幅カウンタから差し引かれます。RSVP アプリケーション ID を使用する場合、音声ストリームは音声帯域幅プールから差し引かれ、ビデオ ストリームはビデオ帯域幅プールから差し引かれます。コール アドミッション制御モデルのこの変更により、音声コール用に一定の帯域幅を予約し、プライオリティ キューで使用可能なすべての帯域幅を使用できるようになりました。このため、ビデオ コールが行われていない場合に、音声コール用にすべての使用可能な帯域幅を使用できます。プライオリティ キューに使用可能な帯域幅が十分にある場合、オプションとしてビデオ用のコールを有効にできます。ビデオ対応コールが消費できる帯域幅の量に制限を設定できますが、音声コールが使用可能なすべての帯域幅を消費している場合は、ビデオ コールを発信できないことがあります。RSVP アプリケーション ID、RSVP ポリシー、および LLQ の設定方法の詳細については、P.3-45 の「RSVP のアプリケーション ID」を参照してください。

RSVP 機能のある Cisco IOS Gatekeeper および IP-to-IP ゲートウェイ

シスコのマルチサービス IP-to-IP ゲートウェイ（IP-IP ゲートウェイまたは IPIPGW とも呼ばれます）を使用すると、Cisco Unified CallManager クラスタ間、H.323 ゲートウェイ間、またはこれらの 2 者間の IP WAN 接続に関して、ハブアンドスポーク トポロジにおける制約を緩和できます。

Cisco IOS 機能が、IP ネットワーク間で H.323 Voice over IP（VoIP）コールおよびビデオ会議コールを使用するためのメカニズムを提供します。IP-IP ゲートウェイの主な目的は、管理ドメインを通過する VoIP コールとビデオ コールにコントロール ポイントと境界を提供することです。このゲートウェイは、PSTN-to-IP ゲートウェイとほぼ同じ機能を実行しますが、公衆網レッグと IP コール レッグの代わりに、通常は 2 つの IP コール レッグに加入します。

企業の IP Communications 環境において、IP-IP ゲートウェイが備える最も興味深い機能は、このゲートウェイを通過する各コールのための RSVP 予約を生成できることです。P.9-8 の「トポロジ対応コール アドミッション制御」の項で説明しているように、RSVP は、トポロジ対応型のコール アドミッション制御メカニズムを提供するためのネットワーク ベース シグナリング プロトコルです。トポロジがハブアンドスポークである必要はなく、任意のネットワーク トポロジで機能します。

結果として、コール フローに 2 つの IP-IP ゲートウェイを挿入し、両者間で RSVP を有効にすることで、任意の IP WAN トポロジ上でコール アドミッション制御を実行できます。図 9-19 に、2 つのサイト A と B による基本的な例を示します。それぞれ Cisco Unified CallManager クラスタがあり、任意のトポロジを持つ IP WAN を通じて接続されています。各サイトには IP-IP ゲートウェイも配置されており、2 つの Cisco Unified CallManager クラスタは、すべてのサイト間コールを、ローカル IP-IP ゲートウェイを指しているトランクを通じてルーティングするように設定されています。サイト A とサイト B の間でコールがセットアップされると、次のイベントが発生します。

- サイト A の Cisco Unified CallManager が、サイト A の IP-IP ゲートウェイに向かう H.323 トランク（図中のコール レッグ 1）を通じてコールをセットアップします。
- サイト A の IP-IP ゲートウェイが、サイト B の IP-IP ゲートウェイに向かう別のコールを確立しようとしますが、まず RSVP を使用して、IP WAN パスに沿って帯域幅リソースを確保します。
- RSVP 予約が成功すると、2 つの IP-IP ゲートウェイ間にコール レッグ 2 が確立されます。
- サイト B の IP-IP ゲートウェイが、サイト B の Cisco Unified CallManager クラスタに向かう別のコール（図中のコール レッグ 3）を生成します。

図 9-19　RSVP コール アドミッション制御のための IP-to-IP ゲートウェイの簡単な例

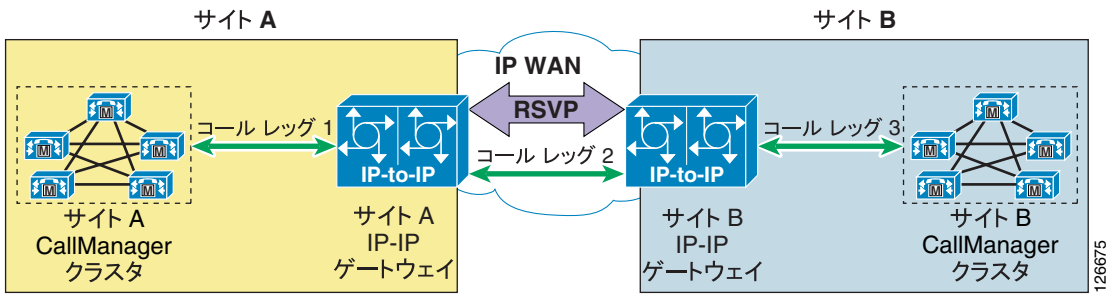


図 9-19 の例は、Cisco Unified CallManager クラスタ間のすべてのコールが、IP-IP ゲートウェイ ペアを通じてルーティングされる単純なシナリオです。しかし、多くの実稼働環境では、このアプローチは十分にスケーラブルで柔軟なものとは言えません。このような場合は、Cisco IOS ゲートキーパーを使用することで、Cisco Unified CallManager クラスタ、H.323 ゲートウェイ、H.323 ビデオ会議エンドポイント、IP-IP ゲートウェイの間に幅広い通信オプションを配置できるようになります。

(注)　この項で説明した IP-IP ゲートウェイ関係のシナリオは、すべて複数の Cisco Unified CallManager クラスタ間のコールに関するものです。同じ Cisco Unified CallManager クラスタに登録されているエンドポイント間で、コールに IP-IP ゲートウェイを挿入することはお勧めしません。同じ Cisco Unified CallManager クラスタに登録されているエンドポイント間の RSVP ベースのコール アドミッション制御については、P.9-18 の「Cisco Unified CallManager の RSVP 対応ロケーション」を参照してください。

中継ゾーン（Via-Zone）ゲートキーパー

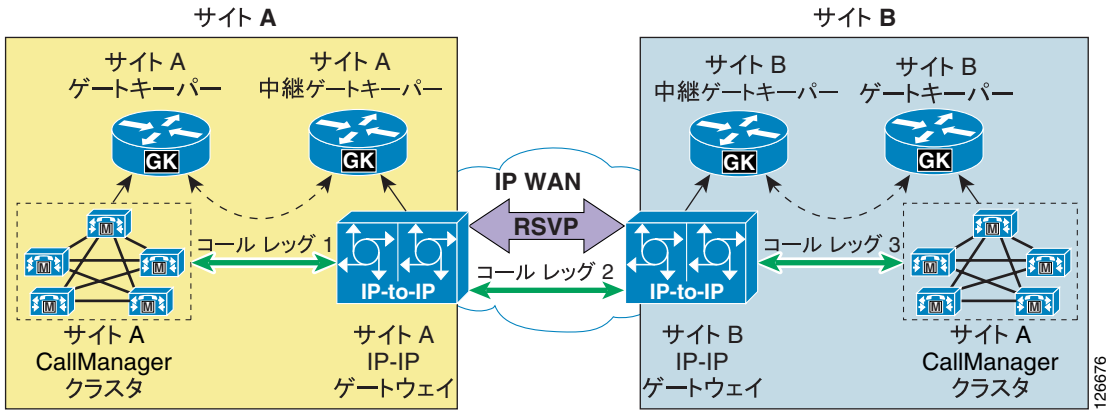
従来の Cisco IOS ゲートキーパー機能は、「中継ゾーン」ゲートキーパーという概念を通じて、IP-IP ゲートウェイに対応するように拡張されました。中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のゲートキーパー機能を維持したまま、追加機能によって拡張されます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれているかどうかを確認します。設定にこれらのキーワードが含まれている場合、ゲートキーパーは新しい中継ゾーン処理を使用します。含まれていない場合は、従来の処理を使用します。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの IP-IP ゲートウェイがポイントされている ACF が返され、コールは IP-IP ゲートウェイに転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求をリモート ゾーンのゲートキーパーではなく outvia ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

図 9-20 に、IP-IP ゲートウェイと中継ゾーン ゲートキーパーを Cisco Unified CallManager クラスタおよびレガシー ゲートキーパーと連携するように使用して、コール ルーティングとコール アドミッション制御を提供する方法の例を示します。このシナリオには、次の考慮事項が適用されます。

- サイト A の Cisco Unified CallManager クラスタは、サイト A のゲートキーパーを使用して、コールをクラスタ間で直接ルーティングする。
- サイト A のゲートキーパーは、サイト B の E.164 番号に転送されるすべてのコールを、サイト A の中継ゾーン ゲートキーパーに送信する。
- サイト A の中継ゾーン ゲートキーパーは、サイト A のゲートキーパーを発信元または宛先とするすべてのコールに対して、IP-IP ゲートウェイを挿入する。
- サイト A の IP-IP ゲートウェイは、コールをサイト B の IP-IP ゲートウェイに送信する前に、RSVP 予約を試行する。
- サイト B の Cisco Unified CallManager クラスタ、ゲートキーパー、および IP-IP ゲートウェイは、サイト A のそれぞれと同様の方法で設定されている。

図 9-20　中継ゾーン ゲートキーパーを使用した RSVP のための IP-to-IP ゲートウェイ



設計上のベスト プラクティス

IP-IP ゲートウェイを Cisco Unified CallManager と連携するように配置して、IP WAN で RSVP コール アドミッション制御を使用できるようにする場合は、次に示す設計上のベスト プラクティスに従ってください。

- 1 つ以上の IP-IP ゲートウェイを通じて、他の Cisco Unified CallManager クラスタとの音声通信またはビデオ通信用に Cisco Unified CallManager のトランクを設定する場合は、ゲートキーパー制御 H.225 トランクを使用します。Cisco IOS Release 12.4（6）T 以降および Cisco Unified CallManager Release 4.1 以降を使用すると、IP-IP ゲートウェイを通じた保留と保留解除、転送、会議などの補足サービスを呼び出すための MTP リソースが不要になります。相互運用性を確保するには、次の項目を設定する必要があります。
  - Cisco Unified CallManager Administration のトランク設定ページで、**Media Termination Point required** フィールドをオフ（デフォルト設定）のままにして、**Wait for Far End H.245 Terminal Capability Set** フィールドもオフにします。
  - Cisco Unified CallManager Administration の Cisco Unified CallManager に関する Advanced Service Parameters ページで、**Send H225 User Info Message** フィールドを **H225 Info For Call Progress Tone** に設定します。
  - 補足サービスを呼び出す場合に Cisco Unified CallManager との相互運用性を確保するには、IP-IP ゲートウェイで次の Cisco IOS コマンドを設定します。

```
voice service voip
   h323
       emptycapability
       h245 passthru tcsnonstd-passthru
```

- 一部の配置では、プロキシ機能を提供し、エンドポイント デバイスに代わってシグナリング ストリームおよびメディア ストリームを終端させるために、MTP リソースが優先されます。MTP リソースが必要な場合は、クラスタ間トランクを介してコールするときに IP WAN 帯域幅の使用が増大するのを避けるために、IP-IP ゲートウェイと同じサイトに MTP リソースを配置することをお勧めします。これらの MTP リソースは、ソフトウェア ベース（Cisco MCS サーバや Cisco IOS ルータなど）でも、ハードウェア ベース（Cisco コミュニケーション メディア モジュールを備えた Catalyst 6500 や、NM-HDV ネットワーク モジュールを備えた Cisco IOS ルータなど）でもかまいません。使用できる MTP リソースの完全なリストについては、P.6-1 の「メディア リソース」の章を参照してください。ただし、MTP を使用すると、コールが持続しているすべての期間にわたって、メディア パケットは最初の MTP リソースを通じて転送されます。以後にコール転送が発生した場合は、ヘアピンが発生する可能性があります。**Media Termination Point required** オプションが H.225 トランクでオフになっている場合、ビデオ コールは IP-IP ゲートウェイを通じてクラスタ間で確立されないことに注意してください（MTP はビデオ コールをサポートしていないため）。

- すべてのクラスタ間コールで IP-IP ゲートウェイを使用する場合にだけ、Cisco Unified CallManager で H.323 ゲートウェイとして IP-IP ゲートウェイを設定します。この場合でも、IP-IP ゲートウェイはゲートキーパーを使用してリモートの宛先を解決することができます。
- クラスタ間コールの解決、およびクラスタ間コールを IP-IP ゲートウェイを通じてルーティングするか、直接ルーティングするかの判定にゲートキーパーを使用する場合は、Cisco Unified CallManager にゲートキーパー制御のクラスタ間トランクを設定します。このアプローチでは、より柔軟でスケーラビリティのある配置になります。
- IP-IP ゲートウェイ上の CallManager 3.3(2) 以降との互換性があるのは、Cisco IOS Release 12.3(1) 以降です。Cisco IOS Release 12.4(6)T 以降を使用することをお勧めします。
- ゲートキーパーと中継ゾーン ゲートキーパーの機能は、それぞれ別のルータ プラットフォーム上で実行して、分離します。各 IP-IP ゲートウェイに対して、専用の中継ゾーン ゲートキーパーを配置する必要があります。
- 中継ゾーン ゲートキーパー機能と IP-IP ゲートウェイ機能は、同じルータ プラットフォーム上で実行（共存）することができます。ただし、P.9-33 の「冗長性」の項で説明しているスケーラビリティの要件に注意してください。
- 同じ Cisco Unified CallManager クラスタに制御されているエンドポイント間では、コールに IP-IP ゲートウェイを使用しないでください。
- 同じ Cisco Unified CallManager クラスタに制御されているエンドポイント間では、トポロジ対応コール アドミッション制御を提供するために RSVP 対応ロケーションを使用します。
- IP-IP ゲートウェイに対して RSVP 予約を有効にする場合は、ダイアル ピア設定で次のオプションを使用します。

```
req-qos guaranteed-delay audio
req-qos guaranteed-delay video
acc-qos guaranteed-delay audio
acc-qos guaranteed-delay video
```

この設定を行うと、各音声コールまたはビデオ コールに対して、IP-IP ゲートウェイは遅延保証付きのサービスを使用して RSVP 予約を要求します。要求された QoS と許容可能な QoS の両方がこの RSVP サービスを指定している場合、コールが成功するためには RSVP 予約が必須になります（予約を確立できない場合はコールが失敗します）。設定の詳細については、P.9-34 の「設定のガイドライン」を参照してください。

冗長性

冗長性とスケーラビリティを実現するには、複数の IP-IP ゲートウェイを同じ中継ゾーン ゲートキーパーおよび同じ中継ゾーンに登録します。中継ゾーン ゲートキーパーは、ラウンドロビン アルゴリズムを使用して、同じ中継ゾーンに含まれているすべての IP-IP ゲートウェイに着信コールを自動的に分配します。

IP-IP ゲートウェイに障害が発生すると、そのゲートウェイは中継ゾーン ゲートキーパーへの登録を失います。ゲートキーパーは、使用可能リソースのリストからそのゲートウェイを削除します。

IP-IP ゲートウェイに対して、最大負荷しきい値を手動で設定することもできます。ある IP-IP ゲートウェイで回線の使用率が一定の割合を超えると、そのゲートウェイは新しいコールの処理用としては選択されなくなり、回線の使用率が一定の割合を下回ると、再び使用可能になります。このように設定するには、次の Cisco IOS コマンドを使用します。

- IP-IP ゲートウェイ上：

  ip circuit *max-calls max-call-number*

- ゲートキーパー上：

  endpoint resource-threshold onset *onset-threshold* **abatement** *abatement-threshold*

これらのコマンドの詳細については、次の Web サイトで入手できる Cisco IOS コマンド解説資料を参照してください。

http://www.cisco.com

設定のガイドライン

ここでは、図 9-21 に示したネットワーク ダイアグラムに基づく簡単な設定例を示します。この項は、詳細なコマンド リファレンス ガイドを意図したものではなく、一般的な配置シナリオに役立つガイドラインをまとめたものです。IP-IP ゲートウェイおよび中継ゾーン ゲートキーパーを設定する方法の詳細については、次の Web サイトで入手可能な、シスコ マルチサービス IP-to-IP ゲートウェイのオンライン ドキュメントで説明しています。

http://www.cisco.com

図 9-21　中継ゾーン ゲートキーパーを使用した IP-IP ゲートウェイの設定例

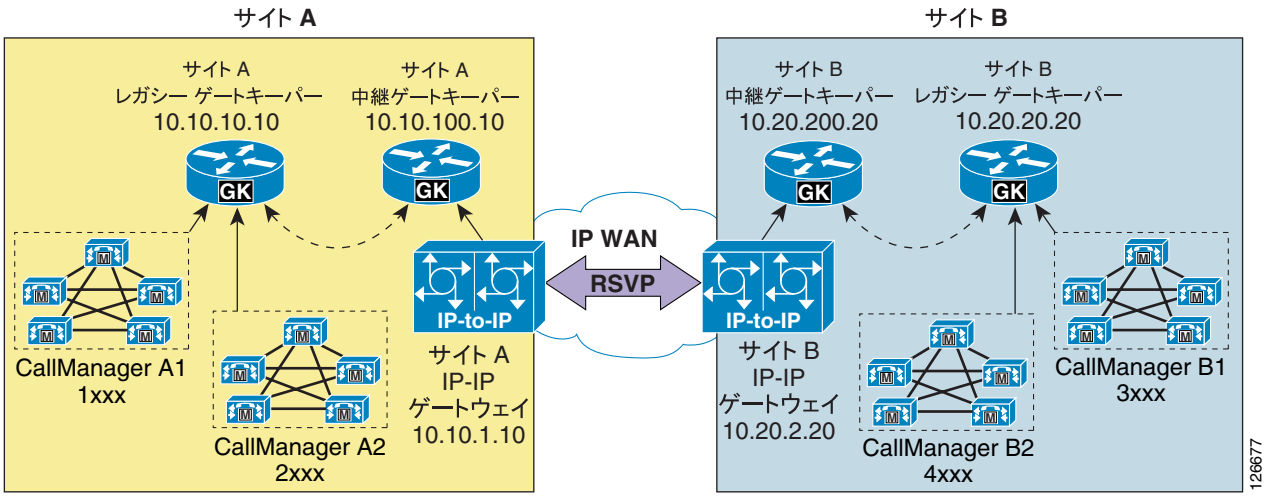


図 9-21 に示すネットワークでは、サイト A に内線番号 1*xxx* のクラスタ A1 と、内線番号 2*xxx* のクラスタ A2 の 2 つの Cisco Unified CallManager クラスタが存在しているとします。サイト B にも、内線番号 3*xxx* のクラスタ B1 と、内線番号 4*xxx* のクラスタ B2 の 2 つの Cisco Unified CallManager クラスタが存在します。

次の各項に、サイト A にあるデバイスに関連する設定を示します。サイト A の内部でやり取りされるコールは、（サイト A のレガシー ゲートキーパーを使用して）Cisco Unified CallManager クラスタ間で直接ルーティングされるのに対して、サイト B に向かうコールは、2 つの IP-IP ゲートウェイを通じて（それぞれのレガシー ゲートキーパーと中継ゾーン ゲートキーパーを使用して）ルーティングされます。

Cisco Unified CallManager

クラスタ A1 とクラスタ A2 は、どちらもゲートキーパー制御クラスタ間トランクを使用します。これは、MTP を必要とせず、サイト A のレガシー ゲートキーパーを指すクラスタ間トランク（ICT）です。

[34]XXX ルート パターンは、ゲートキーパーおよび IP-IP ゲートウェイを通じてサイト B のクラスタに到達するために、ルート リストおよびルート グループを通じて ICT を指しています。

他のルート パターン（クラスタ A1 の 2XXX とクラスタ A2 の 1XXX）は、ルート リストおよびルート グループを通じて ICT を指すことで、クラスタ A1 と A2 がゲートキーパーを通じて互いに通信できるようにしています。

レガシー ゲートキーパー

サイト A のレガシー ゲートキーパーは、クラスタ A1 と A2 の間ではコールを直接ルーティングし、サイト B に向かうコール（内線番号 3*xxx* と 4*xxx*）については、すべてサイト A の中継ゾーン ゲートキーパーに送信します。例 9-1 に、関連する設定を示します。

例 9-1　サイト A のレガシー ゲートキーパー設定

```
gatekeeper
 zone local CCM-A1 customer.com 10.10.10.10
 zone local CCM-A2 customer.com
 zone remote A-VIAGK customer.com 10.10.100.10
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 zone prefix A-VIAGK 3...
 zone prefix A-VIAGK 4...
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

中継ゾーン ゲートキーパー

サイト A の中継ゾーン ゲートキーパーは、サイト B の Cisco Unified CallManager クラスタ（内線番号 3*xxx* と 4*xxx*）に向かうコールをサイト B の中継ゾーン ゲートキーパーに送信し、サイト B で発着信されるコールに使用される IP-IP ゲートウェイを呼び出します。サイト A のクラスタに向かうコールは、サイト A のレガシー ゲートキーパーにルーティングされ、IP-IP ゲートウェイは呼び出されません。例 9-2 に、関連する設定を示します。

例 9-2　サイト A の中継ゾーン ゲートキーパー設定

```
gatekeeper
 zone local A-VIAGK customer.com 10.10.100.10
 zone remote CCM-A1 customer.com 10.10.10.10
 zone remote CCM-A2 customer.com 10.10.10.10
 zone remote B-VIAGK customer.com 10.20.200.20 invia A-VIAGK outvia A-VIAGK
 zone prefix B-VIAGK 3...
 zone prefix B-VIAGK 4...
 zone prefix CCM-A1 1...
 zone prefix CCM-A2 2...
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

例 9-2 に示す設定には、次の考慮事項が適用されます。

- B-VIAGK リモート ゾーンに関連するコマンドラインの **invia** キーワードと **outvia** キーワードが、このゾーンの中継ゾーン ゲートキーパーの処理をアクティブにします。つまり、B-VIAGK リモート ゾーンが宛先または発信元となるすべてのコールについて、中継ゾーン ゲートキーパーは、A-VIAGK ローカル ゾーンに登録されている IP-IP ゲートウェイ リソースを呼び出します。
- CCM-A1 リモート ゾーンおよび CCM-A2 リモート ゾーンに関連するコマンドラインには、**invia** キーワードと **outvia** キーワードがありません。このため、標準のゲートキーパー処理が適用され、これらのゾーンで発着信されるコールに対しては、IP-IP ゲートウェイは呼び出されません。

IP-IP ゲートウェイ

サイト A の IP-IP ゲートウェイは、サイト B の Cisco Unified CallManager クラスタ（内線番号 3*xxx* と 4*xxx*）に向かう音声コールとビデオ コールについては、RSVP 予約を要求します。一方で、サイト A の Cisco Unified CallManager クラスタ（内線番号 1*xxx* と 2*xxx*）に向かうコールについては要求しません。例 9-3 に、関連する設定を示します。

例 9-3　サイト A の IP-IP ゲートウェイ設定

```
voice service voip
   allow-connections h323 to h323
   h323
      emptycapability
      h245 passthru tcsnonstd-passthru
!
gateway
!
interface FastEthernet0/1
   ip address 10.10.1.10 255.255.255.0
   ip rsvp bandwidth 200
   ip rsvp data-packet classification none
   ip rsvp resource-provider none
   h323-gateway voip interface
   h323-gateway voip id A-VIAGK ipaddr 10.10.100.10
   h323-gateway voip h323-id A-IPIPGW
   h323-gateway voip bind srcaddr 10.10.1.10
   h323-gateway voip tech-prefix 1#
!
dial-peer voice 5 voip
   session target ras
   incoming called-number [3-4]...
   codec transparent
!
dial-peer voice 10 voip
   destination-pattern [3-4]...
   session target ras
   req-qos guaranteed-delay audio
   req-qos guaranteed-delay video
   acc-qos guaranteed-delay audio
   acc-qos guaranteed-delay video
   codec transparent
!
dial-peer voice 15 voip
session target ras
   incoming called-number [1-2]...
   req-qos guaranteed-delay audio
   req-qos guaranteed-delay video
   acc-qos guaranteed-delay audio
   acc-qos guaranteed-delay video
   codec transparent
!
dial-peer voice 20 voip
   destination-pattern [1-2]...
   session target ras
   codec transparent
```

例 9-3 に示す設定には、次の考慮事項が適用されます。

- **emptycapability** コマンドは、Cisco Unified CallManager と IP-IP ゲートウェイ間の H.245 ECS を有効にして、確立されたコールに対して補足サービスを呼び出します。
- **req-qos guaranteed-delay** [**audio** | **video**] コマンドで、ダイヤルピア 10 または 15 を使用する音声コールとビデオ コールについて、IP-IP ゲートウェイが遅延保証付きの RSVP 予約を要求することを指定します。
- **acc-qos guaranteed-delay** [**audio** | **video**] コマンドで、音声コールとビデオ コールに関して許容可能な最小限の QoS レベルも、遅延保証付き RSVP 予約であることを指定します。これは、RSVP 要求が失敗した場合はコールも失敗するので、RSVP 予約を必須にすることを意味します。RSVP 予約がオプションになるように（予約が失敗した場合でもコールが成功するように）IP-IP ゲートウェイを設定するには、代わりに **acc-qos best-effort** [**audio** | **video**] コマンドを使用します。

コール アドミッション制御の設計

ここでは、各種の Cisco Unified CallManager 配置モデルおよび次の IP WAN トポロジに対して、コール アドミッション制御メカニズムを適用する方法について説明します。

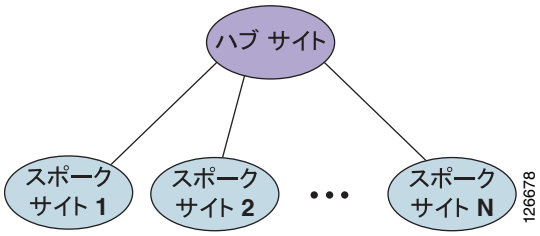
- 単純なハブアンドスポーク トポロジ（P.9-38）
- 2 層ハブアンドスポーク トポロジ（P.9-42）
- 単純な MPLS トポロジ（P.9-46）
- 汎用トポロジ（P.9-52）

これらの項では、採用する Cisco Unified CallManager 配置モデルに基づいて、トポロジごとにそれぞれ別の設計考慮事項を示します。

単純なハブアンドスポーク トポロジ

図 9-22 に、スター トポロジとも呼ばれる単純なハブアンドスポーク トポロジを示します。このタイプのネットワーク トポロジでは、すべてのサイト（「スポーク サイト」と呼ばれる）が、1 つの IP WAN リンクを通じて中央サイト（「ハブ サイト」と呼ばれる）に接続されます。スポーク サイト間には直接のリンクが存在しないため、スポーク サイト間の通信は、すべてハブ サイトを経由する必要があります。

図 9-22　単純なハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する単純なハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、P.9-46 の「単純な MPLS トポロジ」の項を参照してください。

以降では、採用する Cisco Unified CallManager 配置モデルごとに、単純なハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 集中型の Cisco Unified CallManager 配置（P.9-39）

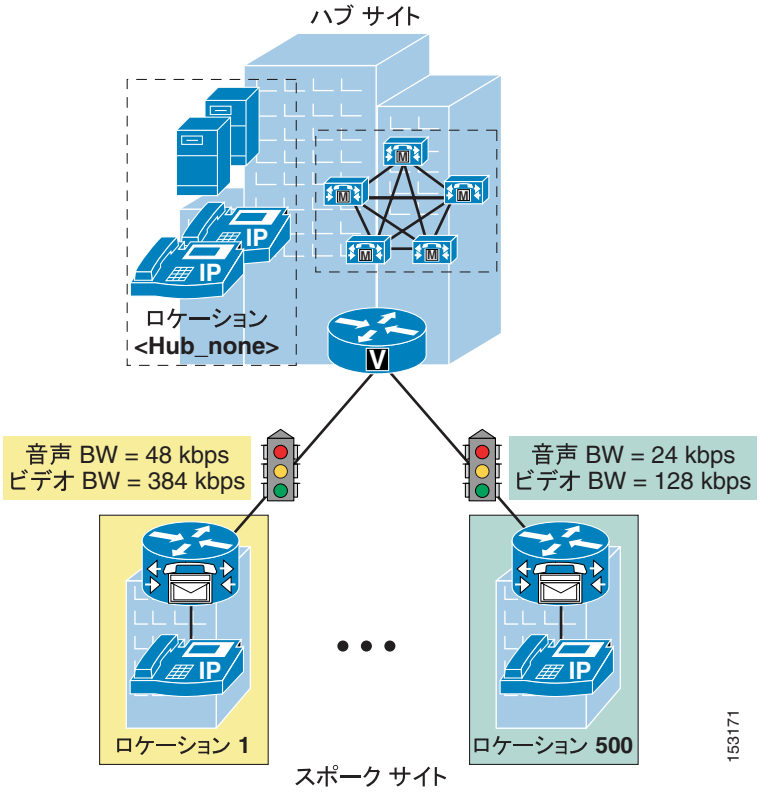
  1 つまたはそれ以上の Cisco Unified CallManager クラスタをハブ サイトに配置し、スポーク サイトには電話とゲートウェイだけを配置します。
- 分散型の Cisco Unified CallManager 配置（P.9-40）

  Cisco Unified CallManager クラスタまたは Cisco Unified CallManager Express を各サイトに配置します。

集中型の Cisco Unified CallManager 配置

単純なハブアンドスポーク トポロジ上にあり、集中型コール処理を使用するマルチサイト WAN 配置では、Cisco Unified CallManager の静的ロケーションを使用してコール アドミッション制御を実装します。図 9-23 に、このメカニズムをこのようなトポロジに適用する方法の例を示します。

図 9-23　静的ロケーションを使用した単純なハブアンドスポーク トポロジのコール アドミッション制御



コール アドミッション制御に対して静的ロケーションを使用する場合は、次のガイドラインに従ってください。

- 各スポーク サイトの Cisco Unified CallManager に対しては、個別にロケーション設定が必要です。
- 各サイトの音声コールとビデオ コールに対する帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の推奨設定については、表 9-1 を参照してください）。
- 各スポーク サイトのすべてのデバイスを適切なロケーションに割り当てます。
- ハブ サイトのデバイスは、Hub_None ロケーションのままにします。
- あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Cisco Unified CallManager は、ロケーションを 500 個所までサポートします。
- WAN の帯域幅が十分にない場合に、公衆網を介した自動ルーティングを実行する必要があるときは、Cisco Unified CallManager 上で Automated Alternate Routing（AAR）機能を設定します（P.10-28 の「Automated Alternate Routing」を参照）。
- 同じハブ サイトに複数の Cisco Unified CallManager クラスタを配置する場合は、クラスタ間トランク デバイスを Hub_None ロケーションのままにします。ダイヤル プランの解決には、ゲートキーパーを使用できます。ただし、この場合、ゲートキーパーのコール アドミッション制御は必要ありません。これは、すべての IP WAN リンクがロケーション アルゴリズムによって制御されるためです。

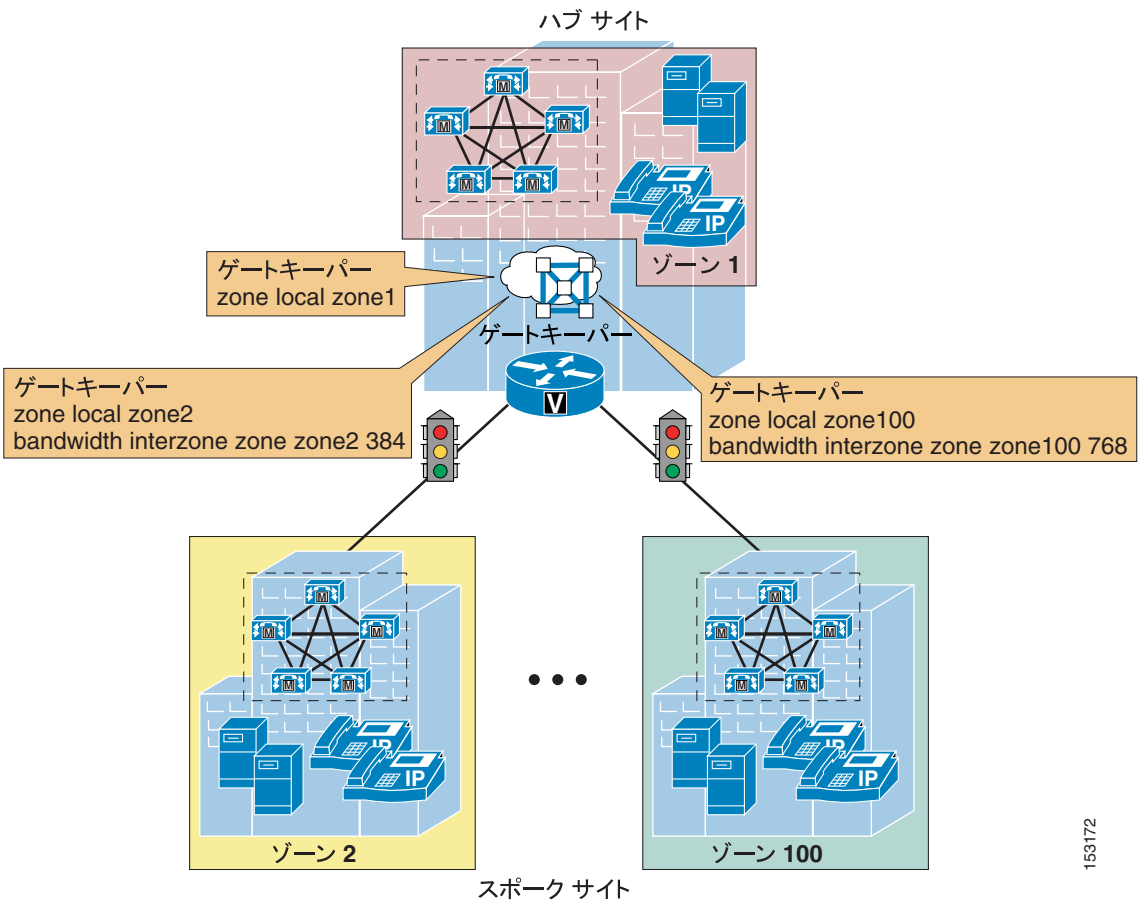
(注)　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、P.9-52 の「汎用トポロジ」の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、P.9-6 の「トポロジ非対応コール アドミッション制御の制限」を参照してください。

分散型の Cisco Unified CallManager 配置

単純なハブアンドスポーク トポロジの分散型コール処理配置では、Cisco IOS ゲートキーパーを使用してコール アドミッション制御を実装できます。この設計では、コール処理エージェント（Cisco Unified CallManager クラスタ、Cisco Unified CallManager Express、または H.323 ゲートウェイなど）は Cisco IOS ゲートキーパーに登録し、エージェントが IP WAN コールを発信しようとするたびにゲートキーパーに照会を行います。Cisco IOS ゲートキーパーは、各コール処理エージェントを、特定の帯域幅制限があるゾーンに関連付けます。したがって、Cisco IOS ゲートキーパーは、ゾーンに出入りする IP WAN 音声コールが消費する最大帯域幅量を制限することができます。

図 9-24 では、ゲートキーパーを使用したコール アドミッション制御を示しています。つまり、コール処理エージェントは、IP WAN コールを発信するときに、まずゲートキーパーに許可を要求します。ゲートキーパーが許可を与えると、コール処理エージェントは、IP WAN を介してコールを発信します。ゲートキーパーが要求を拒否する場合、コール処理エージェントは別のパス（たとえば、公衆網）を試行するか、単にコールを廃棄させることができます。

図 9-24　ゲートキーパーを使用したハブアンドスポーク トポロジのコール アドミッション制御



ゲートキーパーを使用してコール アドミッション制御を配置する場合は、次のガイドラインに従ってください。

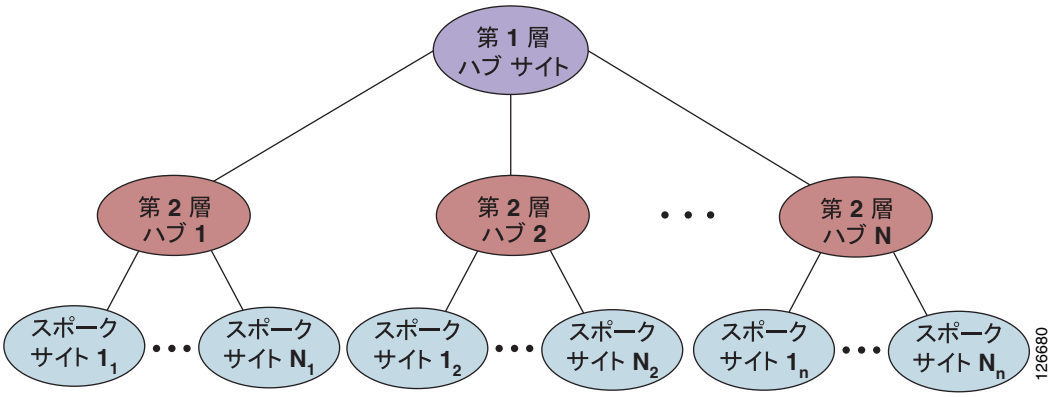
- Cisco Unified CallManager Express と H.323 ゲートウェイの混在環境の場合は、Cisco Unified CallManager で H.225 ゲートキーパー制御トランクを設定します。
- Cisco Unified CallManager クラスタだけに基づく環境の場合は、Cisco Unified CallManager でクラスタ間ゲートキーパー制御トランクを設定します。
- Cisco Unified CallManager で設定したゾーンが、そのサイトの正しいゲートキーパー ゾーンと一致するようにします。
- デバイス プールの Cisco Unified CallManager 冗長性グループにリストされている各 Cisco CallManager サブスクライバは、ゲートキーパー制御トランクをゲートキーパーに登録します（最大で 3 つまで）。
- コールは、Cisco Unified CallManager クラスタ内に登録済みのトランク間にロードバランスされます。
- Cisco Unified CallManager は、複数のゲートキーパーおよびトランクをサポートします。
- トランクをルート グループとルート リスト コンストラクトに配置すると、自動公衆網フェールオーバーを提供できます。詳細については、P.10-1 の「ダイヤル プラン」を参照してください。
- Cisco Unified CallManager、Cisco Unified CallManager Express、または H.323 ゲートウェイをサポートしている各サイトに対するゲートキーパーのゾーンは、個別に設定します。
- **bandwidth interzone** コマンドをゲートキーパーに使用して、そのゲートキーパーに直接登録済みの Cisco Unified CallManager クラスタ、Cisco Unified CallManager Express サーバ、および H.323 デバイス間の帯域幅の制御を行います（コーデック タイプ別の帯域幅の設定については、表 9-2 を参照してください）。
- 1 つの Cisco IOS ゲートキーパーで、100 までのゾーンまたはサイトをサポートできます。
- ゲートキーパーの冗長性は、ゲートキーパー クラスタリング（代替ゲートキーパー）または Cisco ホットスタンバイ ルータ プロトコル（HSRP）を使用すると実装することができます。HSRP は、ソフトウェア機能セットにゲートキーパー クラスタリングが使用可能ではない場合に限り使用します。

（注） 1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、P.9-52 の「汎用トポロジ」の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、P.9-6 の「トポロジ非対応コール アドミッション制御の制限」を参照してください。

2 層ハブアンドスポーク トポロジ

図 9-25 では、2 層ハブアンドスポーク トポロジを示しています。このタイプのネットワーク トポロジは 3 階層のサイト、つまり第 1 層ハブ サイト、第 2 層ハブサイト、およびスポーク サイトから構成されます。スポーク サイトのグループが 1 つの第 2 層ハブ サイトに接続され、各第 2 層ハブ サイトは 1 つの第 1 層ハブ サイトに接続されます。単純なハブアンドスポーク トポロジであるため、スポーク サイト間には直接のリンクが存在しません。したがって、スポーク サイト間の通信は、すべて第 2 層ハブ サイトを経由する必要があります。同様に、第 2 層ハブ サイト間には直接のリンクが存在しないため、これらのハブ サイト間の通信は、すべて第 1 層ハブ サイトを経由する必要があります。

図 9-25　2 層ハブアンドスポーク トポロジ



この項の設計上の考慮事項は、従来のレイヤ 2 IP WAN テクノロジーを使用する 2 層ハブアンドスポーク トポロジに適用されます。

- フレーム リレー
- ATM
- フレーム リレー /ATM 間サービス インターワーキング
- 専用回線

MPLS テクノロジーに基づいた IP WAN 配置については、P.9-46 の「単純な MPLS トポロジ」の項を参照してください。

以降では、採用する Cisco Unified CallManager 配置モデルごとに、2 層ハブアンドスポーク トポロジに関する設計上のベスト プラクティスを示します。

- 集中型の Cisco Unified CallManager 配置（P.9-43）

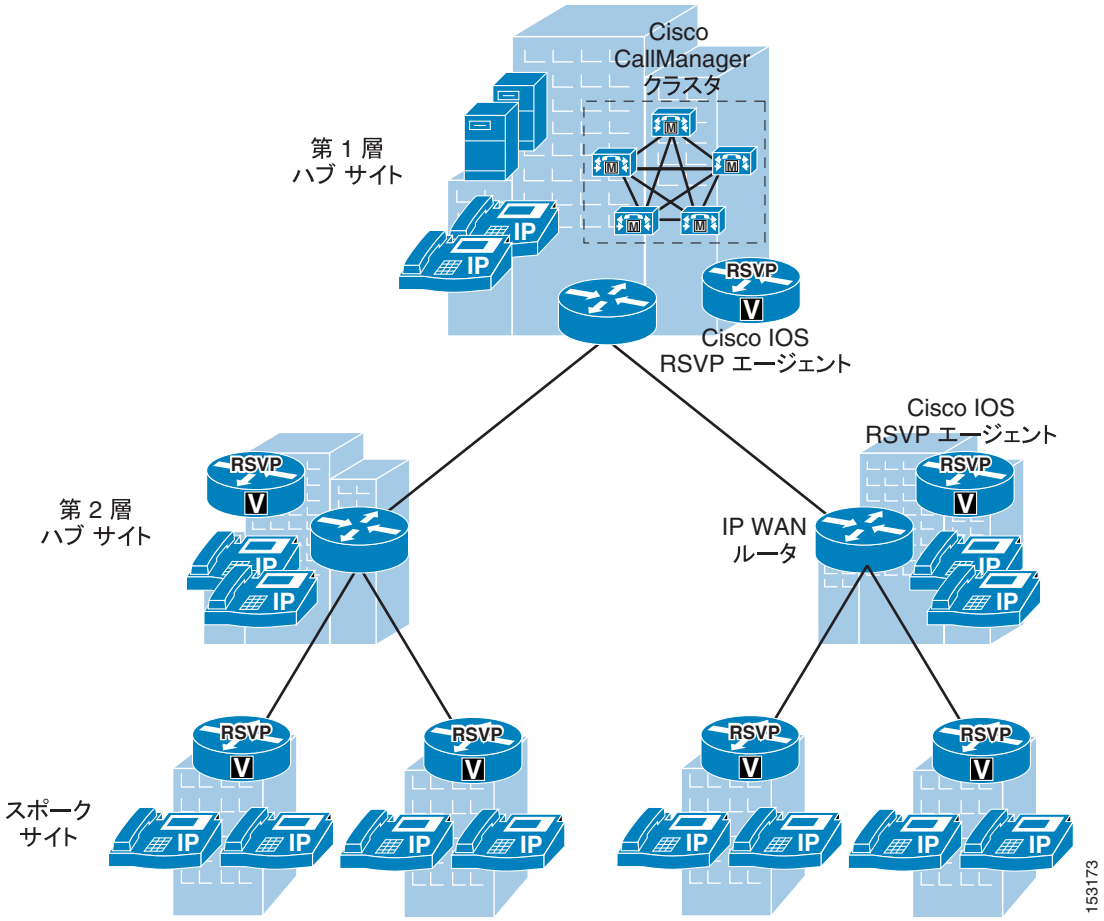
  1 つまたはそれ以上の Cisco Unified CallManager クラスタを第 1 層ハブ サイトに配置し、第 2 層ハブ サイトとスポーク サイトには電話とゲートウェイだけを配置します。
- 分散型の Cisco Unified CallManager 配置（P.9-45）

  Cisco Unified CallManager クラスタを第 1 層ハブ サイトと第 2 層ハブ サイトに配置し、スポーク サイトにはエンドポイントとゲートウェイだけを配置します。

集中型の Cisco Unified CallManager 配置

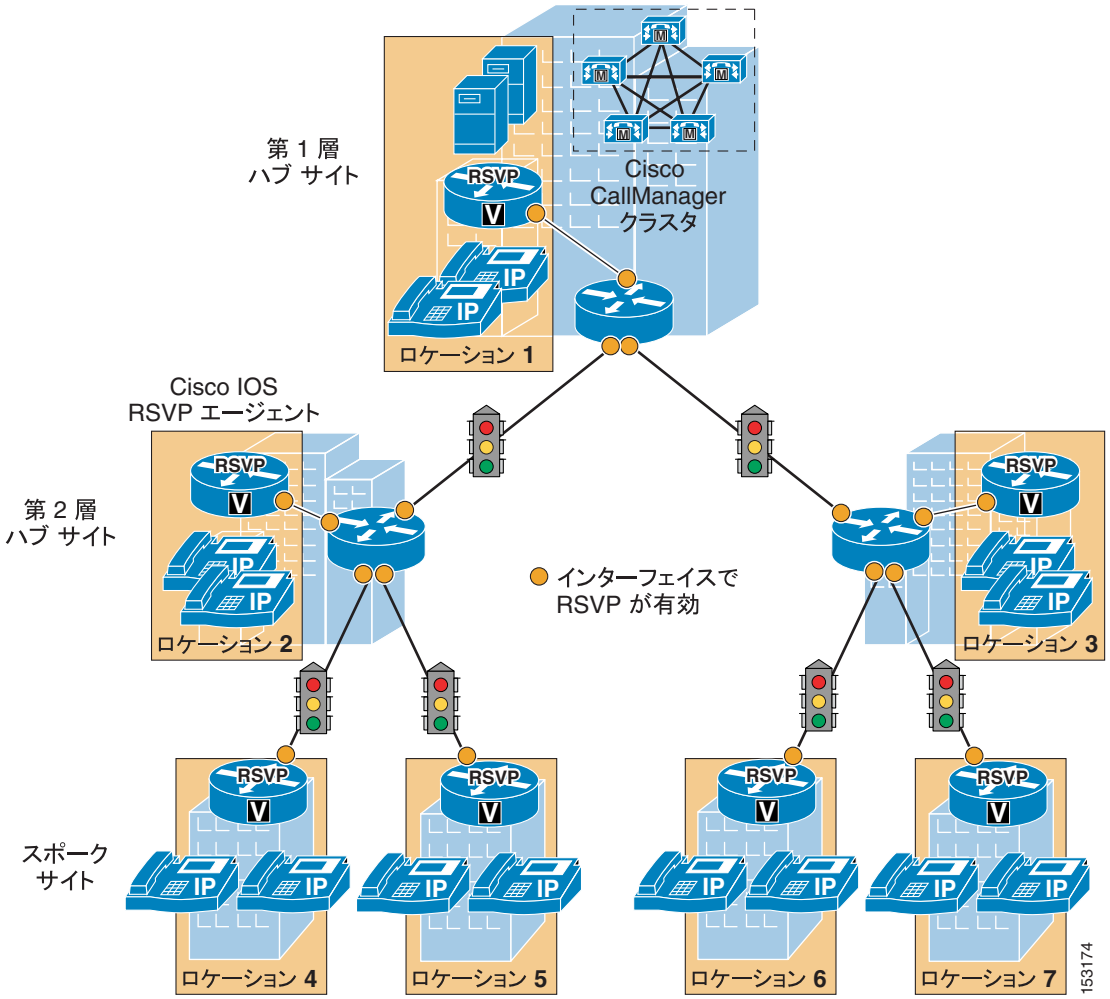
図 9-26 では、2 層ハブアンドスポーク IP WAN トポロジに配置された単一の Cisco Unified CallManager 集中型クラスタを示しています。このシナリオでは、Cisco Unified CallManager クラスタを第 1 層ハブ サイトに配置し、すべての第 2 層ハブ サイトとスポーク サイトにはエンドポイントとゲートウェイだけを配置します。

図 9-26　集中型の Cisco Unified CallManager での 2 層ハブアンドスポーク トポロジ



このシナリオでは、トポロジ対応コール アドミッション制御を配置する必要があります。そのため、単一の Cisco Unified CallManager クラスタにとっては、RSVP 対応ロケーションを使用することになります。図 9-27 では、このメカニズムを配置する方法を示しています。

図 9-27　RSVP 対応ロケーションを使用した 2 層ハブアンドスポーク トポロジのコール アドミッション制御



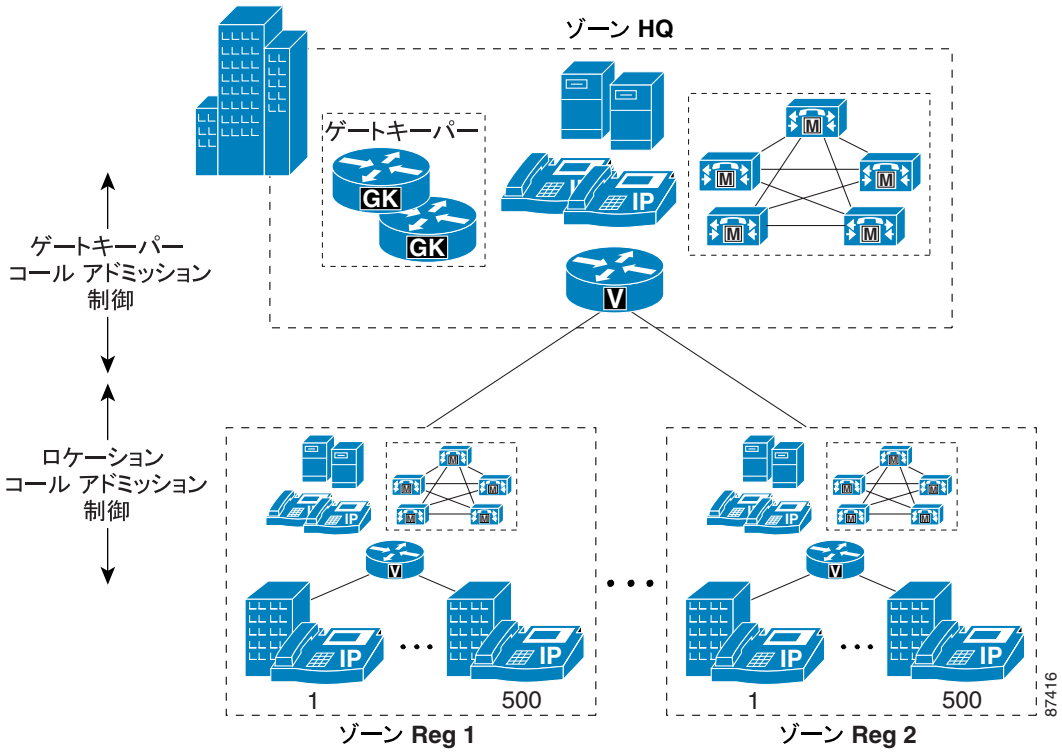
これらの配置には、次のガイドラインが適用されます。

- 各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Cisco Unified CallManager で、各サイトのロケーションを定義し、すべての帯域幅の値を **Unlimited** のままにします。
- 各サイトにあるすべてのデバイスを該当するロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスのメディア リソース グループ リスト（MRGL）のメディア リソース グループ（MRG）に属するようにします。
- Cisco CallManager サービス パラメータで、**Default inter-location RSVP Policy** を **Mandatory** または **Mandatory (video desired)** に設定し、**Mandatory RSVP mid-call error handle option** を **Call fails following retry counter exceeded** に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします（図 9-27 を参照）。

分散型の Cisco Unified CallManager 配置

2 層ハブアンドスポーク トポロジを採用していて、第 1 層ハブ サイトと第 2 層ハブ サイトに Cisco Unified CallManager がある配置にコール アドミッション制御を提供するには、図 9-28 に示されているように静的ロケーションとゲートキーパー ゾーン メカニズムを組み合せて対応します。

図 9-28　コール アドミッション制御にロケーションおよびゲートキーパー メカニズムを組み合せる方式



ゲートキーパー ゾーンを静的ロケーションと組み合せてコール アドミッション制御を実行する場合は、次の推奨事項に従ってください。

- ローカル Cisco Unified CallManager を使用していないサイト（つまり、スポーク サイト）には、静的ロケーションに基づくコール アドミッション制御を使用します。
- Cisco Unified CallManager クラスタ間（つまり、第 1 層ハブ サイトと第 2 層ハブ サイト間）には、ゲートキーパー ベースのコール アドミッション制御を使用します。
- ローカル Cisco Unified CallManager を使用していない各サイトには、そのサイトをサポートしている Cisco Unified CallManager クラスタ内にロケーションを設定します。
- 各サイトの帯域幅の上限を、そのサイトに使用されているコーデックのタイプに応じて、適切に設定します（帯域幅の設定については、表 9-1 と表 9-2 を参照してください）。
- Cisco Unified CallManager に設定された各デバイスをロケーションに割り当てます。あるデバイスを別のロケーションに移した場合、ロケーションの設定も変更します。
- Cisco Unified CallManager は、ロケーションを 500 個所までサポートします。
- 各 Cisco Unified CallManager クラスタは、ゲートキーパー制御のトランクをゲートキーパーに登録します。
- ゲートキーパーでは、各 Cisco Unified CallManager クラスタに対してゾーンを設定し、**bandwidth interzone** コマンドを使用して各クラスタを宛先および発信元とするコール数を制御します。

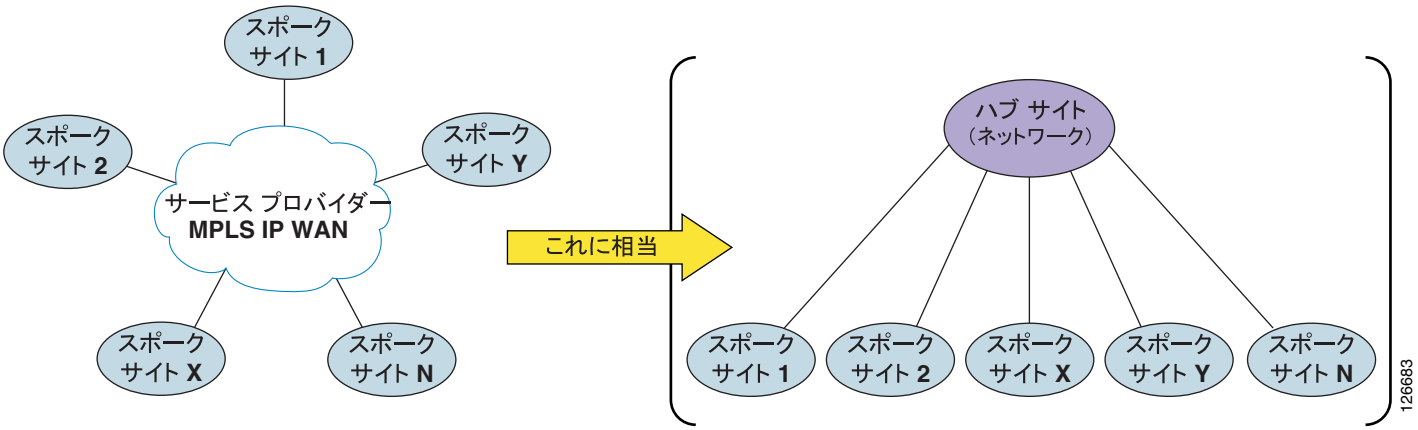
（注）1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、P.9-52 の「汎用トポロジ」の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。詳細については、P.9-6 の「トポロジ非対応コール アドミッション制御の制限」を参照してください。

単純な MPLS トポロジ

図 9-29 では、Multiprotocol Label Switching（MPLS）テクノロジー ベースの（サービス プロバイダーからの）IP WAN を示しています。サービス プロバイダーの提供する従来のレイヤ 2 WAN サービスと MPLS ベースのサービスのデザイン上の大きな違いは、MPLS を使用すると、IP WAN のトポロジはハブアンドスポークに準拠していないということです。すべてのサイト間の接続にはフルメッシュ接続方式を採用します。

このトポロジの違いは、ネットワークを企業側での IP ルーティングという観点から見たとき、各サイトが、他のどのサイトからも IP ホップ 1 つ分しか離れていないことを意味します。したがって、他のサイトに到達するためにハブ サイトを経由する必要はありません。事実上、「ハブ サイト」という概念が存在しません。すべてのサイトが対等と見なされ、各サイトで異なっているのは、IP WAN を介して使用することのできる帯域幅の量のみです。

図 9-29　サービス プロバイダーからの MPLS IP WAN、およびこれに相当するトポロジ



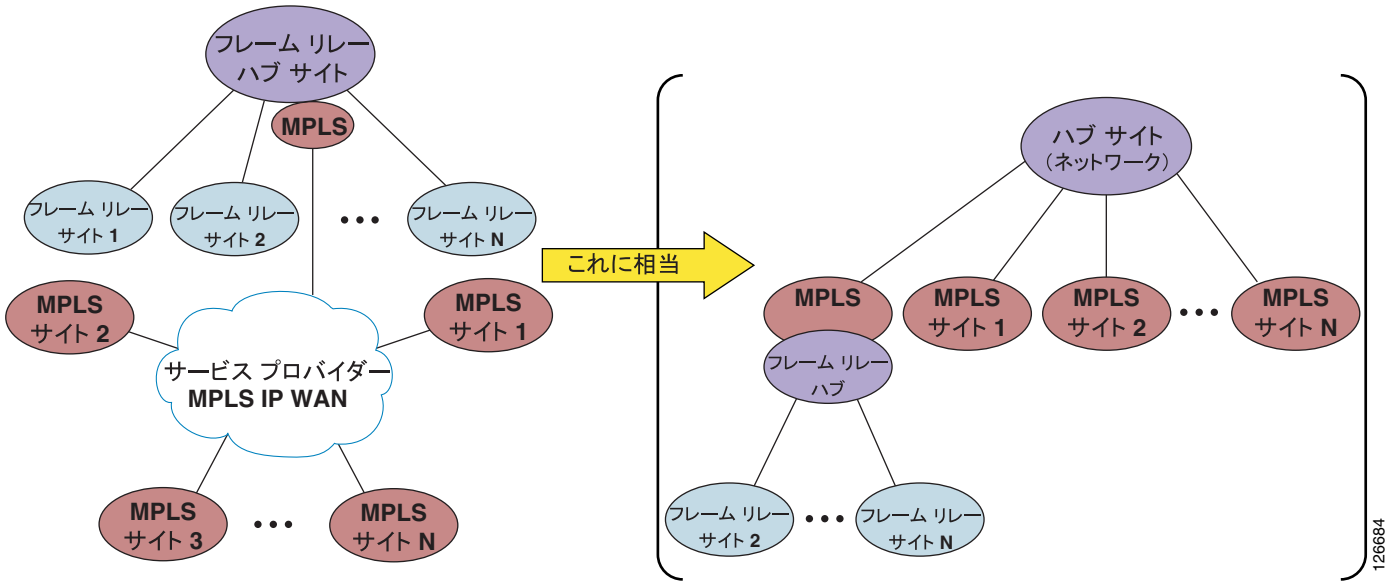
これまでに検討した内容に基づくと、コール アドミッション制御という観点から見たとき、MPLS に基づくサービス プロバイダー IP WAN サービスは、実質的には、ハブ サイトのないハブアンドスポーク トポロジに相当することが簡単にわかります（図 9-29 を参照）。事実上、ネットワーク自体をハブ サイトと見なすことができます。企業サイトは、いずれも（本社、つまり中央サイトを含めて）スポーク サイトに相当します。このように見方を変えると、コール アドミッション制御の実行方法も異なってきます。この方法については、以降で説明します。

上で検討した内容の中で、ここで例外として言及する価値があるのは、マルチサイト配置において、MPLS ベースの WAN がフレーム リレーや ATM などの従来のレイヤ 2 テクノロジー ベースの IP WAN と共存している場合です。このようなシナリオは、実際に発生する可能性があります。たとえば、ネットワークが移行の途中段階にある場合や、企業合併などの状況が発生した場合です。

図 9-30 に示すように、従来のレイヤ 2 テクノロジー（フレーム リレーなど）ベースのハブアンドスポーク IP WAN を MPLS ベースの IP WAN と統合すると、ネットワーク トポロジは単純なハブアンドスポークやフルメッシュではなく、2 層ハブアンドスポークになります。

この場合、MPLS ネットワークが第 1 層ハブ サイトを表し、MPLS 対応のフレーム リレー ハブ サイト、および MPLS ベースのサイトが第 2 層ハブ サイトを表し、フレーム リレー スポーク サイトがスポーク サイトを表します。したがって、このような配置での設計上の考慮事項については、P.9-42 の「2 層ハブアンドスポーク トポロジ」の項を参照してください。

図 9-30　MPLS サイトとフレーム リレー サイトの共存、およびこれに相当するトポロジ



以降では、採用する Cisco Unified CallManager 配置モデルごとに、MPLS ベースのトポロジに関する設計上のベスト プラクティスを示します。

- 集中型の Cisco Unified CallManager 配置（P.9-48）

  1 つまたはそれ以上の Cisco Unified CallManager クラスタを 1 つのサイトだけに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 分散型の Cisco Unified CallManager 配置（P.9-50）

  Cisco Unified CallManager クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

（注） ここでは、サービス プロバイダーによって MPLS サービスが提供されている企業の配置を中心に説明します。MPLS ネットワークが企業自体によって配置される場合、次の 2 つのいずれかの条件が満たされる限り、コール アドミッション制御は効果的に実行できます。最初の条件は、MPLS ネットワークでのルーティングが、ネットワークがハブアンドスポークになるように設定されていること、2 番目の条件は、輻輳が末端部分でしか発生しないように、MPLS ネットワークの核の部分の帯域幅を非常に大きく設定していることです。

(注)　1 つ以上のサイトに IP WAN への二重接続があり、両方のリンクで使用可能な帯域幅を最大限に利用する場合は、P.9-52 の「汎用トポロジ」の項で説明しているように、トポロジ対応コール アドミッション制御を配置することをお勧めします。ロード バランシング リンクが存在する場合は、対称的なルーティングを保証するために特に注意が必要です。詳細については、P.9-6 の「トポロジ非対応コール アドミッション制御の制限」および P.9-12 の「MPLS ネットワークの特別な考慮事項」を参照してください。また、シスコのアカウント チームにお問い合せください。

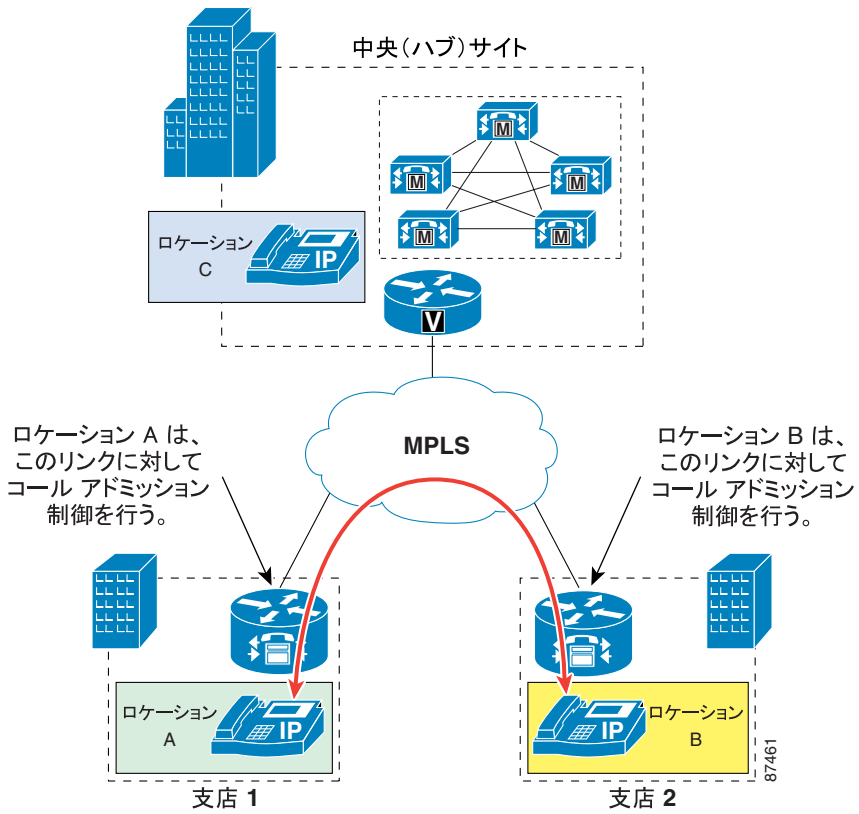
集中型の Cisco Unified CallManager 配置

MPLS トポロジ上で集中型コール処理を使用するマルチサイト WAN 配置では、Cisco Unified CallManager の静的「ロケーション」を使用してコール アドミッション制御を実装します。

ハブアンドスポーク WAN トポロジ（フレーム リレー、ATM など）では、支店サイトとのリンクはすべて、中央サイトで終端します。フレーム リレーを例にすると、支店ルータからのすべての PVC（Permanent Virtual Circuits; 相手先固定接続）は、中央サイトのヘッドエンド ルータに集約されています。この例では、帯域幅に対する課金は WAN リンクの支店エンドで行われているので、中央サイドではデバイスにコール アドミッション制御を適用する必要はありません。したがって、Cisco Unified CallManager　ロケーションの設定では中央サイトのデバイスのロケーションは Hub_None のままにしておきます。一方、各支店のデバイスは適切なコール アドミッション制御を受けるために各支店のロケーションに指定される必要があります。

MPLS WAN ネットワークでは、すべての支店はレイヤ 3 で隣接していると見なされるため、中央サイトに接続する必要はありません。図 9-31 では、スポークツースポーク配置による 2 つの支店間のコールを説明しています。

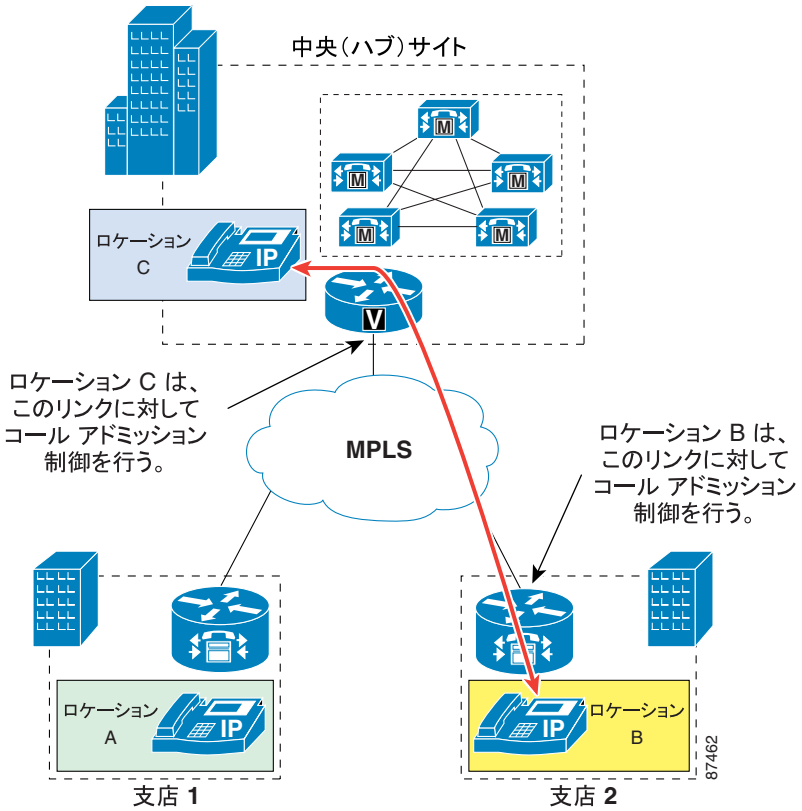
図 9-31　MPLS 配置におけるスポークツースポーク コール



また、MPLS WAN では、中央サイト WAN に接続しているリンクは支店の WAN リンクに集約していません。中央サイトに存在するすべてのデバイスは、個々のデバイスに対応するコール アドミッション制御ロケーション（つまり、Hub_None ロケーションではありません）に指定されています。したがって、このスポークツースポーク設定では支店のリンクとは無関係に、コール アドミッション制御は中央サイト リンク上で実行される必要があります（図 9-32 を参照）。

(注)　トランクなどの一部のデバイスはメディアを終端しないで、通常は Hub_None ロケーションのままにします。ただし、トランクで MTP が要求される場合にコール アドミッション制御のエラーを回避するためには、トランクは Hub_None 以外のロケーションに割り当てる必要があり、トランクの MRGL 内のすべての MTP は、そのロケーションに関連付けられたサイトに物理的に配置する必要があります。MTP はロケーションに直接割り当てることができず、その MTP を選択したデバイスのロケーションを継承するため、この設定が必要です。

図 9-32　MPLS 配置におけるハブとのコール

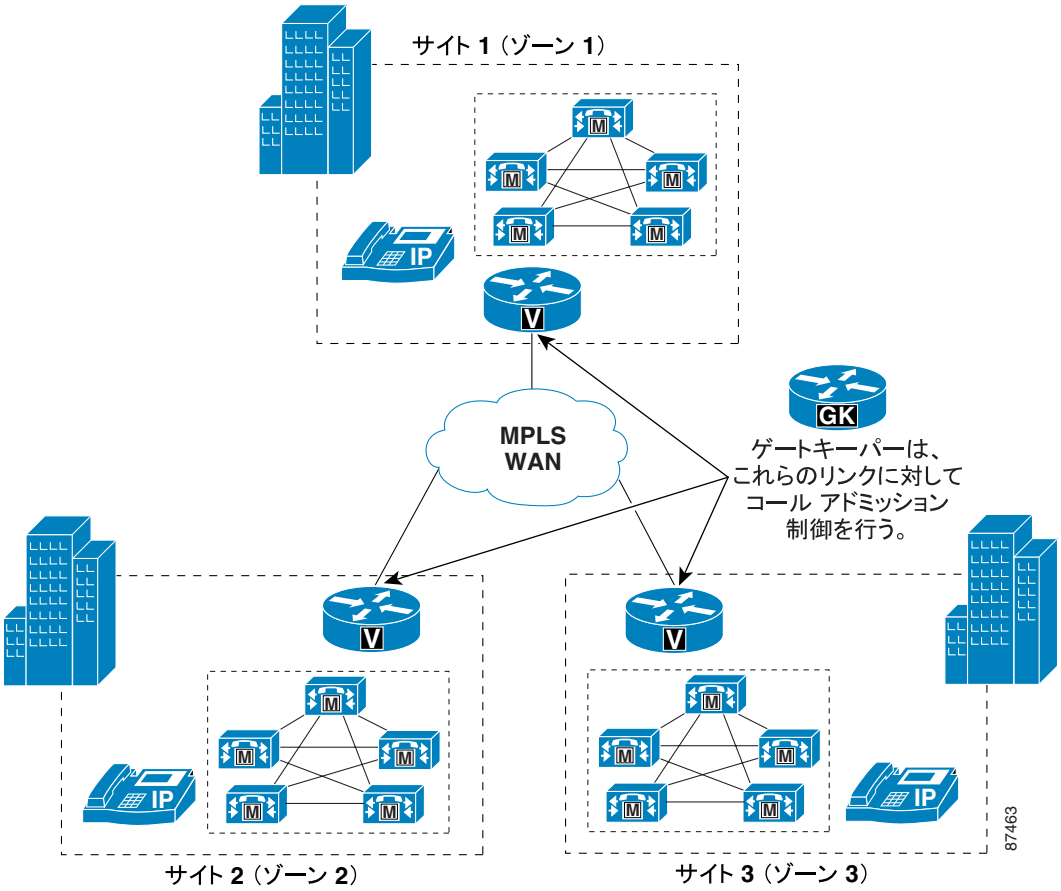


特定サイトに許されている帯域幅がすべて消費されてしまっている場合は、Cisco　Unified CallManager が備えている Automated Alternate Routing（AAR）機能を使用して、公衆網へ自動的にフェールオーバーさせることができます（AAR の詳細については、P.10-28 の「Automated Alternate Routing」を参照してください）。

分散型の Cisco Unified CallManager 配置

支店ロケーションのない複数のサイトに Cisco Unified CallManager クラスタが設定されていて、どのサイト間も MPLS WAN でリンクされているマルチ サイト配置の場合は、ゲートキーパーがダイヤル プランを解決し、サイト間のコール アドミッション制御を行い、個々のサイトを異なるゲートキーパー ゾーンに格納します。この同様のメカニズムは、レイヤ 2 WAN テクノロジーをベースにしたハブアンドスポークトポロジにも適用されています（図 9-33 を参照）。

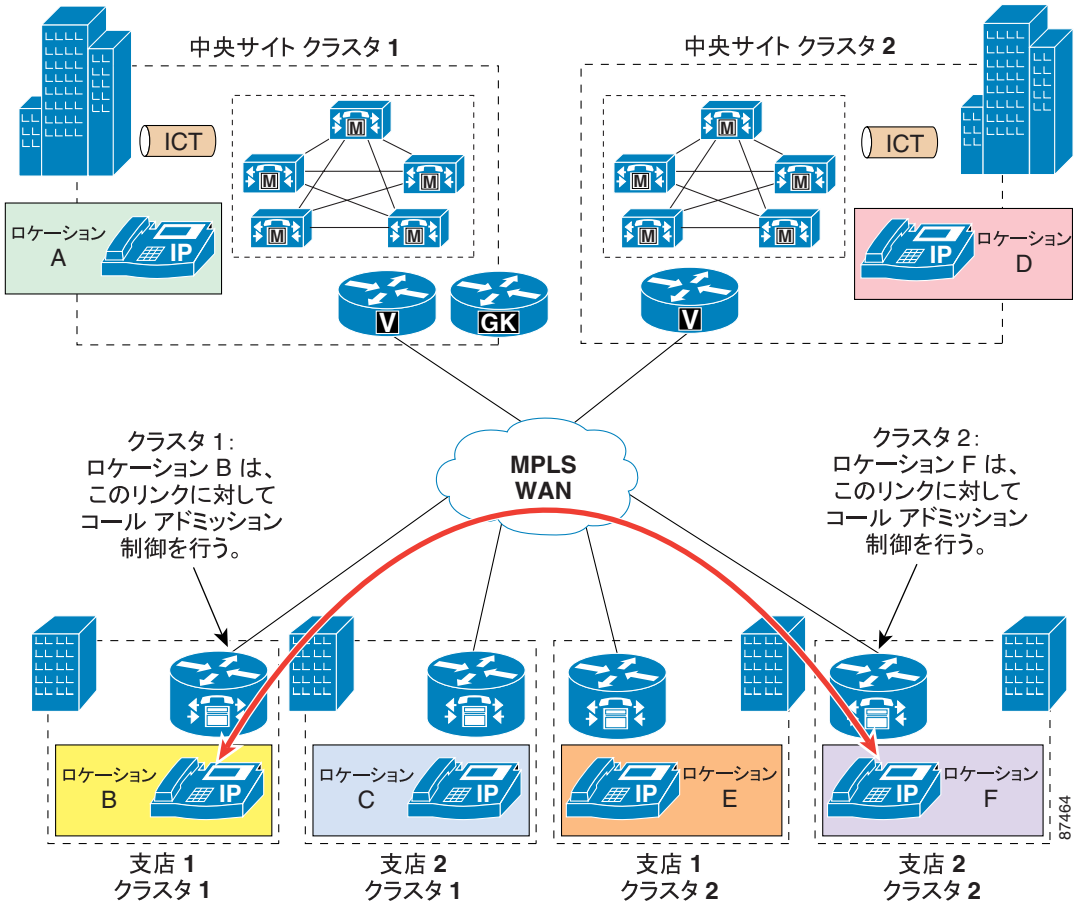
図 9-33　MPLS を使用した分散型配置におけるゲートキーパー コール アドミッション制御



支店サイトが必要な配置では、クラスタ間のダイヤル プランの解決にゲートキーパーを使用することもできますが、コール アドミッション制御にはゲートキーパーを使用しないことをお勧めします。

異なるクラスタに属している支店間にコールが発生した場合は、音声パスはその支店間で直接確立できるので、支店のクラスタから中央サイトへメディアを転送する必要はありません。したがって、コール アドミッション制御は各支店の WAN リンクに必要なだけです（図 9-34 を参照）。

図 9-34　クラスタ間トランク（ICT）によるマルチ クラスタ接続



Cisco Unified CallManager の集中型配置で見られるように、メディアを各サイトで終端するデバイス（各クラスタに対する中央サイトを含む）は、適切に設定されているロケーションに指定されている必要があります。

クラスタ間トランクで重要なことは、これは単なるシグナリング デバイスであって、クラスタ間トランクのメディアを転送する役目をもたないということです。したがって、クラスタ間トランクのロケーションの指定は、Hub_None のままにしておきます。トランクが MTP を必要とする場合は例外です。この場合は、トランクと MTP の両方を、それらが存在するサイトのロケーションに配置する必要があります。

特定のサイトに許されている帯域幅を消費してしまっている場合は、次の 2 つの方式を組み合せて、公衆網へ自動的にフェールオーバーすることができます。

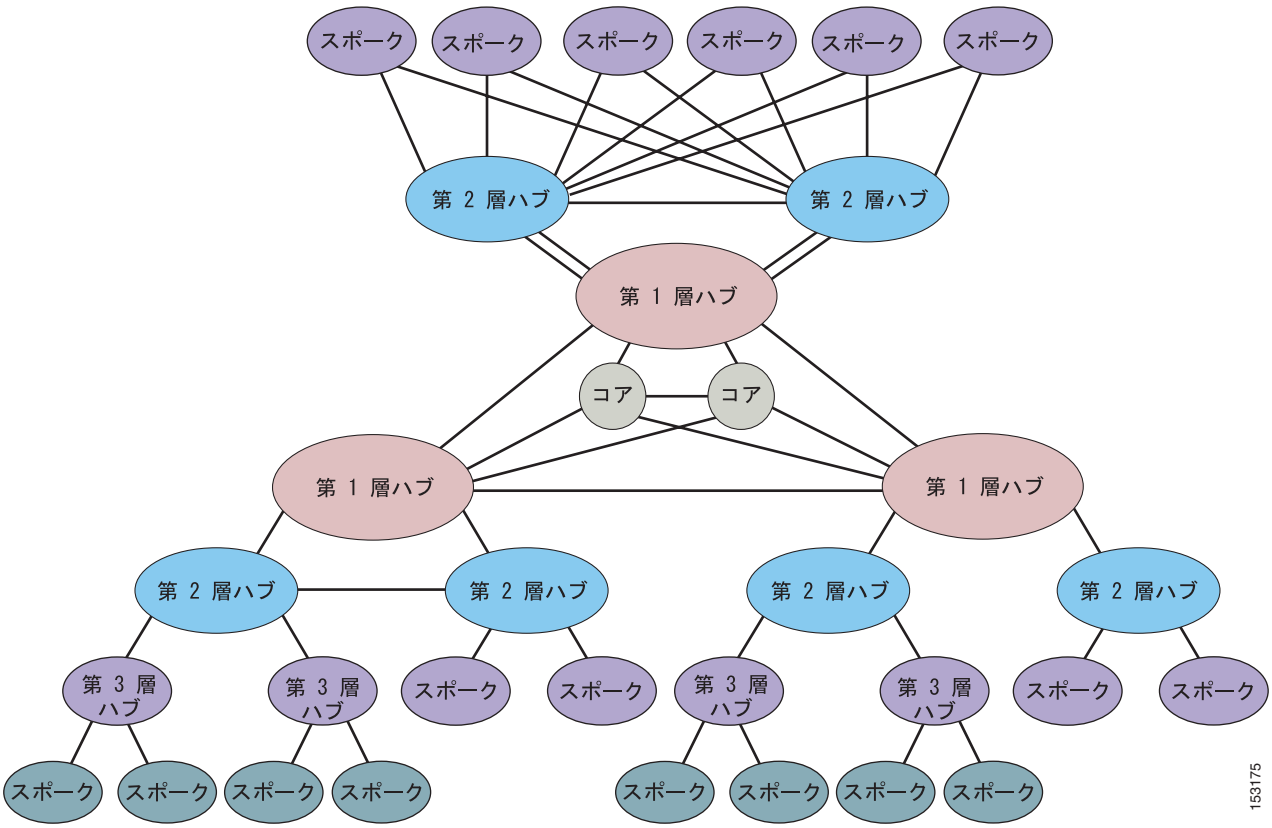
- マルチ Cisco Unified CallManager クラスタに対するコールには、ルート リストおよびルート グループで対応
- Cisco Unified CallManager クラスタ内のコールには、Automated Alternate Routing（AAR）機能で対応（AAR の詳細については、P.10-28 の「Automated Alternate Routing」を参照）

汎用トポロジ

この章の説明における汎用トポロジとは、単純なハブアンドスポーク、2 層ハブアンドスポーク、または単純な MPLS ベースのネットワークに変換できないネットワーク トポロジです。

図 9-35 に示すように、汎用トポロジでは、フルメッシュの機能、ハブアンドスポークの機能、部分メッシュの機能、またはこれらのすべての組み合せを 1 つのネットワーク内で実現できます。これは、サイト間の二重接続、および 1 つのサイトから別のサイトへのマルチ パスを表すこともあります。

図 9-35　汎用トポロジ



このようなネットワークは複雑な性質を持つため、RSVP に基づくトポロジ対応コール アドミッション制御メカニズムを採用する必要があります。このメカニズムは、特にトポロジの形態が次のような場合に、帯域幅を適切に制御できます。

- さまざまなハブ サイトにデュアル ホーム接続されたリモート サイト
- プライマリ / バックアップ設定またはアクティブ / アクティブ ロード バランシング設定のいずれかによる、任意の 2 つのサイト間の複数の IP WAN リンク
- 冗長ハブまたは専用接続を備えたデータ センター
- フル メッシュ構造のコア ネットワーク
- 任意の 2 つのサイト間の複数の等コスト IP パス
- 多層アーキテクチャ

以降では、採用する Cisco Unified CallManager 配置モデルごとに、汎用ネットワーク トポロジに関する設計上のベスト プラクティスを示します。

- 集中型の Cisco Unified CallManager 配置（P.9-53）

  1 つまたはそれ以上の Cisco Unified CallManager クラスタを特定のサイトに配置し、その他のすべてのサイトにはエンドポイントとゲートウェイだけを配置します。

- 分散型の Cisco Unified CallManager 配置（P.9-56）

  Cisco Unified CallManager クラスタを複数のサイトに配置し、その他のすべてのサイトには、エンドポイントとゲートウェイだけを配置します。

集中型の Cisco Unified CallManager 配置

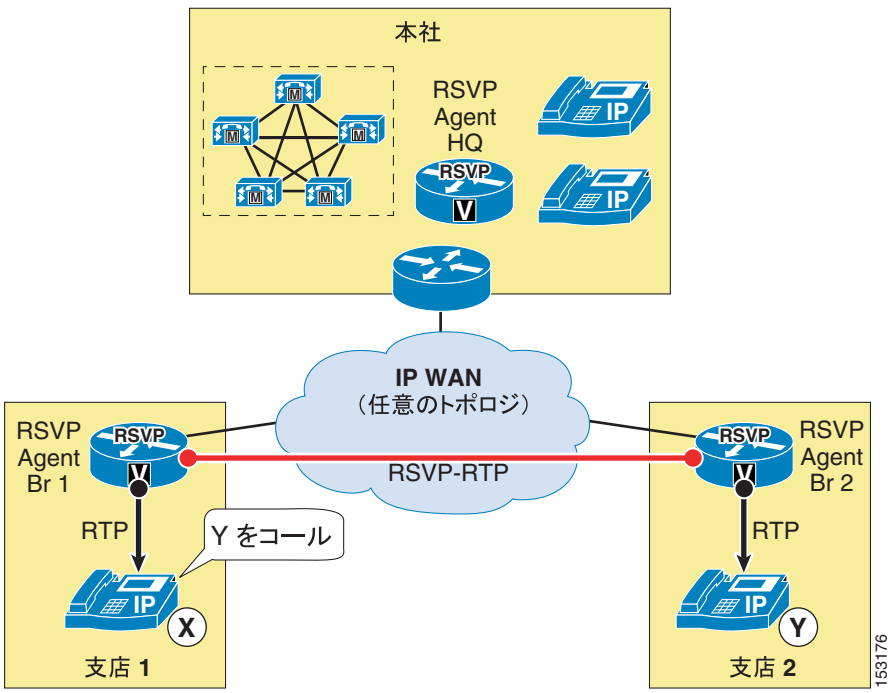
汎用トポロジを使用した Cisco Unified CallManager の集中型配置は、次の 2 つのサブタイプに分類できます。

- 単一の Cisco Unified CallManager クラスタ（P.9-53）
- 同じ場所にある Cisco Unified CallManager クラスタ（P.9-54）

単一の Cisco Unified CallManager クラスタ

この項の推奨事項は、図 9-36 に示すように、汎用ネットワーク トポロジで採用される単一の Cisco Unified CallManager クラスタに適用されます。

図 9-36　汎用トポロジにおける単一の Cisco Unified CallManager クラスタ



このタイプの配置には、次の考慮事項が適用されます。

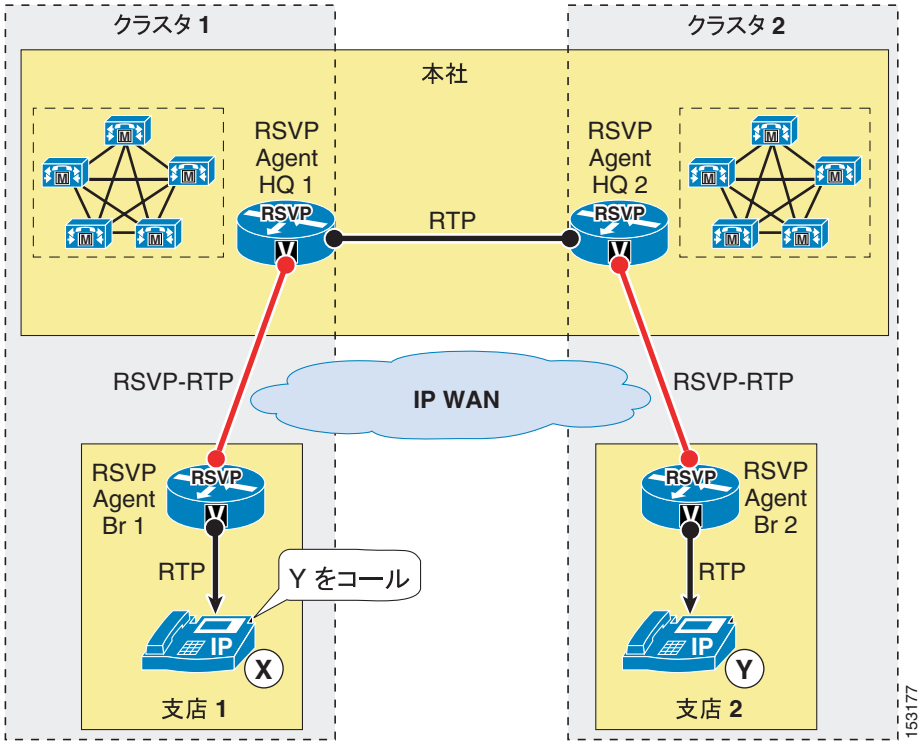
- Cisco Unified CallManager が存在する中央サイトなど、各サイトの Cisco IOS ルータで Cisco IOS RSVP Agent 機能を有効にします。比較的小さなサイトでは、このルータは IP WAN ルータおよび公衆網ゲートウェイと一体になっていることがあり、比較的大きなサイトでは異なるプラットフォームとなっている場合があります。
- Cisco Unified CallManager で、各サイトのロケーションを定義し、すべての帯域幅の値を **Unlimited** のままにします。
- 各サイトにあるすべてのデバイスを適切なロケーションに割り当てます（これにはエンドポイント、ゲートウェイ、会議リソース、および Cisco RSVP Agent 自体が含まれます）。
- 各 Cisco RSVP Agent が、そのサイトのすべてのデバイスのメディア リソース グループ リスト（MRGL）のメディア リソース グループ（MRG）に属するようにします。
- Cisco CallManager サービス パラメータで、**Default inter-location RSVP Policy** を **Mandatory** または **Mandatory (video desired)** に設定し、**Mandatory RSVP mid-call error handle option** を **Call fails following retry counter exceeded** に設定します。
- 輻輳が発生する可能性のあるネットワークですべての WAN インターフェイス上の RSVP を有効にし、プライオリティ キューのプロビジョニングに基づいて RSVP 帯域幅を設定します（P.3-52 の「RSVP を使用するベアラ トラフィックに関する追加の考慮事項」を参照）。
- 音声コールとビデオ コールに対して個別に帯域幅をプロビジョニングする必要がある場合は、同じ WAN ルータ インターフェイス上で RSVP アプリケーション ID も設定する必要があります。
- Cisco RSVP Agent が IP WAN ルータと共存していない場合、そのエージェントを WAN ルータに接続する LAN インターフェイスで RSVP を有効にします。

同じ場所にある Cisco Unified CallManager クラスタ

この項の推奨事項は、複数の Cisco Unified CallManager が同じ LAN または MAN にある配置に適用されます。Cisco Unified CallManager クラスタが存在するサイトが、高速リンクを通じて接続されている場合は、同じ考慮事項が有効なこともあります。ただし、そのリンクのプライオリティ キューに輻輳が発生せず、音声とビデオ用の帯域幅を無制限と見なせることが条件になります。

図 9-37 では、所定のサイト（本社）にある 2 つの Cisco Unified CallManager クラスタ、およびエンドポイントとゲートウェイを持つ複数のリモート サイトの配置を示しています。これらのリモート サイトは、クラスタ 1（たとえば支店 1）またはクラスタ 2（たとえば支店 2）のいずれかによって制御されます。

図 9-37　汎用トポロジにおける同じ場所にある Cisco Unified CallManager クラスタ



P.9-53 の「単一の Cisco Unified CallManager クラスタ」に示すガイドラインに加えて、このタイプの配置では次のベスト プラクティスに従ってください。

- 各クラスタに対して、クラスタ間トランクを定義して他のクラスタとの通信を有効にします。ゲートキーパーはダイヤル プラン解決のために使用できますが、コール アドミッション制御のためには不要です。
- 中央サイト（図 9-37 の例では本社）にあるすべてのデバイスで使用される同じロケーションにクラスタ間トランクを割り当てます。
- クラスタ間トランクが、MRGL を指定するデバイス プールに割り当てられるようにします。この MRGL は、中央サイトにある Cisco RSVP Agent（図 9-37 のクラスタ 1 では Cisco RSVP Agent HQ 1）を含む MRG を指します。
- クラスタ内でコール アドミッション制御に障害が発生した場合に備えて、AAR 機能を使用して自動公衆網フェールオーバーを提供します。
- クラスタ間でコール アドミッション制御に障害が発生した場合に備えて、ルート リストとルート グループ コンストラクトを使用して、自動公衆網フェールオーバーを提供します。
- メディア トラフィックとシグナリング トラフィックの両方は、異なるクラスタに属する 2 つの支店サイト間のコールに対して、中央サイトを通じたヘアピンになります（図 9-37 に示すように支店 1 の電話機 X と支店 2 の電話機 Y 間のコールは本社サイトを通じたヘアピンになります）。

分散型の Cisco Unified CallManager 配置

汎用ネットワーク トポロジで Cisco Unified CallManager の分散型配置にコール アドミッション制御を提供するには、関係する Cisco Unified CallManager クラスタの数によって、次の 2 つの方法が可能です。

- リモート Cisco RSVP Agent による方法（P.9-56）

  このソリューションは、帯域幅に制限のある IP WAN で接続された異なるサイトに、3 つ以下の Cisco Unified CallManager クラスタが配置される場合に適用されます。

- IP-IP ゲートウェイによる方法（P.9-59）

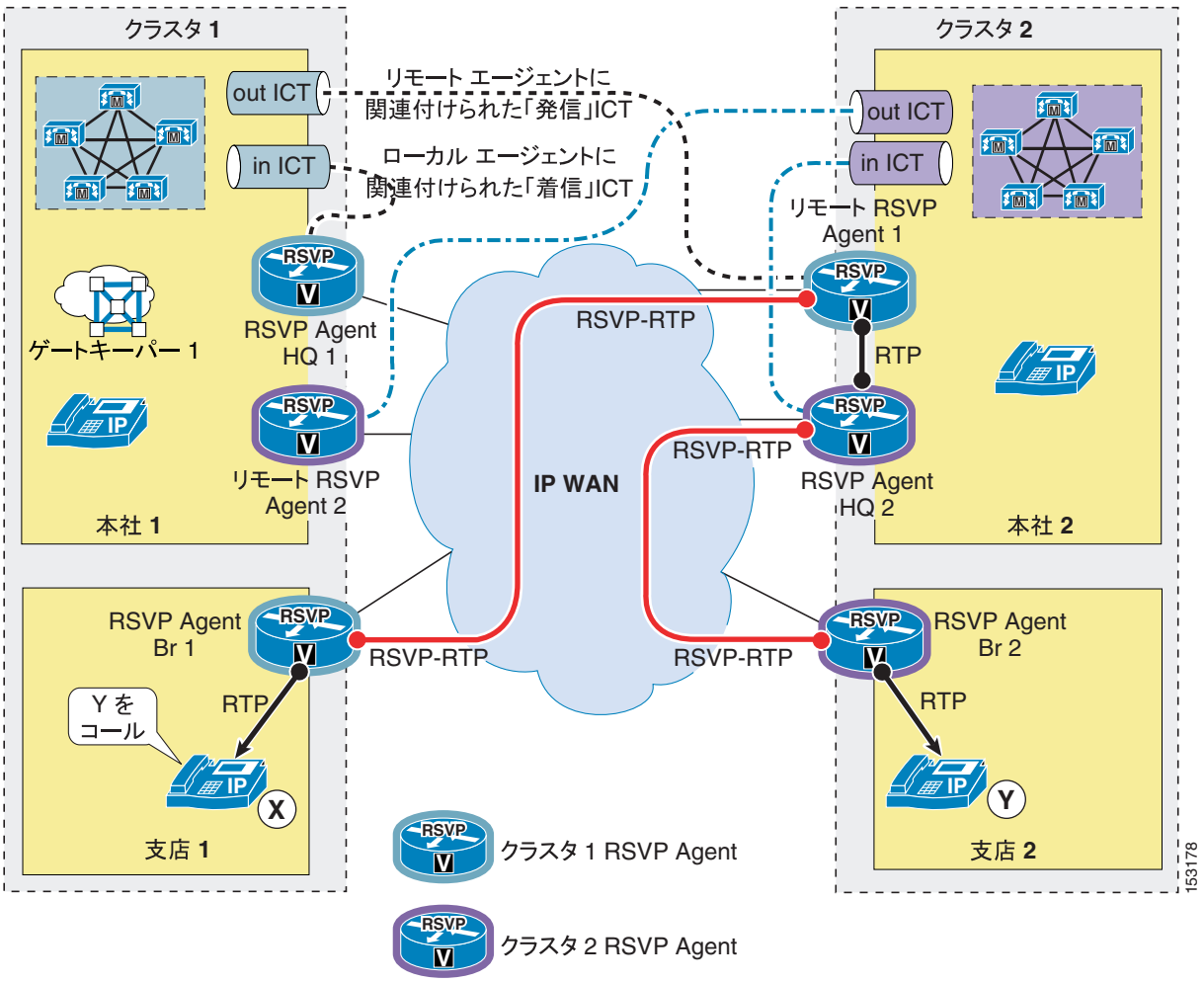
  このソリューションは、帯域幅に制限のある IP WAN で接続された異なるサイトに、任意の数の Cisco Unified CallManager クラスタが配置される場合に適用されます。

（注） 高速 IP WAN で接続されたサイトに Cisco Unified CallManager クラスタが配置される場合は、P.9-54 の「同じ場所にある Cisco Unified CallManager クラスタ」の項にある説明のように、このシナリオを扱うことができます。ただし、IP WAN リンクのプライオリティ キューに輻輳が発生しないことが条件になります。

リモート Cisco RSVP Agent による方法

異なるサイトに 3 つ以下の Cisco Unified CallManager クラスタが配置された汎用トポロジでコール アドミッション制御を提供するには、図 9-38 に示すように、「リモートの」Cisco RSVP Agent を定義することで、RSVP 対応ロケーションの概念を拡張してクラスタ間コールに対応できます。

図 9-38　汎用トポロジでの分散型クラスタ用のリモート Cisco RSVP Agent による方法



(注)　簡単にするため、この項の説明は図 9-38 に示すように、2 つの Cisco Unified CallManager クラスタの例に基づいています。3 つの Cisco Unified CallManager クラスタの配置については、項の末尾に注記を示しておきます。

P.9-53 の「単一の Cisco Unified CallManager クラスタ」の項に示すガイドラインに加えて、このような配置では次のベスト プラクティスに従ってください。

- 各クラスタでは、他のクラスタとの通信を可能にする 2 つのクラスタ間トランク（ICT）を定義します。1 つは「発信」クラスタ間トランク、もう 1 つは「着信」クラスタ間トランクです。
- ダイヤル プラン解決のために（コール アドミッション制御ではなく）Cisco IOS ゲートキーパーを設定し、Cisco Unified CallManager クラスタあたり 1 つのゾーンを定義します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
  zone local cluster2 customer.com
```

- 各クラスタでは、そのクラスタの通常ゾーン内のゲートキーパーに着信トランクを登録します（たとえば、クラスタ 1 の着信トランクはゾーン cluster1 に登録し、クラスタ 2 の着信トランクはゾーン cluster2 に登録します）。

- 各クラスタで、特別に作成したゾーン内のゲートキーパーに着信トランクを登録します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
  zone local cluster2 customer.com
  zone local cluster1-to-cluster2 customer.com
  zone local cluster2-to-cluster1 customer.com
```

- 他のクラスタに対する発信コールが着信クラスタ間トランクを使用するように、Cisco Unified CallManager ダイヤル プランを設定します（たとえば、クラスタ 1 では、ルート リストとルート グループ コンストラクトを通じて発信トランクを指す 2XXX ルートを設定します）。
- 特定のクラスタを宛先とするコールがその着信トランクにルーティングされるように、ゲートキーパー ダイヤル プランを設定します。次の例を参考にしてください。

```
gatekeeper
  zone local cluster1 customer.com 10.10.10.10
  zone local cluster2 customer.com
  zone local cluster1-to-cluster2 customer.com
  zone local cluster2-to-cluster1 customer.com
  zone prefix cluster1 1...
  zone prefix cluster2 2...
```

- そのサイトに配置されているすべてのデバイスと同じロケーションに着信トランクを割り当てます（たとえば、クラスタ 1 の着信トランクは本社 1 のロケーションに割り当て、クラスタ 2 の着信トランクは本社 2 のロケーションに割り当てます）。
- 新しく作成したロケーションに発信トランクを割り当てます（たとえば、クラスタ 2 に向かうクラスタ 1 の発信トランクは本社 2 に対するリモートのロケーションに割り当て、クラスタ 1 に向かうクラスタ 2 の発信トランクは本社 1 に対するリモートのロケーションに割り当てます）。
- Cisco Unified CallManager が常駐する 2 つの各サイトで、ローカル クラスタに登録された Cisco RSVP Agent のインスタンスを配置します（たとえば、本社 1 サイトに Cisco RSVP Agent HQ1 を配置し、本社 2 サイトに Cisco RSVP Agent HQ2 を配置します）。
- 該当のサイトに配置されているすべてのデバイスと同じロケーションにローカル Cisco RSVP Agent を割り当てます（たとえば、Cisco RSVP Agent HQ1 は本社 1 のロケーションに割り当て、Cisco RSVP Agent HQ2 は本社 2 のロケーションに割り当てます）。
- 各クラスタで、デバイス プールを通じて着信トランクによって使用される MRGL など、中央サイトに配置されたすべてのデバイスの MRGL に含まれる MRG にローカル Cisco RSVP Agent を割り当てます。
- Cisco Unified CallManager クラスタが存在する 2 つの各サイトで、その他の Cisco Unified CallManager クラスタに登録された Cisco RSVP Agent のインスタンスを追加します（たとえば、リモート Cisco RSVP Agent 1 はクラスタ 1 に登録され、本社 2 サイトに配置されます（このサイトにはクラスタ 2 があります）。一方、リモート Cisco RSVP Agent 2 は クラスタ 2 に登録され、本社 1 サイトに配置されます（このサイトにはクラスタ 1 があります）。
- 発信トランク用に作成されたロケーションに、これらのリモート Cisco RSVP Agent を割り当てます（たとえば、リモート Cisco RSVP Agent 1 はクラスタ 1 内の本社 2 に対するリモートのロケーションに割り当て、リモート Cisco RSVP Agent 2 はクラスタ 2 内の本社 1 に対するリモートのロケーションに割り当てます）。
- 各クラスタで、（デバイス プールを通じて）発信トランクで使用される MRGL に含まれる MRG に、リモート Cisco RSVP Agent を割り当てます。

（注） 論理的には区別されますが、リモート Cisco RSVP Agent インスタンスは、他のクラスタに登録されたローカル Cisco RSVP Agent と同じルータ プラットフォームに存在することがあります。たとえば、図 9-38 で、リモート Cisco RSVP Agent 1 と Cisco RSVP Agent HQ2 が実際に同じルータ プラットフォーム上に配置されている可能性があります。また、リモート Cisco RSVP Agent 2 と Cisco RSVP Agent HQ1 についても同じことが当てはまります。

図 9-38 で、支店 1 の電話機 X が支店 2 の電話機 Y にコールを発信した場合、Cisco Unified CallManager クラスタ 1 は、発信トランクを通じてゲートキーパーにそのコールをルーティングします。電話機 X は支店 1 のロケーションに割り当てられ、発信トランクは本社 2 に対するリモートのロケーションに関連付けられているため、Cisco Unified CallManager クラスタ 1 は、Cisco RSVP Agent Br 1 とリモート Cisco RSVP Agent 1 の間で IP WAN を通じて RSVP 予約を開始します（後者はクラスタ 2 とともに本社 2 に配置されています）。

次に、ゲートキーパーは、そのゾーン プレフィックス設定に基づいて、クラスタ 2 の着信トランクにコールをルーティングします。

その後、Cisco Unified CallManager クラスタ 2 は、（本社 1 のロケーションに関連付けられた）着信トランクおよび（支店 2 のロケーションに関連付けられた）電話機 Y からコールを受信し、Cisco RSVP Agent HQ2 と Cisco RSVP Agent Br 2 の間で IP WAN を通じてもう 1 つの RSVP 予約を開始します。

このコールは、4 つのコール レッグにわたって確立され、そのうち 2 つは IP WAN を通過し、RSVP に対応しています。

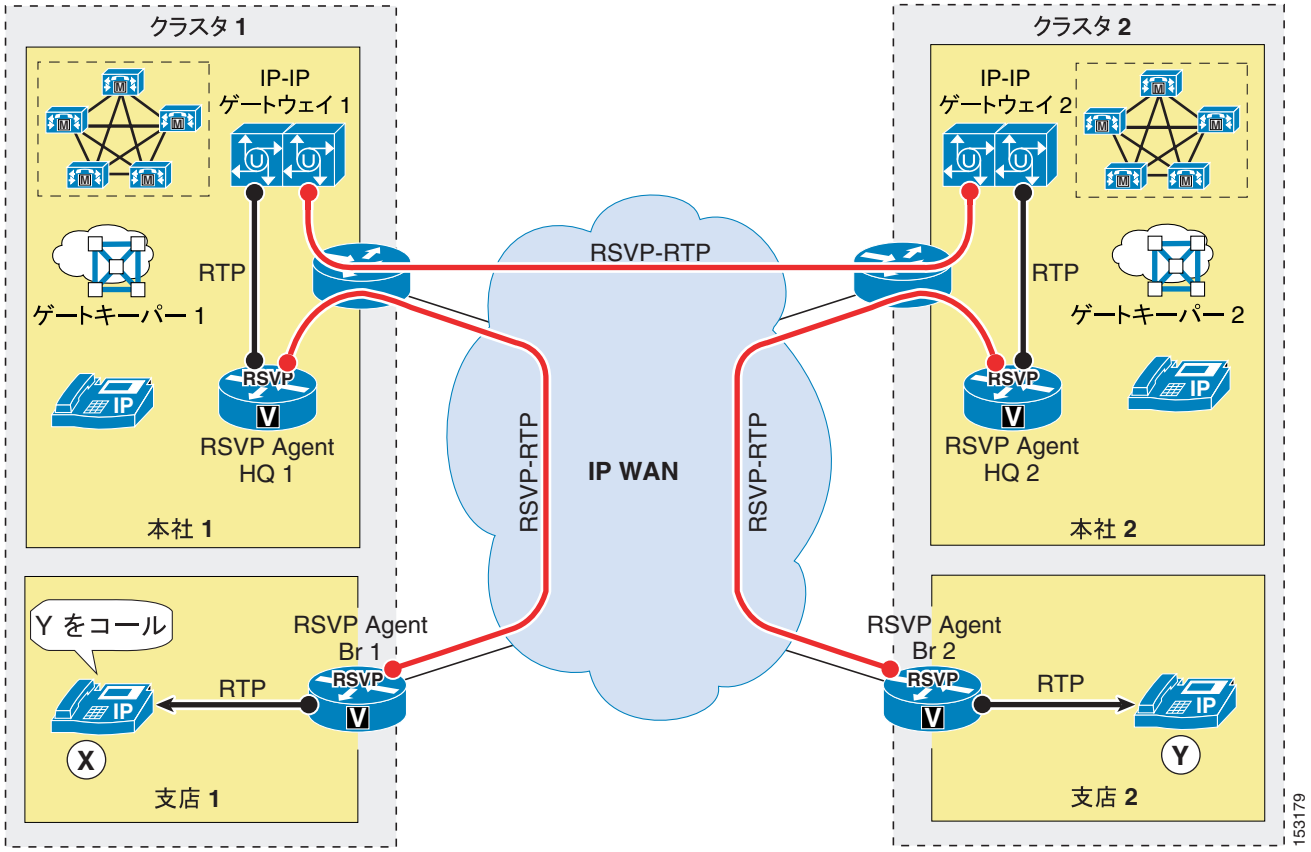
（注）　3 つの Cisco Unified CallManager クラスタのある配置では、同じ検討事項が適用されます。ただし、クラスタあたり 1 つの発信トランクを用意する代わりに、コールされる他の 2 つの各クラスタに対して 1 つずつ、2 つの発信トランクが必要です。同様に、各クラスタには、それぞれ他の 2 つのクラスタの一方に配置される 2 つのリモート Cisco RSVP Agent が必要です。

IP-IP ゲートウェイによる方法

前の項で説明したリモート Cisco RSVP Agent による方法の複雑さは、Cisco Unified CallManager クラスタの数とともに急速に増大します。したがって、最大 3 つのクラスタに限定されます。

異なるサイトに 4 つ以上の Cisco Unified CallManager クラスタが配置された汎用トポロジでコール アドミッション制御を提供するには、図 9-39 に示すように、クラスタ内のコールに対する RSVP 対応ロケーションと、クラスタ間のコールに対する RSVP 対応 IP-IP ゲートウェイを組み合せます。

図 9-39　汎用トポロジでの分散型クラスタ用の IP-IP ゲートウェイによる方法



P.9-53 の「単一の Cisco Unified CallManager クラスタ」の項に示すガイドラインに加えて、このような配置では次のベスト プラクティスに従ってください。

- 各クラスタに対して、ゲートキーパー制御クラスタ間トランクを定義して、他のクラスタとの通信を有効にします（ゲートキーパー ゾーンはダイヤル プラン解決に使用されますが、このシナリオでコール アドミッション制御のためには必要ありません）。
- そのクラスタの中央サイトに配置されたすべてのデバイスで使用される同じロケーションにクラスタ間トランクを割り当てます。
- クラスタ間トランクが、MRGL を指定するデバイス プールに割り当てられるようにします。この MRGL は、中央サイトにある Cisco RSVP Agent（たとえば、図 9-39 のクラスタ 1 では Cisco RSVP Agent HQ1）を含む MRG を指します。
- 各クラスタで、そのクラスタの中央サイトに IP-IP ゲートウェイを配置し、このゲートウェイを有効にして、IP WAN を通じた VoIP コールに RSVP を使用します。
- それぞれのゾーンを宛先または発信元とするすべてのコールに対してローカル　IP-IP　ゲートウェイが呼び出されるように、各クラスタで中継ゾーン ゲートキーパーとしてゲートキーパーを設定します（ゲートキーパーは、IP-IP ゲートウェイと共存する場合があることに注意してください）。
- クラスタ内でコール アドミッション制御に障害が発生した場合に備えて、AAR 機能を使用して自動公衆網フェールオーバーを提供します。
- クラスタ間でコール アドミッション制御に障害が発生した場合に備えて、ルート リストとルート グループ コンストラクトを使用して、自動公衆網フェールオーバーを提供します。

- メディア トラフィックとシグナリング トラフィックの両方は、異なるクラスタに属する 2 つの支店サイト間のコールに対して、それぞれのクラスタの中央サイトを通じたヘアピンになります（図 9-39 に示すように支店 1 の電話機 X と支店 2 の電話機 Y 間のコールは本社 1 および本社 2 サイトを通じたヘアピンになります）。

(注)　論理的には区別されますが、Cisco RSVP Agent、ゲートキーパー、および IP-IP ゲートウェイは、同じルータ プラットフォームに存在することがあります。たとえば、図 9-39 に示すシナリオで、IP-IP ゲートウェイ 1、ゲートキーパー 1、および Cisco RSVP Agent HQ1 は、IP-IP ゲートウェイ 2、ゲートキーパー 2、および Cisco RSVP Agent HQ2 と同様に、同じルータ プラットフォームに存在することがあります。

図 9-39 で、支店 1 の電話機 X が支店 2 の電話機 Y にコールを発信した場合、Cisco Unified CallManager のクラスタ 1 は、クラスタ間トランクを通じて ゲートキーパー 1 にそのコールをルーティングします。電話機 X は支店 1 のロケーションに割り当てられ、クラスタ間トランクは本社 1 のロケーションに関連付けられているため、Cisco Unified CallManager のクラスタ 1 は、Cisco RSVP Agent Br 1 と Cisco RSVP Agent HQ1 の間で IP WAN を通じて RSVP 予約を開始します。

次に、ゲートキーパー 1 は、中継ゾーン設定に基づいて IP-IP ゲートウェイ 1 にコールをルーティングし、IP-IP ゲートウェイ 1 は、IP WAN を通じて IP-IP ゲートウェイ 2 と RSVP 予約を確立します。一方、IP-IP ゲートウェイ 2 は、ゲートキーパー 2 を通じて Cisco Unified CallManager のクラスタ 2 と通信します。

その後、Cisco Unified CallManager のクラスタ 2 は、本社 2 のロケーションに関連付けられたクラスタ間トランクから、（支店 2 のロケーションに関連付けられた）電話機 Y に向けられたコールを受信し、Cisco RSVP Agent HQ2 と Cisco RSVP Agent Br 2 の間で IP WAN を通じてもう 1 つの RSVP 予約を開始します。

このコールは、7 つのコール レッグにわたって確立され、そのうち 3 つは IP WAN を通過し、RSVP に対応しています。

CHAPTER 10

ダイヤル プラン

ダイヤル プランは、IP テレフォニー システムの重要な要素の 1 つであり、すべてのコール処理エージェントにとって不可欠となる部分です。概説すると、ダイヤル プランは、コールをどのようにルーティングするかをコール処理エージェントに指示する役割を果たします。具体的には、ダイヤル プランは次の機能を実行します。

- エンドポイントのアドレッシング

  システム内部の宛先への到達は、すべてのエンドポイント（IP Phone、FAX マシン、アナログ電話機など）とアプリケーション（ボイスメール システム、自動アテンダント、会議システムなど）にディレクトリ番号（DN）を割り当てることで実現しています。

- パスの選択

  発信側のデバイスによっては、同じ宛先に到達する場合でも、複数のパスから選択することができます。また、プライマリ パスが使用不可になっている場合にはセカンダリ パスを使用できます。たとえば、IP WAN に障害が発生した場合は、コールを公衆網を介して透過的に再ルーティングできます。

- コール特権

  特定の宛先へのアクセスを許可または拒否することによって、複数のデバイス グループにそれぞれ別のサービス クラスを割り当てることができます。たとえば、ロビーにある電話からはシステム内部および市内の公衆網宛先にしか到達できないようにし、その一方で、幹部社員の電話からは無制限に公衆網アクセスできるようにします。

- 番号操作

  特定の状況では、ダイヤルされたストリングをコールのルーティング前に操作する必要があります。たとえば、オンネットのアクセス コードを使用してダイヤルされたコールを公衆網を通じて再ルーティングするときや、省略コード（オペレータにつなぐ場合の 0 など）を内線番号に展開するときです。

- コールのカバレッジ

  特殊なデバイス グループを作成して、特定サービスの着信コールを別の規則（トップダウン、循環ハント、最長アイドル時間、またはブロードキャスト）に従って処理することができます。

この章では、ダイヤル プランの主な側面について、次の項目を説明します。

- プランニングの考慮事項（P.10-3）

  この項では、IP テレフォニー ダイヤル プランのプランニングに関係するプロセスを詳しく説明します。取り扱う範囲は、内線番号に使用される桁数から、企業内部のダイヤル プラン アーキテクチャ全般までです（前提条件：ダイヤル プラン一般について、ある程度の知識があること）。

- ダイヤル プランの要素（P.10-9）

  この項では、Cisco Unified Communications ダイヤル プランの要素について詳しく説明します。取り扱うトピックには、コール ルーティングのロジック、コール特権、および各種シスコ製品における番号操作の方法が含まれています（前提条件：Cisco Unified CallManager および Cisco IOS の操作知識があることを推奨）。

- 設計上の考慮事項（P.10-57）

  この項では、マルチサイト IP テレフォニー ネットワーク、エンドポイントのアドレッシング方式、サービス クラスを作成するためのアプローチ、およびコール カバレッジ機能について、設計と配置のガイドラインを示します（前提条件：Cisco Unified CallManager および Cisco IOS の操作知識があることを推奨）。

詳細については、次の Web サイトから入手可能な『*Cisco Unified CallManager System Guide*』、『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』、およびその他の製品マニュアルを参照してください。

http://www.cisco.com

この章では説明のため、次の 2 つのタイプの IP Phone を定義します。

- タイプ A

  Cisco Unified IP Phone 7905、7912、7940、および 7960。

- タイプ B

  Cisco Unified IP Phone 7911、7941、7961、7970、および 7971。

タイプ A 電話機はタイプ B 電話機と動作が少し異なり、タイプ B 電話機では Keypad Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（P.10-10 の「タイプ A の SIP 電話機でのユーザ入力」および P.10-12 の「タイプ B の SIP 電話機でのユーザ入力」を参照）。

プランニングの考慮事項

ダイヤル プランは、テレフォニー システムの根本となる構成要素です。ユーザがどのように宛先に到達するかを規定する規則を定義しているので、まさにユーザ エクスペリエンスの中心部分になります。このような規則には、次のものがあります。

- 内線番号ダイヤリング：システム上の内線番号に到達するために、何桁ダイヤルする必要があるか。
- 内線番号アドレッシング：内線番号の識別に何桁を使用するか。
- ダイヤリング権限：特定のタイプのコールを許可するかどうか。
- パスの選択：たとえば、オンネット コールには IP ネットワークを使用する。または、国内公衆網コールにはあるキャリアを使用し、国際コールには別のキャリアを使用する。
- ネットワークが輻輳した場合の代替パス自動選択：たとえば、優先使用する国際キャリアがコールを処理できない場合に、国際コールに国内キャリアを使用する。
- 特定番号のブロック：たとえば、有料情報サービスへのコール。
- 着信番号の変換：たとえば、10 桁の番号としてダイヤルされたコールの最後の 5 桁のみを保持する。
- 発信番号の変換：たとえば、公衆網に発信するとき、発信者の内線番号をオフィスのメイン番号に置き換える。

IP テレフォニー システムに適したダイヤル プランは、従来の TDM テレフォニー システム用に設計するダイヤル プランと基本的には違いません。ただし、IP ベースのシステムによって、ダイヤル プランの構造にいくつかの新しい選択肢が生まれています。たとえば、個々のサイトにいるテレフォニー ユーザは、以前はそれぞれ別の独立 TDM システムによって処理されていましたが、IP ベースのテクノロジーは柔軟であるため、1 つの IP ベース システムに包含できるようになりました。このような新しい選択肢が IP ベースのシステムによってもたらされたため、ダイヤル プランの見方を再検討する必要があります。この項では、ダイヤル プランの設計にかかわる要件を正しく導き出すために、システムの設計担当者が検討する必要のあるいくつかの要素について説明します。

ダイヤル パターン認識

ユーザが電話機でダイヤルする番号ストリングは、一般的にパターンに従っています。たとえば、多くの企業では、同じオフィス ロケーション内で行われるコールに 5 桁の省略ダイヤリング パターンを使用しています。また、多くの企業では、外部へのダイヤリングを表すのに 1 桁のアクセス コードを用い、その直後に何桁かの番号をダイヤルして、ローカル公衆網の番号または長距離公衆網の番号に到達します（たとえば、ローカル番号への到達には 9 に続く 7 桁の番号を使用し、長距離の通話先への到達には 9 の後に 1 と 10 桁の番号をダイヤルします）。

システム管理者は、このようなパターンのシステムによる認識を計画し、あらかじめ決められたパターンに対応するストリングが検出されると同時にシステムが素早く反応し、ユーザがダイヤル後に遅延を感じない（または、その遅延が最小になる）ようにする必要があります。

Skinny Client Control Protocol（SCCP）を使用する電話機、およびダイヤル中に Keypad Markup Language（KPML）を使用する SIP 電話機の場合、パターン認識を実装するには、Cisco Unified CallManager でルート パターン、トランスレーション パターン、電話機 DN などを設定します。ユーザが 1 つの桁をダイヤルするたびに、電話機から Cisco Unified CallManager へシグナリング メッセージが送信され、一致するパターンを認識する差分処理が行われます。ユーザ入力に含まれる個々のキー操作が収集されるたびに、Cisco Unified CallManager の番号分析は次のような適切なユーザ フィードバックを提供します。

- 電話機が最初にオフフックになったときにダイヤル トーンを再生する。
- 番号がダイヤルされたらダイヤル トーンを停止する。

- 特定の番号のシーケンスがダイヤルされた場合、たとえば、オフネット アクセス コードの 9 がダイヤルされたときなどに、2 次ダイヤル トーンを提供する。

番号のダイヤリングが完了すると、Cisco Unified CallManager はユーザ フィードバックとしてコールプログレストーンを提供します。たとえば、通話先がアラート段階ならばリングバック トーン、通話先が無効であればリオーダー トーンを再生します。

SIP（Session Initiation Protocol）を実行する IP Phone には、設定に SIP ダイヤル規則というパターン認識命令を使用できます。この命令を使用すると、電話機内でパターン認識の大部分のタスクを実行できます。あるパターンが認識されると、SIP 電話機はユーザの入力に対応する番号にコールを発信するために、Cisco Unified CallManager に発信要求を出します。この動作は SIP INVITE と呼ばれ、SCCP プロトコルを実行している IP Phone からのコールと同じように、Cisco Unified CallManager のダイヤル プランによる制御対象となります。ただし、Cisco Unified CallManager の番号分析は完全なダイヤル ストリングを使用して行われます（ユーザが入力したすべての桁が、1 つのブロックとして Cisco Unified CallManager に渡されて処理されます）。この動作モードでは、番号ストリングのダイヤル中のユーザ フィードバックは、電話機が提供できるものだけに制限されます（P.10-14 の「SIP ダイヤル規則」を参照）。ストリングが合成された後も、Cisco Unified CallManager はユーザ フィードバックとしてコールプログレストーンを提供できます。

オンネットとオフネットのダイヤリング

同じテレフォニー ネットワーク上で発信され、終端するコールは、オンネットワーク（オンネット）と見なされます。これとは逆に、A 社で発信され、B 社で終端するコールは、通常は最初に A 社のネットワーク、次に公衆網、最後に B 社のネットワークというように、複数のテレフォニー ネットワークを通じてルーティングする必要があります。発信者から見ると、コールはオフネットワーク（オフネット）でルーティングされています。着信側から見ると、コールはオフネットで発生しています。

TDM システムでは、PBX または Centrex システムがテレフォニー システムのオンネット境界になります。TDM システムは、通常は 1 つのサイトの外側まで伸びていることはありません。伸びている場合も、その TDM システムは、大規模なシステム ハブの外周上に配置されていないサイトを含んでいないのが普通です。

IP テレフォニーの重要な特性の 1 つは、オンネットと見なすことのできるコール境界を拡張する機能です。たとえば、6 つの支店を保有している企業に所属するテレフォニー ユーザが、着信側が同じサイトにいる場合は省略ダイヤリング（4 桁の内線番号など）を使用して同僚に到達し、他のサイトにいる別の同僚に到達するときは、完全な公衆網番号をダイヤルしているとします。IP ベース システムを使用すると、すべてのユーザが同じ IP ネットワークによって処理されるため、6 つの支店を 4 桁の省略ダイヤリング プランによって経済的に結ぶことが可能になります。IP ネットワークを優先パスとして使用し、IP ネットワークが輻輳した場合のセカンダリ パスとして、公衆網への自動オーバーフローを使用します。

省略ダイヤリング

公衆網から直接到達可能な、ダイヤルイン（DID）機能を使用した内線番号があるとします。オフネットの公衆網発信者が DID 内線番号に到達するには、完全修飾公衆網番号（たとえば、1 415 555 1234）をダイヤルする必要があります。しかし、オンネットの発信者については、DID 番号の最後のいくつかの桁をダイヤルするだけでこの内線番号に到達する機能を利用することを考えています。4 桁の省略ダイヤル プランを使用すると、この例のオンネットの発信者は、1234 のみダイヤルすればこの内線番号に到達します。

内線ダイヤリングの重複の防止

テレフォニー システムは、どの内線番号にも明確な方法で到達できるように設定する必要があります。この目標を達成するには、ダイヤル プランが次の要件を満たす必要があります。

- すべてのオンネット内線ダイヤリングを、グローバルに一意なものにする。たとえば、4 桁の省略オンネット ダイヤル プランを使用するシステムで、サイト A とサイト B のどちらの内線番号についても、サイト C から 4 桁のみダイヤルして到達することが要件である場合、サイト A に内線番号 1000 があり、サイト B の別の内線番号も 1000 である状態は許されません。
- 個々のダイヤルストリングは、部分的にも重複していない。
  - たとえば、4 桁の省略ダイヤル プランにおいて、9 をオフネット アクセス コードとして使用する場合（公衆網コールを発信する場合など）、内線番号を 9XXX にすることはできません。このように設定すると、コールがすぐにはルーティングされない状況が発生します。たとえば、ユーザが 9141 をダイヤルしたとします。システムは、追加の数字が入力されるか（ユーザが 9 1 415 555 1234 をダイヤルしようとしている場合など）、桁間タイムアウトに達するまで待機し、その後でコールを内線番号 9141 にルーティングします。同様に、オペレータ コード（たとえば 0）を使用する場合にも、0XXX の内線番号範囲全体を 4 桁の定型ダイヤル プランから除外する必要があります。
  - 長さが異なっていても、ストリングが重複していることは許されません。たとえば、システムで内線番号 1000 と 10000 を使用すると、1000 にダイヤルする場合、ユーザは桁間タイムアウトに達するまで待機する必要があります。

ダイヤリング ストリングの長さ

内線番号にダイヤルするときの必要桁数は、ダイヤル可能な内線番号の数によって決まります。たとえば、4 桁の省略ダイヤル プランでは、内線番号が 10,000 個（0000 ～ 9999）を超える場合には対応できません。0 と 9 をオペレータ コードおよびオフネット アクセス コードとしてそれぞれ予約する場合、この番号範囲は、さらに 8,000 個（1000 ～ 8999）まで減ります。

定型オンネット ダイヤル プラン

ダイヤル プランは、システム内のすべての内線番号に一定の方法で到達するように設計できます。つまり、任意のオンネット発信地点から、特定の内線番号に一定の桁数で到達することができます。ユーザにとって簡潔であるため、定型ダイヤリングを使用することをお勧めします。各種のオンネット ロケーションから発信するときに、番号をダイヤルするための方法をユーザがいくつも覚えておく必要がありません。

たとえば、任意のオンネット ロケーションから 1234 をダイヤルすると電話 A に到達するとします。この場合、発信側の電話が同じオフィスまたは別のサイトのどちらにあっても、企業のダイヤル プランは定型と見なすことができます。

企業のサイト数が少ない場合は、このアプローチを容易に採用できます。企業の内線番号とサイトの数が多くなるほど、定型ダイヤル プランを設計するときに次の点が問題になってきます。

- 内線番号の数は、ダイヤル　プラン用に予定した桁数で対応できる範囲を超える場合もあります。たとえば、8,000 個（内線番号 0XXX と 9XXX を除外するものと想定）を超える内線番号が必要になった場合は、5 桁以上使用する省略ダイヤル プランが必要になります。
- オンネット省略内線番号を DID 番号と同じものにする場合、地域通信事業者から新しい DID 範囲を取得するときに、その範囲が既存のオンネット省略ダイヤルの範囲と競合することが許されなくなります。たとえば、4 桁の定型省略ダイヤル プランを使用しているシステムに、DID 範囲 415 555 1XXX があるとします。DID 範囲 650 556 1XXX の取得も検討している場合は、オンネット ダイヤリングの桁数を 5 に増やすことが望ましくなります。この例では、5 桁のオンネット範囲 51XXX と 61XXX は重複することがありません。

- ほとんどのシステムでは、一定の範囲をオフネット アクセス コードとオペレータ ダイヤリング用に除外する必要があります。9 と 0 が予約コードになっているシステムで、9 または 0 で始まるオンネット内線番号ダイヤリングに対応できるダイヤル プランは、(定型もそれ以外も) 存在しません。つまり、ダイヤル プランで最初の数字として 9 または 0 を使用する必要がある場合は、最初の数字が 9 または 0 である DID 範囲を使用できません。たとえば、5 桁の省略ダイヤル プランを使用する場合、DID 範囲 415 559 XXXX（およびこのサブセット）は使用できません。この例では、代替策として、省略ダイヤリングの長さを 6 桁以上に増やすか、末尾の 5 桁が 9 で始まる DID 範囲を使用しないようにするという方法があります。

桁数を選定し、必要な範囲（たとえば、9 または 0 で始まる範囲）を除外したら、残りのダイヤリング スペースをすべてのサイトに分配する必要があります。

ほとんどのシステムでは、2 つの範囲を除外する必要があります。このため、ダイヤル範囲の先頭となる可能性が残っている数字は、8 つです。表 10-1 では、一般的な 4 桁の定型ダイヤル プランにおける、ダイヤリング スペースの分配例を示しています。

表 10-1　一般的な 4 桁定型ダイヤル プランでの番号の分配

範囲	用途	DID 範囲	DID 以外の範囲
0XXX	除外（0 はオフネット アクセス コードとして使用される）		
1XXX	サイト A の内線番号	418 555 1XXX	適用対象外
2XXX	サイト B の内線番号	919 555 2XXX	適用対象外
3XXX	サイト C の内線番号	415 555 30XX	3[1-9]XX
4[0-4]XX	サイト D の内線番号	613 555 4[0-4]XX	適用対象外
4[5-9]XX	サイト E の内線番号	450 555 4[5-9]XX	適用対象外
5XXX	サイト A の内線番号	418 555 5XXX	適用対象外
6XXX	サイト F の内線番号	514 555 6[0-8]XX	69XX
7XXX	将来的にサポート	XXX XXX 7XXX	7XXX
8XXX	将来的にサポート	XXX XXX 8XXX	8XXX
9XXX	除外（9 はオフネット アクセス コードとして使用される）		

表 10-1 の例では、さまざまなサイトが次の方法に従って番号を割り当てられています。

- サイト A（企業の本社）では、必要な内線番号が 1,000 個を超えるため、2 つの番号範囲（1XXX と 5XXX）全体を確保しています。対応する DID 範囲も、このサイトの地域通信事業者から取得する必要があります。
- サイト B は、1 つの範囲全体（2XXX）を割り当てられているため、内線番号を 1,000 個まで使用できます。
- サイト C も 1 つの範囲全体を割り当てられていますが、100 個の DID 内線番号（415 555 30XX）と 900 個の DID 以外の内線番号に分割されています。DID 内線番号がさらに必要になった場合は、DID 以外の範囲にある、まだ割り当てられていない番号を使用することができます。
- サイト D と E は、4XXX 範囲からそれぞれ 500 個ずつ番号を割り当てられています。対応する DID 範囲は、それぞれのサイトの 4XXX 範囲の部分と一致している必要があります。DID 範囲がサイトごとに異なっているため（おそらく、別の公衆網サービス プロバイダーから取得したことが原因）、サイト間で範囲を分割するには、密接な連携作業が必要です。特定の範囲内で割り当てられるサイトの数が多くなるほど、範囲全体をすべて使用することは困難になり、場合によっては不可能になります。
- サイト F の範囲は、900 個の DID 番号（6[0-8]XX）と 100 個の DID 以外の番号（69XX）に分割されています。
- 範囲 7XXX と 8XXX は、将来の使用に備えて予約されています。

新しいダイヤル プランを実装する場合、プラン立案者の主な目標の 1 つは、電話番号の変更が必要になるのを避けることです。また、既存の電話システムで内線番号範囲が重複している場合、過去に問題がなくても、定型ダイヤル プランでは許容されない場合があります。

可変長のオンネット ダイヤル プラン

サイトの数が多いシステムや、サイトの内線番号範囲が重複しているシステムでは、次の特性を備えた可変長ダイヤル プランを使用すると効果的です。

- サイトの内部では、オンネット内線番号へのコールに対して、省略ダイヤリング（4 桁の内線番号など）を引き続き使用できる。
- サイト間では、ユーザはアクセス コードをダイヤルし、次にサイト コードと宛先のオンネット内線番号をダイヤルする。
- オフネット コールの場合は、アクセス コードの次に公衆網番号をダイヤルする必要がある。

アクセス コードとダイヤル コードを使用すると（表 10-2 を参照）、定型省略ダイヤル プランであれば重複となる内線番号を、オンネット ダイヤル プランで区別できるようになります。

表 10-2　サイト コードの一般的な使用方法

サイト コード	範囲	用途	DID 範囲	DID 以外の範囲
1	1XXX	サイト A の内線番号	418 555 10XX	1[1-9]XX
2	1XXX	サイト B の内線番号	919 555 1XXX	適用対象外
3	1XXX	サイト C の内線番号	907 555 1XXX	適用対象外

表 10-2 では、サイト A、B、C はそれぞれ独自に 4 桁範囲 1XXX を割り当てられています。従来のテレフォニー システムでは、サイト A からサイト B へのコールはオフネット コールとしてルーティングする必要がありました。新しいシステムでは、これらのコールをオンネット コールとしてダイヤルできます。

サイト A からは、ユーザは 1234 をダイヤルするだけで内線番号 1234 に到達できます。一方で、サイト B からサイト A の内線番号 1234 に対して、サイト B にある内線番号 1234 と競合することなく到達するには、ダイヤル プラン側で対応する必要があります。このため、各サイトにサイト コードが割り当てられています。

サイト B から、単にサイト A のコードを目的の内線番号と組み合せてダイヤルすることだけでは不十分です。この場合、11234 はサイト B の内線番号 1123 と部分的に重複しているため、桁間タイムアウトの問題が発生します。代わりに、サイト間オンネット アクセス コードとして 8 を割り当てると、サイト B から 81234 をダイヤルしてサイト A の内線番号 1234 に到達できるようになります。

オンネットのオフサイト内線番号にダイヤルするために必要な桁数は、次の要素によって決まります。

- サイト間アクセス コードに使用する 1 桁
- サイト コードに使用する N 桁（N は、必要となるサイト コードの数に見合う数値。たとえば、システムに 13 のサイトがある場合、サイト コードには少なくとも 2 桁が必要）
- 宛先サイトのローカル ダイヤル プランで必要となる桁数

たとえば、システムに 75 のサイトがあり、各サイトが 4 桁の省略ダイヤリングを使用している場合は、8 + SS + XXXX という形式が必要になります。8 はオンネット アクセス コード、SS は 2 桁のサイト コード、XXXX は 4 桁の内線番号で、合計 7 桁です。

オンネットとオフネットのアクセス コード

ほとんどの企業のテレフォニー システムでは、オフネットの宛先にコールを振り分けるためのオフネット アクセス コード専用として、1 つの数字（たとえば 9）を割り当てることが一般的です。可変長のオンネット ダイヤル プランでは、他のサイトにあるオンネット内線番号宛てのコールをダイヤルするために、オンネット アクセス コードとして、振り分け用の数字（たとえば 8）がもう 1 つ必要です。これらの 2 つのアクセス コードをオペレータ アクセス コード（たとえば 0）とともに使用するので、ダイヤル ストリングの先頭の数字となる可能性のある 10 個の数字からは、3 つが暗黙的に除外されます。この制限事項は、次の両方の理由から、好ましいものとは言えません。

- ユーザは、オンネットとオフネットの違いを理解し、適切なアクセス コードを選択する必要がある。
- 3 つのダイヤリング範囲全体を除外することによって、著しい制約や、一部の割り当て済み内線番号範囲との競合が生じる恐れがある。たとえば、サイトですでに 8 で始まる省略ダイヤリング範囲を使用している場合、この数字をアクセス コードとして使用するには、変更作業が必要になります。

定型オフネット アクセス コード（たとえば 9）をすでにすべてのサイトで使用しているシステムでは、同じコードをオフネットとオンネットの両方のオフサイト宛先に使用することをお勧めします。このアプローチには、主に次の 2 つの暗黙的要件があります。

- 部分的な重複や待ちが発生することを避けるには、アクセス コードの後に続く桁数を一定にする必要がある。
- テレフォニー システムは、ダイヤルされるすべてのオンネット番号をオフネット番号として認識し、IP ネットワーク経由でルーティングできる必要がある。このタスクは、Cisco Unified CallManager クラスタが 1 つしかない小規模システムの場合は単純ですが、複数の Cisco Unified CallManager クラスタがある大規模システムでは複雑なものになります。

事前の計画

IP ベースのシステムを実装するときは、ユーザの普段の操作手順を変更する必要が生じる場合もあります。新しいシステムのプランニングでは、この実装をできる限りユーザから見えないようにすることが望ましいのですが、それぞれ別のテレフォニー システム上にあった複数のサイトの統合に対応するには、ダイヤリング手順の調整が必要になることもあります。たとえば、企業全体にわたる新しいグローバルなダイヤル プランに対応するには、ユーザが他のサイトにいる別のユーザに到達する方法、サイト内コールに使用している桁数、ときには内線番号までも変更することが必要な場合もあります。ユーザが何度もダイヤル プラン変更を経験することを避けるには、企業規模の拡大を見越しておくようにします。企業が成長すると、複数のダイヤリング リージョンへのサイトの追加、オンネット内線番号の必要数の増加、公衆網番号の再割り当て（たとえば、エリア コードの分割など）、他国への事業展開が発生する可能性があります。

ダイヤル プランの要素

この項では、Cisco Unified Communication システムに含まれている次のダイヤル プラン要素について、設計と設定のガイドラインを示します。

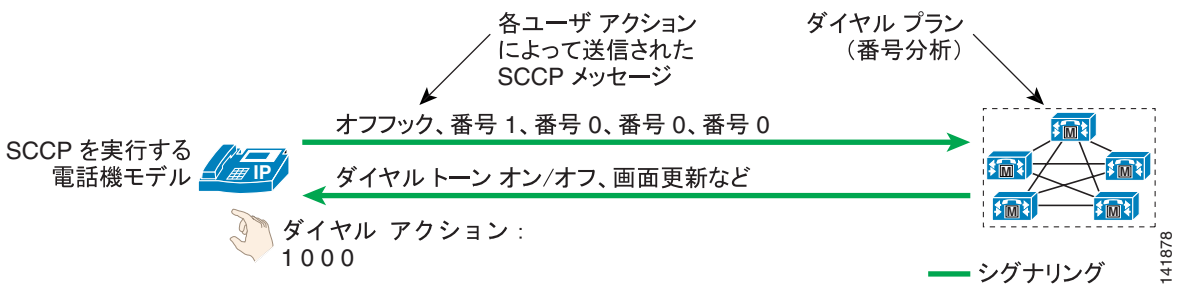
- SCCP 電話機でのユーザ入力（P.10-9）
- タイプ A の SIP 電話機でのユーザ入力（P.10-10）
- タイプ B の SIP 電話機でのユーザ入力（P.10-12）
- SIP ダイヤル規則（P.10-14）
- Cisco Unified CallManager におけるコール ルーティング（P.10-16）
- Cisco Unified CallManager におけるコール特権（P.10-22）
- Cisco Unified CallManager における番号操作（P.10-27）
- Automated Alternate Routing（P.10-28）
- エクステンション モビリティ（P.10-31）
- ハント リストと回線グループ（P.10-33）
- H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング（P.10-39）
- H.323 ダイヤル ピアを使用する Cisco IOS のコール特権（P.10-52）
- H.323 ダイヤル ピアを使用する Cisco IOS での番号操作（P.10-55）

SCCP 電話機でのユーザ入力

SCCP を使用する IP Phone は、すべてのユーザ入力イベントをただちに Cisco Unified CallManager に報告します。たとえば、ユーザがオフフックにするとすぐに、その電話機が登録されている Cisco Unified CallManager サーバに電話機からシグナリング メッセージが送信されます。電話機は 1 つの端末と考えることができ、Cisco Unified CallManager サーバに設定されたダイヤル プランによって、ユーザ入力に起因するすべての決定がその端末で下されます。

その他のユーザ イベントが電話機で検出されると、そのイベントは個別に Cisco Unified CallManager にリレーされます。オフフックして 1000 をダイヤルしたユーザは、電話機から Cisco Unified CallManager に 5 つの独立したシグナリング イベントをトリガすることになります。その結果としてユーザに提供されるフィードバック、たとえば画面メッセージ、ダイヤル トーンの再生、2 次ダイヤル トーン、リングバック、リオーダーなどは、Cisco Unified CallManager がダイヤル プラン設定に基づいて電話機へ発行するコマンドです（図 10-1 を参照）。

図 10-1　SCCP 電話機でのユーザ入力とフィードバック



SCCP を実行する IP Phone 上にダイヤル プラン情報を設定する必要はなく、また設定できません。ダイヤル プラン機能は、ユーザ入力が収集されたときのダイヤリング パターンの認識も含めて、すべて Cisco Unified CallManager クラスタに含まれています。

ユーザのダイヤルしたパターンが Cisco Unified CallManager に拒否された場合は、そのパターンが Cisco Unified CallManager の番号分析でベストマッチになるとすぐに、そのユーザに対してリオーダー トーンが再生されます。たとえば、1 分刻みで課金される番号計画エリア（または市外局番）976 へのコールがすべて拒否される場合は、ユーザが 91976 をダイヤルするとすぐに、そのユーザの電話機にリオーダー トーンが送信されます。

タイプ A の SIP 電話機でのユーザ入力

この章では説明のため、タイプ A 電話機として Cisco Unified IP Phone 7905、7912、7940、および 7960 を定義します。タイプ A 電話機はタイプ B 電話機と動作が少し異なり、タイプ B 電話機では Keypad Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（P.10-12 の「タイプ B の SIP 電話機でのユーザ入力」を参照）。

SIP を使用するタイプ A の IP Phone には、次の 2 つの異なる動作モードがあります。

- 電話機に SIP ダイヤル規則が設定されていない場合（P.10-10）
- 電話機に SIP ダイヤル規則が設定されている場合（P.10-11）

電話機に SIP ダイヤル規則が設定されていない場合

図 10-2 は、電話機にダイヤル プラン規則が設定されていない SIP タイプ A 電話機の動作を表しています。このモードでは、電話機はユーザが # キーを押すか Dial ソフトキーを押すまで、すべてのユーザ入力イベントを蓄積します。この機能は、多くの携帯電話で使用されている「送信」ボタンによく似ています。たとえば、内線 1000 にコールするユーザは、1、0、0、0 を押した後に Dial ソフトキーまたは # キーを押す必要があります。その後、電話機は Cisco Unified CallManager に SIP INVITE メッセージを送信し、内線 1000 へのコールの要求を示します。コールが Cisco Unified CallManager に到達すると、その電話機のダイヤル プラン設定に従います。その設定には、Cisco Unified CallManager のダイヤル プランに実装されているすべてのサービス クラスおよびコール ルーティング ロジックが含まれます。

図 10-2　ダイヤル規則が設定されていないタイプ A の SIP 電話機でのユーザ入力とフィードバック

ユーザが番号をダイヤルした後に Dial ソフトキーや # キーを押さなかった場合、電話機は桁間タイムアウト（デフォルトでは 10 秒）だけ待ってから、SIP INVITE メッセージを Cisco Unified CallManager に送信します。図 10-2 の例では、1、0、0、0 をダイヤルして桁間タイムアウトの時間だけ待つと、電話機は 10 秒後に内線 1000 にコールをつなぎます。

（注） ユーザが Redial ソフトキーを押した場合は、ただちに処理が行われるため、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません。

ユーザが Cisco Unified CallManager に拒否されるパターンをダイヤルした場合、そのユーザはパターン全体を入力して Dial キーを押し、INVITE メッセージを Cisco Unified CallManager に送信した後でなければ、コールが拒否されたという通知（リオーダー トーン）は発信元に送信されません。たとえば、NPA 976 へのコールが拒否される場合は、919765551234 をダイヤルして Dial を押してから、リオーダー トーンが再生されます。

電話機に SIP ダイヤル規則が設定されている場合

SIP ダイヤル規則を使用すると、ユーザがダイヤルしたパターンを電話機が認識できます。認識作業が完了すると、SIP INVITE メッセージが Cisco Unified CallManager に自動的に送信され、ユーザは Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（詳細については、P.10-14 の「SIP ダイヤル規則」を参照してください）。

たとえば、企業の支店で同一支店内の電話機間のコールに 4 桁の内線番号をダイヤルする必要がある場合は、4 桁のパターンを認識するように電話機を設定すれば、ユーザが Dial キーを押したり、桁間タイムアウトを待ったりする必要がありません（図 10-3 を参照）。

図 10-3　ダイヤル規則が設定されているタイプ A の SIP 電話機でのユーザ入力とフィードバック

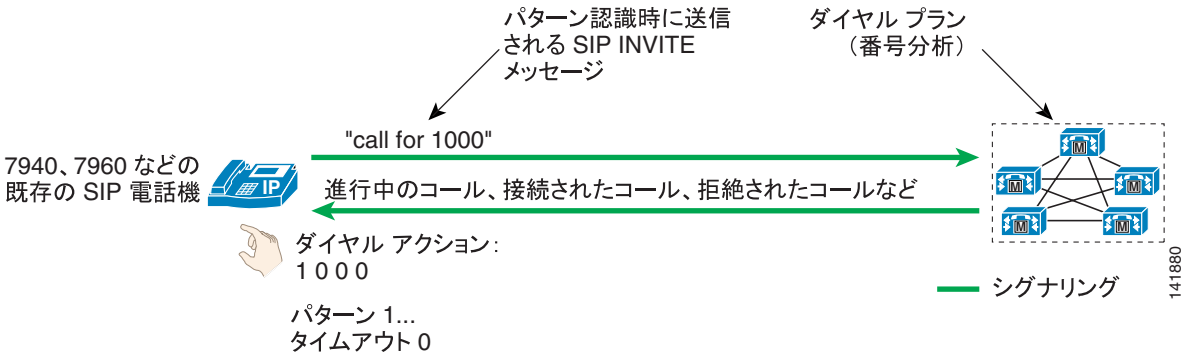


図 10-3 で、電話機は 1 で始まる 4 桁のパターンをすべて認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、SIP INVITE メッセージがすぐに Cisco Unified CallManager に送信され、ユーザが Dial キーを押す必要はありません。

SIP ダイヤル規則を使用するタイプ A 電話機では、電話機上に明示的に設定されていないパターンをダイヤルすることもできます。ダイヤルしたパターンが SIP ダイヤル規則と一致しない場合、ユーザは Dial キーを押すか、桁間タイムアウトを待ちます。

特定のパターンが電話機で認識され、それが Cisco Unified CallManager によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Cisco Unified CallManager ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（最後の 4 のキーを押した後）にリオーダー トーンを受信します。

タイプ B の SIP 電話機でのユーザ入力

この章では説明のため、タイプ B 電話機として Cisco Unified IP Phone 7911、7941、7961、7970、および 7971 を定義します。タイプ B 電話機はタイプ A 電話機と動作が少し異なり、タイプ B 電話機では Keypad Markup Language（KPML）がサポートされていますが、タイプ A 電話機ではサポートされません（P.10-10 の「タイプ A の SIP 電話機でのユーザ入力」を参照）。

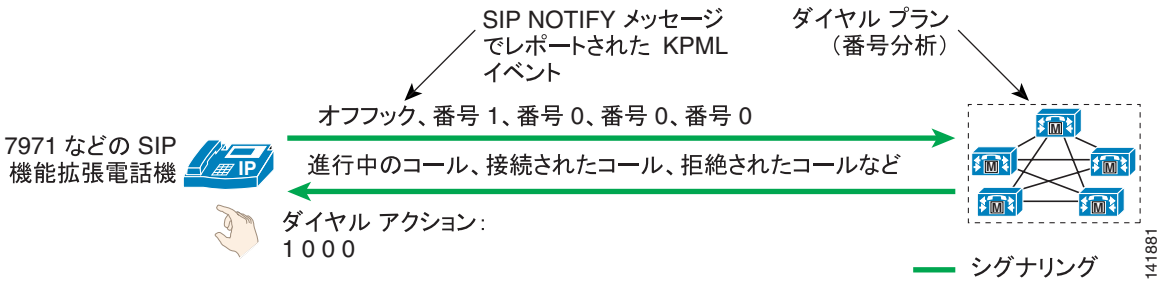
SIP を実行するタイプ B の IP Phone（Cisco Unified IP Phone 7911、7941、7961、7970、7971 など）には、次の 2 つの異なる動作モードがあります。

- 電話機に SIP ダイヤル規則が設定されていない場合（P.10-12）
- 電話機に SIP ダイヤル規則が設定されている場合（P.10-13）

電話機に SIP ダイヤル規則が設定されていない場合

タイプ B の IP Phone は、Keypad Markup Language（KPML）に基づいて、ユーザによるキー操作を報告する機能を提供します。ユーザ入力イベントの 1 つ 1 つにより、Cisco Unified CallManager に対して KPML をベースとした独自のメッセージが生成されます。ユーザの個々の操作をすぐに Cisco Unified CallManager にリレーするという点では、この操作モードは SCCP を実行している電話機の操作モードと非常によく似ています（図 10-4 を参照）。

図 10-4　ダイヤル規則が設定されていないタイプ B の SIP 電話機でのユーザ入力とフィードバック



ユーザのすべてのキー操作によって、Cisco Unified CallManager に対する SIP NOTIFY メッセージがトリガされることで、ユーザが押したキーに対応する KPML イベントが報告されます。このメッセージ機能により、Cisco Unified CallManager の番号分析はユーザが合成する部分パターンをその都度認識し、無効な番号がダイヤルされるとすぐにリオーダー トーンを再生するなど、適切なフィードバックを提供することができます。

ダイヤル規則なしに SIP を実行しているタイプ A の IP Phone とは異なり、タイプ B の SIP 電話機には、ユーザ入力の終わりを示す Dial キーがありません。図 10-4 では、1000 をダイヤルするユーザは、最後の 0 をダイヤルした後、Dial キーを押さなくても、コールプログレストーン（リングバック トーンかリオーダー トーン）を受け取ります。この動作は、SCCP プロトコルを実行する電話機のユーザ インターフェイスとの整合性がとれています。

電話機に SIP ダイヤル規則が設定されている場合

タイプ B の IP Phone では、ダイヤルされたパターンの認識が電話機によって行われるように SIP ダイヤル規則を設定できます（図 10-5 を参照）。

図 10-5　ダイヤル規則が設定されているタイプ B の SIP 電話機でのユーザ入力とフィードバック

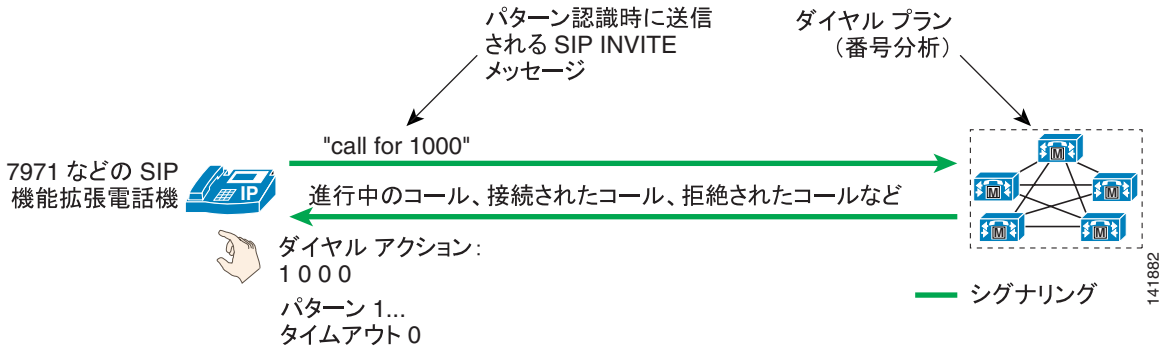


図 10-5 で、電話機は 1 で始まる 4 桁のパターンをすべて認識するように設定され、それに対応するタイムアウト値が 0 に設定されています。このパターンと一致するすべてのユーザ入力操作によって、Cisco Unified CallManager への SIP INVITE メッセージの送信がトリガされます。

（注） SIP ダイヤル規則がタイプ B の IP Phone に実装されるとすぐに、KPML ベースのダイヤリングは無効になります。ユーザが SIP ダイヤル規則と一致しない番号ストリングをダイヤルした場合は、個々の桁のイベントが、どれも Cisco Unified CallManager にリレーされません。その代わり、ダイヤリングが完了すると（桁間タイムアウトの発生後）、ダイヤルされた番号全体が Cisco Unified CallManager にまとめて送信されます。

SIP ダイヤル規則を使用するタイプ B 電話機では、電話機上に明示的に設定されていないパターンをダイヤルする方法は 1 つだけです。ダイヤルされたパターンが SIP ダイヤル規則と一致しない場合、ユーザは桁間タイムアウトを待った後でなければ、Cisco Unified CallManager に SIP NOTIFY メッセージが送信されません。タイプ A の IP Phone とは異なり、タイプ B の IP Phone にはオンフック ダイヤルを使用した場合を除いて、ダイヤリングの終わりを示す Dial キーがありません。その場合、ユーザはいつでも「Dial」キーを押すことで、ダイヤルしたすべての桁の Cisco Unified CallManager への送信をトリガできます。

（注） タイプ B 電話機を SRST ルータに登録した場合、設定した SIP ダイヤル規則は無効になります。

特定のパターンが電話機で認識され、それが Cisco Unified CallManager によってブロックされる場合、ユーザがダイヤル ストリング全体をダイヤルした後でなければ、コールがシステムで拒否されたという通知を受け取ることができません。たとえば、電話機に 919765551234 という形式でダイヤルされたコールを認識するように SIP ダイヤル規則が設定され、そのコールが Cisco Unified CallManager ダイヤル プランによってブロックされる場合、ユーザはダイヤリングの終了時（4 のキーを押した後）にリオーダー トーンを受信します。

SIP ダイヤル規則

Cisco Unified CallManager には、ユーザ入力が収集されたときに電話機でパターン認識を実行できるように、SIP ダイヤル規則機能が備わっています。たとえば、誰もが知る 911 というパターンを認識したら Cisco Unified CallManager にメッセージを送信し、すぐに緊急コールが開始されるように電話機を設定できます。それと同時に、ユーザが国際電話番号の可変長のパターンを入力できるようにも設定できます。

注意すべき重要な点は、SIP ダイヤル規則を使用して電話機にパターン認識を設定しても、Cisco Unified CallManager のサービス クラスとルート プランの設定の方が優先されることです。ある電話機が長距離通話のパターンを認識するように設定されていても、その電話機がローカル コールのみを許可するサービスクラスに割り当てられていると、Cisco Unified CallManager がそのコールをブロックします。

SIP ダイヤル規則には、それらの規則を設定する電話機のモデルに基づいて、次の 2 つのタイプがあります。

- 7905_7912（Cisco Unified IP Phone 7905 および 7912 に使用）
- 7940_7960_OTHER（上記以外のすべての IP Phone モデルに使用）

ダイヤル規則の一部として使用できる基本的なダイヤル パラメータは、次の 4 つです。

- Pattern

  このパラメータは、パターンの実際の数値表現です。数字、ワイルドカード、2 次ダイヤル トーンを再生する命令を含めることができます。次の表は、2 つのタイプのダイヤル規則について、値とその効果を示しています。

	ダイヤル規則のタイプ	
パターン	7905_7912	7940_7960_OTHER
数字の 0 ～ 9	対応する数字。	対応する数字。
.	任意の数字（0 ～ 9）と一致します。	任意の文字（0 ～ 9、*、#）と一致します。
-	続けて追加の数字が入力される場合があることを示します。個々の規則の末尾に置く必要があります。	適用対象外
#	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は # キーが入力終了として認識されます。たとえば、9>#... と指定すると、9 が押された後は、いつでも # 文字が認識されます。	適用対象外
t*n*	*n* 秒のタイムアウト値を示します。たとえば、1…t3 は 1000 と一致し、3 秒後に Cisco Unified CallManager への Invite の送信をトリガします。	適用対象外
r*n*	最後の文字を *n* 回繰り返します。たとえば、1.r3 は 1… に相当します。	適用対象外
S	パターンに修飾子 S が含まれていると、このパターン以後の他のダイヤル規則がすべて無視されます。実質的に、S によって規則照合が終了します。	適用対象外

パターン	ダイヤル規則のタイプ	
	7905_7912	7940_7960_OTHER
*	入力終了キー。ダイヤル規則の中に文字位置を示す > 文字を置くと、その文字位置以後は * キーが入力終了として認識されます。	1 文字以上と一致します。たとえば、パターン 1* は 10、112、123456 などと一致します。
,	適用対象外	電話機で 2 次ダイヤル トーンを再生します。たとえば、8,.... と指定すると、ユーザには 8 を押した後に 2 次ダイヤル トーンが聞こえます。

- IButton

  このパラメータは、ダイヤル パターンの適用対象となるボタンを指定します。ユーザが回線ボタン 1 でコールを開始しようとしている場合は、ボタン 1 用に指定されたダイヤル パターンのみが適用されます。このオプション パラメータを設定しなかった場合、ダイヤル パターンは電話機のすべての回線に適用されます。このパラメータは、Cisco SIP IP Phone モデル 7940、7941、7960、7961、7970、および 7971 のみに適用されます。ボタン番号は、画面横にあるボタンの上から下の順に対応し、一番上のボタンが 1 になります。

- Timeout

  このパラメータは、システムがタイムアウトになり、ユーザが入力した番号にダイヤルするまでの時間を秒単位で指定します。ダイヤルされた番号がすぐにダイヤルされるようにするには、0 を指定します。7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータを省略した場合は、電話機のデフォルトの桁間タイムアウト値（デフォルトは 10 秒）が使用されます。

- User

  このパラメータは、ダイヤルされた番号に自動的に追加されるタグを表します。有効な値は、**IP**（Cisco Unified CallManager 以外の SIP コール エージェントが配置される場合）と **Phone** です。7940_7960_OTHER ダイヤル規則にのみ適用されます。このパラメータはオプションであり、Cisco Unified CallManager が唯一のコール エージェントとなる配置では省略してください。

（注） Cisco Unified IP Phone 7905 および 7912 は、パターンを SIP ダイヤル規則内で作成された順に選択します。これに対し、その他の電話機モデルでは、最長一致のパターンが選択されます。次の表は、ユーザが 95551212 をダイヤルした場合に選択されるパターンを示しています。

SIP ダイヤル規則	7905_7912	7940_7960_OTHER
…….. 9…….	最初に一致するパターンの ……. が選択されます。	最長一致パターンの 9…… が選択されます。

Cisco Unified CallManager におけるコール ルーティング

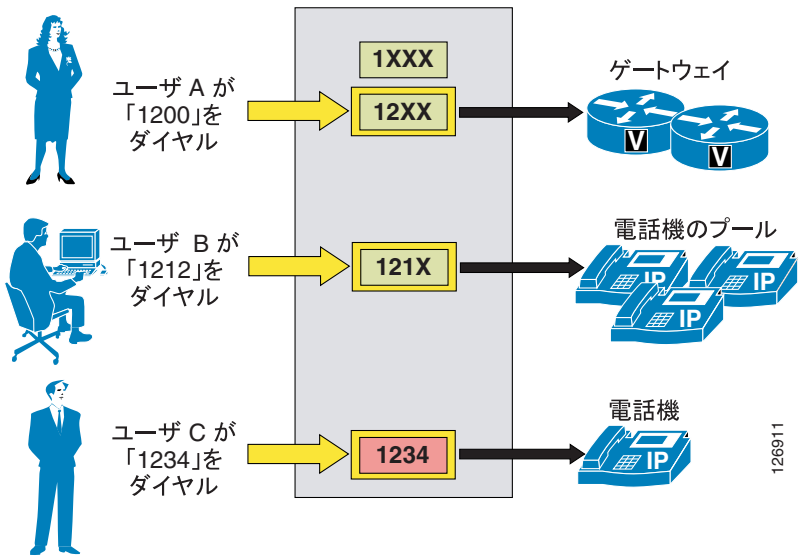
Cisco Unified CallManager 内に設定されるダイヤリング宛先は、すべて内部のコール ルーティング テーブルにパターンとして追加されます。このような宛先としては、IP Phone 回線、ボイスメール ポート、ルート パターン、トランスレーション パターン、および CTI ルート ポイントがあります。

番号がダイヤルされると、Cisco Unified CallManager は closest-match ロジックを使用し、コール ルーティング テーブルにあるすべてのパターンの中から一致パターンを選択します。一致している可能性のあるパターンが複数ある場合は、次の基準に基づいて宛先パターンを選択します。

- ダイヤルされたストリングに一致するもの。
- ポテンシャルマッチパターンのうち、ダイヤルされたストリング以外にマッチするパターンが最も少ないもの。

たとえば、図 10-6 の場合を考えます。ここでは、コール ルーティング テーブルにパターン 1XXX、12XX、および 1234 が保持されています。

図 10-6　Cisco Unified CallManager のコール ルーティング ロジックの例



ユーザ A がストリング 1200 をダイヤルすると、Cisco Unified CallManager は、この番号をコール ルーティング テーブル内のパターンと比較します。この場合は、一致する可能性のあるパターンが 2 つあります（1XXX と 12XX）。両方ともダイヤル ストリングに一致していますが、1XXX は合計 1,000 個のストリングに一致する一方で（1000 ～ 1999）、12XX は 100 個のストリングに一致します（1200 ～ 1299）。したがって、12XX がこのコールの宛先として選択されます。

ユーザ B がストリング 1212 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、121X に一致するストリングは 10 個しかありません。したがって、このパターンがコールの宛先として選択されます。

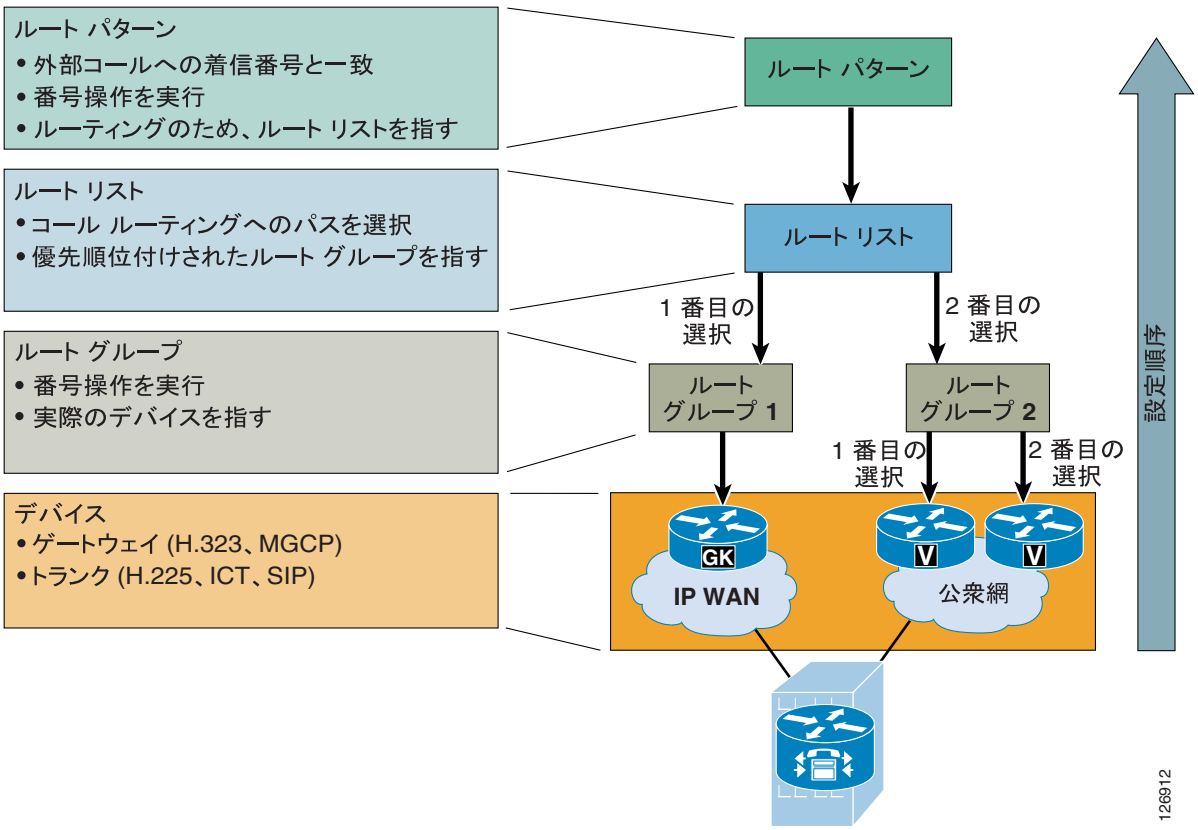
ユーザ C がストリング 1234 をダイヤルした場合、一致する可能性のあるパターンは 3 つあります（1XXX、12XX、1234）。上で説明したように、1XXX に一致するストリングは 1,000 個あり、12XX に一致するストリングは 100 個あります。しかし、1234 に一致するストリングは 1 個しかありません（ダイヤルされたストリング）。したがって、このパターンがコールの宛先として選択されます。

(注)

Cisco Unified CallManager Release 4.0 以降でディレクトリ番号（DN）を設定すると、それぞれのデバイス（IP Phone など）が登録済みかどうかにかかわらず、その番号はコール ルーティング テーブルに配置されます。この動作は、これより前の Cisco Unified CallManager バージョンとは異なります。旧バージョンでは、パターンがコール ルーティング テーブルに追加されるのは、それぞれのデバイスが登録済みの場合のみでした。この仕様変更によって、アプリケーション（およびそのプライマリ パターン）が未登録である場合、セカンダリの一致パターンを利用してフェールオーバー機能を提供することができなくなりました。プライマリ パターンがコール ルーティング テーブルに必ず存在するため、セカンダリ パターンに一致するかどうかは検索されません。ただし、CTI ルート ポイントなどのプライマリ パターンの Forward Busy フィールドを使用して、フェールオーバーと同じ効果を得ることは可能です。Cisco Unified CallManager Release 4.0 以降では、このフィールドでワイルドカードを使用できるためです。

Cisco Unified CallManager は、同じクラスタ内の宛先にコールをルーティングする方法を自動的に「習得」します。公衆網ゲートウェイ、H.323 ゲートキーパー、またはその他の Cisco Unified CallManager クラスタなどの外部宛先の場合、外部ルート コンストラクト（次の項で説明）を使用して、明示的にルーティングを設定する必要があります。このコンストラクトは、3 層式のアーキテクチャに基づいています。このアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。Cisco Unified CallManager は、外部ダイヤル ストリングと一致する設定済みルート パターンを検索し、それを使用して、対応するルート リストを選択します。ルート リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、ルート グループと呼ばれ、従来の PBX でトランク グループと呼ばれていたものに非常によく似ています。図 10-7 では、Cisco Unified CallManager 外部ルート コンストラクトの 3 層式アーキテクチャを示しています。

図 10-7　外部ルート パターンのアーキテクチャ



次の各項では、Cisco Unified CallManager の外部ルート コンストラクトの個々の要素について説明します。

- ルート パターン（P.10-18）
- ルート リスト（P.10-21）
- ルート グループ（P.10-21）
- ルート グループ デバイス（P.10-22）

ルート パターン

ルート パターンは、コールを外部エンティティにルーティングするために Cisco Unified CallManager で設定された、数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ルート パターンでは、コールをルーティングするゲートウェイを直接指すことも、ルート リストを指すこともできます。ルート リストはルート グループを指しており、最終的にゲートウェイを指します。

ルート パターン、ルート リスト、およびルート グループ コンストラクトとを完全パスで指定するようにシスコは強くお勧めします。その理由は、この構造を使用するとコール ルーティング、番号操作、および将来のダイヤル プランの拡張を最も柔軟に行うことができるからです。

@ ワイルドカード

- @ ワイルドカードは、特殊なマクロ関数であり、特定の国の番号計画全体を表す一連のパターンに拡張されます。たとえば、フィルタ処理されていない単一のルート パターン（たとえば、9.@）を北米番号計画を使用して設定すると、実際には、Cisco Unified CallManager の内部ダイヤル プラン データベースに 166 個の個別ルート パターンが追加されます。
- その他の国別番号計画を受け入れるように Cisco Unified CallManager を設定できます。この作業が完了すると、Route Pattern 設定ページの Numbering Plan フィールドで選択した値に応じて、同じ Cisco Unified CallManager クラスタ内で、複数の番号計画に対して @ ワイルドカードを使用できるようになります。詳細については、次の Web サイトで入手可能な『*Cisco Unified CallManager Dial Plan Deployment Guide*』を参照してください。

  http://www.cisco.com/en/US/products/sw/voicesw/ps5629/prod_maintenance_guides_list.html
- @ ワイルドカードは、いくつかの中小規模の配置では十分に実務で使用できますが、大規模な配置では、管理とトラブルシューティングが困難になる可能性があります。これは、@ ワイルドカードを利用する場合、ルート フィルタを使用して、管理者が特定のパターンをブロックする必要があるためです（P.10-18 の「ルート フィルタ」を参照してください）。

ルート フィルタ

- ルート フィルタは、@ ワイルドカードによって作成されるルート パターン数を減らすために、@ ルート パターンと一緒にのみ使用します。
- ルート フィルタと一緒に入力する論理式は、NOT-SELECTED フィールドを除いて、最大 1024 文字にすることができます。
- ルート フィルタ内の論理文節数が増えるにつれて、設定ページのリフレッシュ時間も増え、容認できないほど長くなる場合があります。
- 大規模な配置の場合、@ ワイルドカードとルート フィルタではなく、明示ルート パターンを使用してください。この方法を利用すると、管理とトラブルシューティングも容易になります。これは、Cisco Unified CallManager で設定されているすべてのパターンが、Route Pattern 設定ページから簡単に参照できるからです。

国際および可変長ルート パターン

- 国際間の宛先は、通常、任意の桁数を表す！ワイルドカードを使用して設定されます。たとえば、北米では通常、国際コール用にルート パターン 9.011! が設定されています。欧州諸国のほとんどでは、0.00! ルート パターンを使用することで同じ結果が得られます。

- ! ワイルドカードは、ダイヤルされる番号の長さが変化する国では配置にも使用されます。このような場合、Cisco Unified CallManager は、ダイヤルがいつ完了するかわからないので、コールの送信前に 15 秒待機します。この遅延は、次の方法のいずれかで短縮できます。
  - ダイヤルの終わりを指定する T302 タイマー（サービス パラメータ TimerT302_msec）の値を減らします。ただし、ユーザがダイヤルを終了する前のコールの早期送信を防止するために、4 秒以上に設定します。
  - # ワイルドカードで終了する同じパターンのルートパターンを設定し（たとえば、北米の場合 9.011!#、欧州の場合 0.00!#）、ダイヤルの終わりを示すために # をダイヤルするようにユーザに指示します。この処置は、携帯電話で送信ボタンを押すことに相当します。

重複送信と重複受信

国内の番号計画をスタティック ルート パターンで定義することが難しい国では、Cisco Unified CallManager に重複送信および重複受信を設定することができます。

重複送信とは、エンドユーザのダイヤルする数字を Cisco Unified CallManager で収集しながら、数字がダイヤルされると同時に公衆網に渡すことを意味します。Cisco Unified CallManager Release 4.0 以降で重複送信を使用可能にするには、Route Pattern Configuration ページの Allow Overlap Sending チェックボックスをオンにします。これより前の Cisco Unified CallManager リリースで重複送信を使用可能にするには、SendingCompleteIndicator サービス パラメータを False に設定します。ルート パターンには、公衆網アクセス コード（たとえば、北米では 9、欧州諸国の多くでは 0）を含める場合のみです。

重複受信とは、ダイヤルされる数字を PRI 公衆網ゲートウェイから Cisco Unified CallManager で 1 つずつ受信し、ストリングのダイヤルが完了するまで待機し、その後でコールを内部宛先にルーティングすることを意味します。Cisco Unified CallManager Release 3.3(3) 以降で重複受信を使用可能にするには、OverlapReceivingFlagForPRI サービス パラメータを Trule に設定します。これより前の Cisco Unified CallManager リリースでは、パラメータ名は OverlapReceivingForPriFlag です。

ルート パターンにおける番号操作

- 番号操作は、ルート パターンではなく、ルート グループのみで設定してください。
- ルート グループでの番号操作は、ルート パターンで行われた番号操作を完全に上書きします。
- ルート パターンで番号操作を設定する場合、コール詳細レコード（CDR）は、番号操作が行われた後のダイヤル番号を記録します。ルート グループだけで番号操作を設定する場合、CDR は、番号操作が行われる前の実際のダイヤル番号を記録します。
- 同様に、ルート パターンでの番号操作を設定すると、発信側の IP Phone ディスプレイおよび Placed Calls レジスタには、操作後の番号が示されます。ルート グループのみで番号操作を設定する場合、この操作はエンドユーザには見えなくなります。

発呼回線 ID

- 発呼回線 ID の表示は、ゲートウェイで使用可能または使用不可にすることができます。また、サイトの要件に基づいて、ルート パターンで操作することもできます。
- Use Calling Party's External Phone Number Mask オプションを選択する場合、外部コールは、コールを発信する IP Phone に指定された発呼回線 ID を使用します。このオプションを選択しない場合、Calling Party Transform Mask フィールドに指定されたマスクが、発信者番号識別の生成に使用されます。

緊急プライオリティ

- Urgent Priority チェックボックスは、一般に、パターンに一致したコールを T302 タイマーの満了を待たずにすぐルーティングする目的で使用されます。たとえば、北米でパターン 9.911 と 9.[2-9]XXXXXX が設定されている場合、ユーザが 9911 をダイヤルすると、Cisco Unified CallManager は T302 タイマーが満了するまで待機し、その後でコールをルーティングします。これは、9911 の後に数字が入力されて、9.[2-9]XXXXXX に一致する可能性があるためです。

9.911 ルート パターンについて緊急プライオリティを有効にすると、Cisco Unified CallManager はユーザが 9911 とダイヤルした直後にルーティング処理を実行し、T302 タイマーの満了までは待機しません。

- Urgent Priority チェックボックスをオンにした場合に実行されるのは、設定済みのパターンがダイヤルされた番号とのベストマッチになったとき、その直後に T302 タイマーを満了させることです。つまり、緊急パターンが他のパターンよりも高い優先順位を持っているわけではありません。P.10-16 の「Cisco Unified CallManager におけるコール ルーティング」の項で説明した closest-match ロジックは、依然として有効です。

  たとえば、ルート パターン 1XX が緊急パターンとして設定され、パターン 12! が通常のルート パターンとして設定されているとします。ユーザが 123 とダイヤルした場合、Cisco Unified CallManager は 3 番目の数字を受信した直後にはルーティング処理を実行しません。1XX は緊急パターンであっても、ベストマッチではないからです（12! が合計 10 個のパターンに一致するのに対して、1XX は 100 個のパターンに一致）。パターン 12! では、ユーザがさらに番号を入力する可能性があるため、Cisco Unified CallManager は桁間タイムアウトを待ってから、コールをルーティングする必要があります。

  別の例として、パターン 12[2-5] に緊急のマークが付けられ、12! が通常のパターンとして設定されている場合を考えてみます。ユーザが 123 とダイヤルすると、パターン 12[2-5] はベストマッチになります（12[2-5] が合計 4 個のパターンに一致するのに対し、12! は 10 個のパターンに一致）。緊急プライオリティ パターンがベストマッチなので、T302 タイマーは打ち切られ、それ以上のユーザ入力は想定されません。Cisco Unified CallManager は、パターン 12[2-5] を使用してコールをルーティングします。

コール分類

- このルート パターンを使用しているコールは、オンネットまたはオフネットのコールとして分類することができます。このルート パターンを使用すると、オフネット間でのコール転送を禁止したり、オンネット通話者がいないコンファレンス ブリッジを終了したりすることによって、料金詐欺を防止できます（これらの機能は、どちらも Cisco Unified CallManager Administration の Service Parameters を使用して制御します）。
- Allow device override チェックボックスをオンにすると、コールは、関連するゲートウェイまたはトランク上で、コール分類設定に基づいて分類されるようになります。

強制アカウント コード（FAC）

- Forced Account Codes（FAC）チェックボックスを使用すると、個々のルート パターンを使用して発信コールが制限されます。ルート パターンに対して FAC を有効にすると、ユーザは、目的のコール受信者に到達するための許可コードを入力するように要求されます。
- ユーザのダイヤルした番号が、FAC が有効になったルート パターンを通じてルーティングされるものである場合、システムは許可コードの入力を求めるトーンを再生します。コールを確立するには、ユーザ許可コードが、ダイヤルされた番号のルーティングに必要となる許可レベルにを満たしているか、そのレベルを超えている必要があります。
- コール詳細レコード（CDR）に表示されるのは、許可名のみです。許可コードは CDR には表示されません。
- FAC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。

クライアント証明書コード（CMC）

- Client Matter Code（CMC）チェックボックスを使用すると、個々のルート パターンを使用して特定番号へのコールがトラッキングされます。たとえば、企業で使用すると、特定のクライアントへのコールをトラッキングできます。
- ルート パターンに対して CMC を有効にすると、ユーザは目的の宛先に到達するためのコードを入力するように要求されます。
- ユーザのダイヤルした番号が、CMC が有効になったルート パターンを通じてルーティングされるものである場合、システムはコードの入力を求めるトーンを再生します。コールを確立するには、ユーザが正しいコードを入力する必要があります。

- クライアント証明書コードは、コール詳細レコードに表示されます。これは、クライアントの課金およびアカウンティングに関するレポートを生成するための、CDR の分析およびレポート ツールで使用できるようにするためです。
- CMC 機能は、Allow overlap sending チェックボックスがオンの場合は使用できません。
- CMC と FAC を両方とも有効にすると、ユーザは番号をダイヤルするとき、FAC の入力を求められたら入力し、次のプロンプトで CMC を入力します。

ルート リスト

ルート リストは、発信コールに使用できるパス（ルート グループ）が優先順位順に並べられたリストです。一般に、1 つのルート リストは、1 つのリモート ロケーションに関連付けられ、複数のルート パターンがそのルート リストを指定することができます。ルート リストの標準的な用途は、リモートの宛先に 2 つのパスを指定することです。この場合、第一選択のパスは、IP WAN を介したパスであり、第二選択のパスは、ローカル公衆網ゲートウェイを介したパスです。

ルート リストには次の特性があります。

- 複数のルート パターンが同一ルート リストを指すことができます。
- ルート リストは、所定の宛先への代替パスの役目をするルート グループが、優先順位順に並べられたリストです。たとえば、ルート リストを使用して最低料金選択機能をサポートすることができます。この場合、リスト内のプライマリ ルート グループが、コール当たりのコストがより低くなるようにします。プライマリ ルート グループが「all trunks busy（全トランク使用中）」状態、または IP WAN リソースの不足により使用できない場合だけ、セカンダリ ルート グループが使用されます。
- ルート リスト内の各ルート グループは、独自の番号操作を行うことができます。たとえば、ルート パターンが 9.@ であるときに、ユーザが 91 408 555 4000 をダイヤルした場合、IP WAN ルート グループは 9 1 を削除し、公衆網ルート グループは 9 だけを削除することが可能です。
- 複数のルート リストに、同じルート グループを含むことができます。ルート グループの番号操作は、そのルート グループを指定する特定のルート リストに関連しています。
- ルート パターンまたはルート グループ内で複数の番号操作を実行しようとする場合、変換が実行される順序が、変換結果の E.164 アドレスに影響を与える可能性があります。Cisco Unified CallManager は、次に示す主要なタイプの番号操作を表示されている順に実行します。
  1. 数字を破棄する
  2. 着信番号変換
  3. 数字をプレフィックスとして付加する

ルート グループ

ルート グループは、一般にゲートキーパーまたはリモート Cisco Unified CallManager クラスタとのゲートウェイ（MGCP または H.323）、H.323 トランク、または SIP プロキシへの SIP トランクである特定のデバイスを制御し、それを指定します（Cisco CallManager Release 3.2 以前では、H.323 トランクの役割は、「Anonymous Device」ゲートウェイ、および Intercluster Trunk プロトコルを使用して設定された H.323 ゲートウェイによって実行されていました）。

Cisco Unified CallManager は、割り当てられている分配アルゴリズムに従ってコールをデバイスに送信します。Cisco Unified CallManager では、トップダウン アルゴリズムと循環アルゴリズムをサポートしています。

ルート グループ デバイス

ルート グループ デバイスは、ルート グループによってアクセスされるエンドポイントであり、一般に、ゲートキーパーまたはリモート Cisco Unified CallManager とのゲートウェイまたは H.323 トランクで構成されます。次のタイプのデバイスは、Cisco Unified CallManager で設定できます。

- メディア ゲートウェイ コントロール プロトコル（MGCP）ゲートウェイ
- H.323 ゲートウェイ
- H.225 トランク、ゲートキーパー制御：ゲートキーパーを介した標準 H.323 ゲートウェイとのトランク
- クラスタ間トランク、非ゲートキーパー制御：別の Cisco Unified CallManager クラスタとの直接トランク
- クラスタ間トランク、ゲートキーパー制御：ゲートキーパーを介した他の Cisco Unified CallManager クラスタまたは H.323 ゲートウェイとのトランク
- SIP トランク：SIP プロキシへのトランク（Cisco Unified CallManager Release 4.0 以降で使用可能）

（注）　H.225 トランクとクラスタ間トランク（ゲートキーパー制御）はどちらも、相手方エンドポイントが標準 H.323 ゲートウェイであるか、Cisco Unified CallManager であるかを自動的に検出し、それに応じて H.225 または Intercluster Trunk プロトコルを選択します

Cisco Unified CallManager におけるコール特権

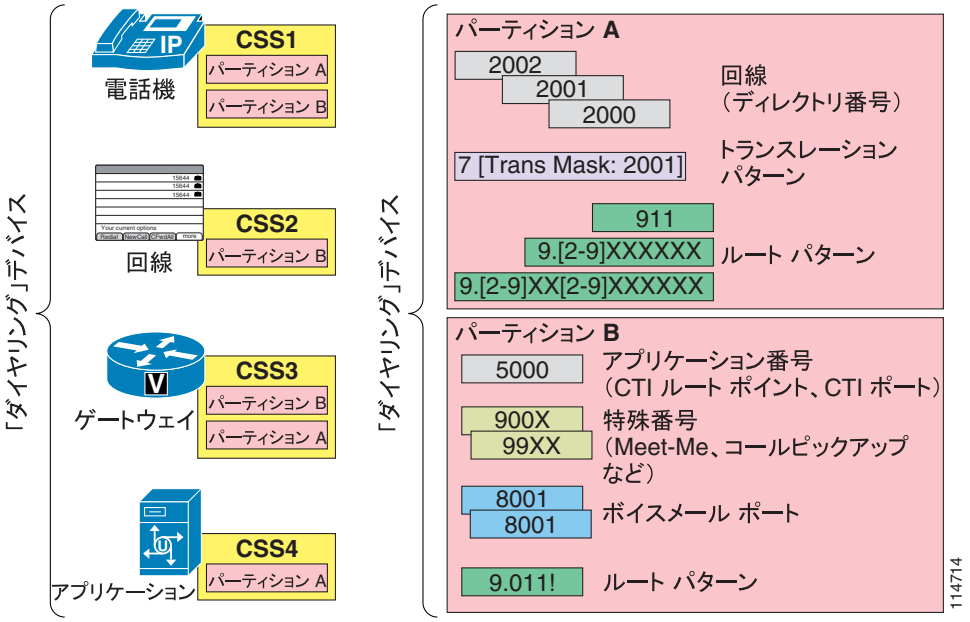
ダイヤリング特権は、特定のエンドポイント（電話、ゲートウェイ、または CTI アプリケーションなど）にどのタイプのコールを許可する（または禁止する）かを制御するために設定されます。Cisco Unified CallManager で処理されるすべてのコールは、次の要素の設定で実装されたダイヤリング特権の対象になります。

- パーティション（P.10-23）
- コーリング サーチ スペース（P.10-24）

パーティションは、同じアクセス可能性を持つディレクトリ番号のグループです。コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。デバイスは、コーリング サーチ スペースに含まれているパーティション内の DN だけを呼び出すことができます。

図 10-8 に示すように、パーティション内に配置できるすべての項目は、ダイヤリングの対象となるパターンを持っています。このような項目としては、電話回線、ルート パターン、トランスレーション パターン、CTI ルート グループ回線、CTI ポート回線、ボイスメール ポート、および Meet-Me 会議番号があります。逆に、コーリング サーチ スペースを持つ項目は、コールをダイヤルできるすべてのデバイスです。たとえば、電話機、電話回線、ゲートウェイ、アプリケーション（CTI ルート グループまたはボイスメール ポート経由）などです。

図 10-8　パーティションとコーリング サーチ スペース

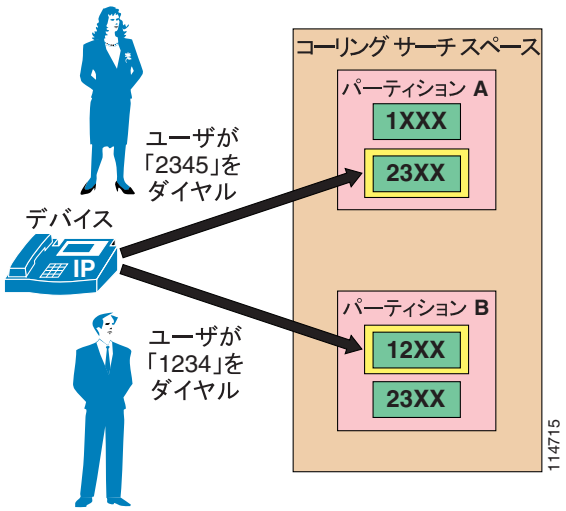


パーティション

パーティションに含めることができるダイヤル プラン項目には、IP Phone のディレクトリ番号、トランスレーション パターン、ルート パターン、CTI ルート ポイント、およびボイスメール ポートがあります。P.10-16 の「Cisco Unified CallManager におけるコール ルーティング」で説明するように、複数のダイヤル プラン項目（ディレクトリ番号、ルート パターンなど）が重複する場合、Cisco Unified CallManager は、ダイヤルされた番号と一致するか、または最も近い（最も固有性の高い一致）項目を選択します。2 つのダイヤル プラン項目が、ダイヤルされたパターンに等しく一致した場合、Cisco Unified CallManager は、コールを発信するデバイスのコーリング サーチ スペース内で最初に表示されているダイヤル プラン項目を選択します。

たとえば、図 10-9 について考えます。ルート パターン 1XXX と 23XX はパーティション A の一部であり、ルート パターン 12XX と 23XX はパーティション B の一部です。発信デバイスのコーリング サーチ スペースには、パーティション A: パーティション B の順にパーティションがリストされています。このデバイスのユーザが 2345 をダイヤルすると、Cisco Unified CallManager は、パーティション A のルート パターン 23XX を一致項目として選択します。これは、このパターンが発信デバイスのコーリング サーチ スペースで最初に示されているためです。ただし、ユーザが 1234 をダイヤルした場合には、Cisco Unified CallManager はパーティション B のルート パターン 12XX を一致項目として選択します。これは、パーティション A の 1XXX よりも一致率が大きいためです。コーリング サーチ スペースに含まれているパーティションの順序は、closest-match ロジックに基づいて均等一致項目が複数あった場合に、競合を解消する要素としてのみ使用されます。

図 10-9　マッチング ロジックにおけるパーティション順序の影響



（注） 均等一致項目が同じパーティションに複数ある場合、Cisco Unified CallManager は、ローカルのダイヤル プラン データベース内で最初にリストされている項目を選択します。ダイヤル プラン データベース内でダイヤル プラン項目がリストされる順序は、設定することができません。したがって、同じパーティション内で均等一致項目が共存しないようにすることを強くお勧めします。これはこのような場合に発生するダイヤル プラン ロジックが予測できないからです。

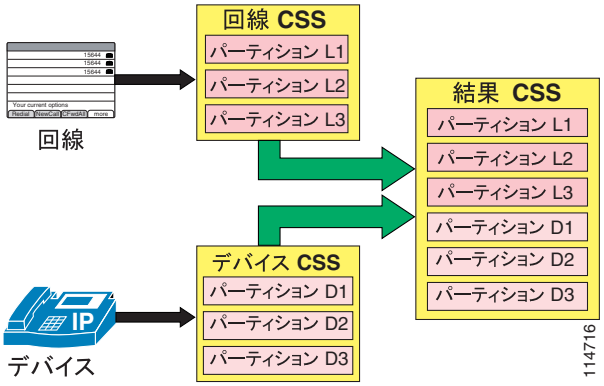
Cisco Unified CallManager Release 4.1 以降では、日時に基づいてパーティションをアクティブまたは非アクティブにすることができます。パーティションをアクティブまたは非アクティブにするには、まず、Cisco Unified CallManager Administration で期間とスケジュールを設定し、次に個々のタイム スケジュールを各パーティションに割り当てます。スケジュールに指定した日時の範囲外では、このパーティションは非アクティブになります。このパーティションに含まれているパターンは、Cisco Unified CallManager コール ルーティング エンジンによってすべて無視されます。この機能の詳細については、P.10-38 の「時間帯ルーティング」を参照してください。

コーリング サーチ スペース

コーリング サーチ スペースは、特定のデバイスからどのパーティションがアクセス可能であるかを指定します。所定のコーリング サーチ スペースが割り当てられるデバイスは、そのコーリング サーチ スペースにリストされているパーティションだけにアクセスできます。そのコーリング サーチ スペース以外のパーティションの DN へのダイヤルは失敗します。発信者にはビジー信号が聞こえます。

IP Phone 回線とデバイス（電話機）自体の両方でコーリング サーチ スペースを設定する場合、Cisco Unified CallManager は、この 2 つのコーリング サーチ スペースを図 10-10 に示すように連結し、デバイスのコーリング サーチ スペースの前に、回線のコーリング サーチ スペースを置きます。

図 10-10　IP Phone の回線とデバイスのコーリング サーチ スペース（CCS）の連結



同じルート パターンが、2 つのパーティション（回線のコーリング サーチ スペースに含まれているパーティションとデバイスのコーリング サーチ スペースに含まれているパーティション）に指定されている場合、Cisco Unified CallManager は、P.10-23 の「パーティション」の項で説明している規則に従って、パーティションの連結リスト内で最初にリストされているルート パターン（この場合、回線のコーリング サーチ スペースに関連したルート パターン）を選択します。

回線とデバイスのコーリング サーチ スペースを設定する方法に関する推奨事項については、P.10-80 の「従来のアプローチによる Cisco Unified CallManager のサービス クラスの構築」とP.10-84 の「回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築」の項を参照してください。

結合されたコーリング サーチ スペース（デバイスと回線）の最大長は、各パーティション名間の区切り文字を含めて、1024 文字です（たとえば、ストリング「partition_1:partition_2:partition_3」は 35 文字です）。したがって、コーリング サーチ スペース内の最大パーティション数は、パーティション名の長さに応じて変動します。また、コーリング サーチ スペースの文節は、デバイスのコーリング サーチ スペースと回線のコーリング サーチ スペースを結合するので、個々のコーリング サーチ スペースの最大文字の上限は、512 文字（結合されたコーリング サーチ スペース文節の上限 1024 文字の半分）です。

したがって、パーティションとコーリング サーチ スペースを作成するときは、コーリング サーチ スペースに含める予定のパーティション数を基準にして、パーティション名を短くしてください。コーリング サーチ スペースの設定の詳細は、次の Web サイトで入手可能なオンラインの『*Cisco Unified CallManager Administration Guide*』を参照してください。

http://www.cisco.com

パーティションまたはコーリング サーチ スペースを設定する前に、すべての DN は、<None> という名前が付いた特別なパーティションに置かれ、すべてのデバイスには、<None> という名前が付いたコーリング サーチ スペースが割り当てられます。カスタム パーティションとコーリング サーチ スペースを作成する場合は、作成するどのコーリング サーチ スペースにも、<None> パーティションが含まれています。一方、<None> コーリング サーチ スペースには、<None> パーティションだけが入っています。

(注) <None> パーティションに残っているどのダイヤル プラン項目も、コールを発信する任意のデバイスから暗黙的に到達可能です。したがって、予期しない結果を避けるために、<None> パーティションにダイヤル プラン項目を残さないように強くお勧めします。

(注) <None> と定義されたままのコーリング サーチ スペースを残さないでください。そのままにしておくと、ダイヤル プランの動作が予測困難になる可能性があります。

自動転送コーリング サーチ スペース

Release 5.0 以外のバージョンの Cisco Unified CallManager では、回線に対して設定されているメインのコーリング サーチ スペースは、デバイスのコーリング サーチ スペースと連結されます。一方、3 タイプの自動転送（Forward All、Forward Busy、Forward No Answer）に対して設定されているコーリング サーチ スペースは、他のどのコーリング サーチ スペースとも連結されないスタンドアロン値です。

Cisco Unified CallManager Release 5.0 では、Call Forward All コーリング サーチ スペースは Directory Number 設定ページにある Secondary Calling Search Space for Forward All に連結され、それで得られるコーリング サーチ スペースは、Forward All 動作が User ページまたは Administrative ページから開始された場合にすべてのコールに適用されます。

これらの連結されたコーリング サーチ スペースは、SCCP を実行している電話機または SIP を実行しているタイプ B の電話機から Forward All 動作が起動されたときにも使用されます。詳細については、P.10-84 の「回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築」を参照してください。

SIP を実行しているタイプ A の IP Phone では、Call Forward All がその電話機自体から起動された場合、転送されるコールにデバイスの Rerouting Calling Search Space が使用されます。Forward All 動作が CallManager User ページまたは CallManager Administrative ページから起動される場合、その電話機から開始される Forward All 動作とは無関係になります。

たとえば、SIP を実行するタイプ A の IP Phone に、CallManager User ページで内線 3000 への Forward All が指定されているとします。同時に、その電話機自体には、内線 2000 への Forward All が設定されています。この場合、その電話機に対するすべてのコールは、内線 3000 に転送されます。

(注) SIP を実行するタイプ A の IP Phone では、CallManager User ページまたは Administrative ページからの Forward All の起動は、電話機に反映されません。電話機には、コールの転送に関する確認は何も表示されません。

SCCP を実行する IP Phone または SIP を実行するタイプ B の IP Phone から Forward All が起動された場合、ユーザ入力は入力と同時に、設定済みの Forward All コーリング サーチ スペースの中で許可されるパターンと比較されます。無効な宛先パターンが設定されていると、ユーザにはリオーダー トーンが聞こえます。SIP を実行するタイプ A の IP Phone から Forward All が起動された場合、Forward All ユーザ入力は電話機上にローカルに保管され、Cisco Unified CallManager 内のコーリング サーチ スペースとは照合されません。ユーザ入力が無効な宛先に対応している場合でも、ユーザへの通知はありません。その電話機へのコールに対しては、電話機が無効な宛先番号に対して SIP 再ルーティング動作を開始しようとしたときに、リオーダー トーンが再生されます。

Forward All コーリング サーチ スペースが <None> のままになっている場合、処理の結果は Cisco Unified CallManager のリリースによって異なり、予想することは困難です。このため、自動転送のコーリング サーチ スペースを設定する場合は、次のベスト プラクティスに従うことをお勧めします。

- 自動転送コーリング サーチ スペースは、常に <None> 以外の値を使用して設定する。この設定により混乱を避けることができ、トラブルシューティングが容易になります。転送されるコールにどのコーリング サーチ スペースが使用されるかについて、ネットワーク管理者が正確に把握できるためです。
- Call Forward Busy コーリング サーチ スペースと Call Forward No Answer コーリング サーチ スペースは、ボイスメール パイロットおよびボイスメール ポートの DN に到達可能で、かつ外部公衆網番号以外の値を使用して設定する。
- Call Forward All コーリング サーチ スペースと Secondary Calling Search Space for Forward All は、どちらも企業のポリシーに従って設定する。多くの企業では、コールを社内の番号にしか転送できないように制限しています。この方法によって、ユーザが IP Phone の回線を長距離電話の番号に転送したり、私用電話の長距離通話料金がかからないようにするためにローカル IP Phone の番号に公衆網からダイヤルしたりすることを防止します。

Cisco Unified CallManager における番号操作

Cisco Unified CallManager の番号操作機能は、次のツールが提供しています。

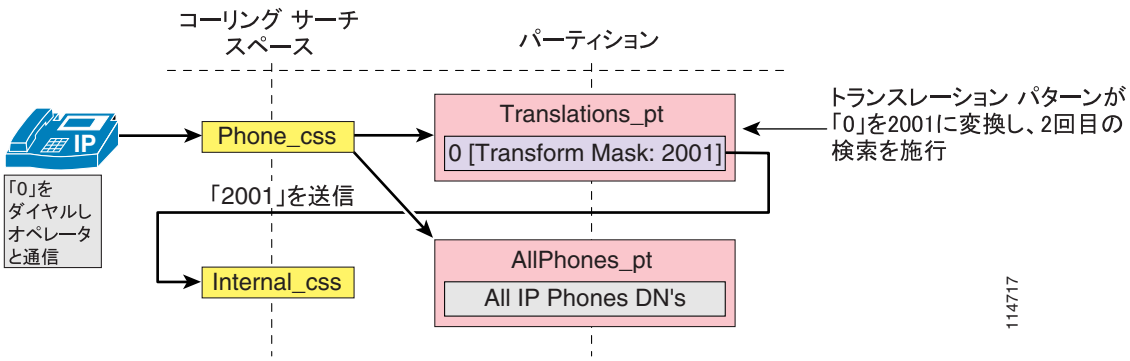
- 外部ルート コンストラクト（ルート パターン、ルート リスト、ルート グループ）
- トランスレーション パターン

外部ルート コンストラクトを使用すると、コールを外部デバイスにルーティングしながら一部の番号操作を実行できます。この機能については、P.10-16 の「Cisco Unified CallManager におけるコール ルーティング」の項で説明しています。

トランスレーション パターンは、Cisco Unified CallManager で最も強力な番号操作ツールであり、あらゆるタイプのコールに対して使用できます。トランスレーション パターンは、ルート パターンと同じ一般規則に従い、同じワイルドカードを使用します。ルート パターンと同じように、トランスレーション パターンをパーティションに割り当てます。しかし、ダイヤルされた数字がトランスレーション パターンと一致する場合、Cisco Unified CallManager は、ゲートウェイなどの外部エンティティにコールをルーティングしません。代わりに、まず変換を実行した後、トランスレーション パターン内で設定されたコーリング サーチ スペースを使用して、コールを再度ルーティングします。

トランスレーション パターンは、図 10-11 の例に示すように、さまざまな用途に使用することができます。

図 10-11　トランスレーション パターンの応用例



この例では、管理者は、0 をダイヤルすると到達できるオペレータ サービスをユーザに提供し、一方で定型の内部番号計画をそのまま維持することを考えています。IP Phone は、Translations_pt パーティションを（他のパーティションとともに）含んでいる Phone_css コーリング サーチ スペースを使用して設定されています。このパーティションには、トランスレーション パターン 0 が定義されています。設定済みの Called Party Transform Mask によって、ダイヤル ストリング（0）を新しいストリング 2001 で置き換えるように Cisco Unified CallManager に指示しています。2001 は、オペレータの電話の DN に対応しています。2 回目の（この場合は 2001 の）ルックアップが、Internal_css コーリング サーチ スペースを使用して、コール ルーティング エンジンを通じて強制的に実行されます。この時点で、AllPhones_pt パーティションに含まれている実際のオペレータ DN（2001）までコールを伸ばすことができます。

（注） ダイヤルされた番号をトランスレーション パターンを使用して操作すると、その変換後の番号が、コール詳細レコード（CDR）に記録されます。ただし、番号操作がルート リスト内で発生した場合、CDR には変換後の番号ではなく、ダイヤルされた元の番号が表示されます。IP Phone の Placed Calls ディレクトリには、常にユーザがダイヤルしたストリングがそのまま表示されます。

Automated Alternate Routing

自動代替ルーティング（AAR）機能を使用すると、Cisco Unified CallManager で音声メディア用の代替パスを確立することができます。このパスが確立されるのは、同じクラスタ内の 2 つのエンドポイント間にある優先パスで、コール アドミッション制御用のロケーション メカニズムによって決定される使用可能帯域幅が使い果たされたときです。

AAR 機能の主な適用対象は、集中型コール処理配置です。たとえば、支店 A の電話から支店 B の電話にコールする場合、支店間の WAN リンクで使用可能な帯域幅（ロケーション メカニズムによって計算）が不足しているときは、AAR によって公衆網経由でコールを再ルーティングできます。コールの音声パスは、発信元の電話からローカルの（支店 A の）公衆網ゲートウェイまでは IP ベース、このゲートウェイから公衆網を経由して支店 B のゲートウェイまでは TDM ベース、支店 B のゲートウェイから宛先の IP Phone までは IP ベースです。

AAR による処理は、ユーザには見えません。ユーザが着信側電話のオンネット（たとえば 4 桁の）ディレクトリ番号にしかダイヤルできないように AAR を設定すると、公衆網などの代替ネットワーク経由で宛先に到達するときに、ユーザによる追加入力が不要になります。

（注） AAR では、CTI ルート ポイントがコールの発信元や宛先になることはサポートしていません。また、ユーザが複数のサイトにわたってローミングする場合、AAR はエクステンション モビリティ機能と共存できません。詳細については、P.10-31 の「エクステンション モビリティ」を参照してください。

AAR を正常に動作させるには、AAR の次の主要要素を指定する必要があります。

- 宛先公衆網番号の確立（P.10-29）
- 必要なアクセス コードの付加（P.10-29）
- 適切なダイヤル プランおよびルートの選択（P.10-30）

（注） Cisco Unified CallManager Release 4.1.3 以降では、自動代替ルーティング（AAR）をボイスメール ハント グループのメンバーに適用することができます。

宛先公衆網番号の確立

コールを再ルーティングするには、公衆網などの代替ネットワーク経由でルーティングできる宛先ディレクトリ番号（DN）を使用する必要があります。AAR は、ダイヤルされた番号を使用してコールのクラスタ上での宛先を特定し、この番号を着信側の外部電話番号マスクと結合します。この 2 つの要素を結合することで、代替ネットワークによってルーティング可能な、完全修飾番号（Fully Qualified Number）が生成される必要があります。

たとえば、San Francisco にある電話 A（DN = 2345）から、New York の電話 B 上に設定されているオンネット DN（1234）にダイヤルするとします。ロケーション ベースのコール アドミッション制御によってコールが拒否された場合、AAR は New York の電話の外部電話番号マスク（212555XXXX）を取得して使用し、公衆網上でルーティング可能な完全修飾番号（2125551234）を導出します。

San Francisco から New York へのコールを公衆網でルーティングするには、電話番号のプレフィックスとして「1」が必要です。このプレフィックスは、電話の外部電話番号マスクには含めないことをお勧めします。この電話からオフネットの宛先に発信されるコールでは、このプレフィックスが Calling Party Identification（CallerID）の一部として表示されるためです。代わりに、AAR グループ設定の一部として「1」を追加することをお勧めします。

同じ Cisco Unified CallManager クラスタの内部で複数の国にわたる配置を実現するには、外部電話番号マスクを設定するときに、プレフィックス番号を付けるだけで同じ国または別の国から宛先電話機に到達できるようにする必要があります。つまり、国内であることを示すプレフィックス（多くの国では 0）は、それらが E.164 アドレスの一部でない場合、外部電話番号マスクには含めないでください。

この状況を十分に理解するために、London（英国）、Paris（フランス）、Nice（フランス）にサイトがある Cisco Unified CallManager クラスタの例を考えます。Paris の DID 範囲の E.164 アドレスは、+33145678XXX です。ただし、フランスの公衆網内からコールする場合、これらの内線には、通常は 0145678XXX として到達します。

London のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、ダイヤル ストリングは 90033145678XXX です。一方で、Nice のオフィスにいる人物が Paris のオフィスに公衆網経由でダイヤルする場合、ダイヤル ストリングは 00145678XXX です。したがって、Paris のオフィスにある電話の外部電話番号マスクは、通常のフランス国内番号 0145678XXX ではなく、この場合 145678XXX に設定する必要があります。このマスクに 0 を含めた場合、単に追加番号をプレフィックスとして付加するだけでは、ストリング 90033145678XXX を取得できなくなります。

必要なアクセス コードの付加

宛先番号が元の支店のダイヤル プランによって正常にルーティングされるためには、オフネット アクセス コードのプレフィックス（たとえば 9）が必要になる場合もあります。また、発信地点が別のエリア コード（番号計画エリア（NPA）とも呼ばれます）内に配置されている場合、ダイヤル ストリングの一部として、プレフィックス「1」が必要になります。AAR を設定する場合は、DN を AAR グループ内に配置します。AAR グループのペアごとに、同じ AAR グループ内で発信または終端するコールのプレフィックス番号も含めて、その 2 グループ間のコールで DN に追加するプレフィックス番号を設定できます。

一般的な規則として、複数の DN が次の特性をすべて共有している場合は、それらを同じ AAR グループに配置します。

- 共通のオフネット アクセス コード（たとえば 9）
- エリア間コールにおける共通の公衆網ダイヤリング構造（たとえば、北米では 1-NPA-NXX-XXXX）
- 共通の外部電話番号マスク形式

たとえば、San Francisco と New York の両方のサイトで、上の特性がすべて共通しているとします。San Francisco と New York の DN を 1 つの AAR グループに配置して、この AAR グループ内で発生した AAR コールにプレフィックス 91 を付けるようにこのグループを設定します。San Francisco の電話 A が New York の電話 B（212 555 1234）に到達するには、ダイヤル ストリングにプレフィックス 91 を付けるように AAR グループを設定して、全体で 91 212 555 1234 というストリングが完成されるようにします。

複数の国にわたる配置では、通常は国ごとに少なくとも 1 つの AAR グループが必要です。前の項で示した例について考えると、2 つの AAR グループを定義することができます。UK AAR グループ（London にあるすべての DN に割り当てられるグループ）と France AAR グループ（Paris と Nice にあるすべての DN に割り当てられるグループ）です。UK AAR グループは、France AAR グループに向かうコールにプレフィックス 90033 を付加するように設定します。一方、France AAR グループは、同じ AAR グループ内でのコールに対して 00 のみをプレフィックスとして付加するようにします。

適切なダイヤル プランおよびルートの選択

AAR コールは、発信元の電話と同じロケーションにあるゲートウェイを通じて出力する必要があります。これによって、完成されたダイヤル ストリングが、発信元サイトのダイヤル プランを通じて送信されます。このように設定するには、Cisco Unified CallManager Administration のデバイス設定ページで、適切な AAR コーリング サーチ スペースを選択します。AAR コーリング サーチ スペース内で、オフネット ダイヤル プラン項目（たとえば、ルート パターン）を、同じ場所にあるゲートウェイを指し、公衆網にコールを転送する前にアクセス コードを削除するように設定します。

たとえば、San Francisco サイトの電話を設定する場合は、91-NPA-NXX-XXXX としてダイヤルされた長距離電話を許可し、アクセス コード（9）を削除して San Francisco のゲートウェイに送信する AAR コーリング サーチ スペースを使用します。

（注） オンネット社内コールを強制的に公衆網コールとしてダイヤルする追加のルート　パターンを設定した場合は、それらのパターンが AAR 機能のものと一致しないことを確認します。詳細については、P.10-57 の「マルチサイト配置用の設計ガイドライン」を参照してください。

（注） コール アドミッション制御による再ルーティングされたコールの拒否を避けるため、AAR 機能は、各エンドポイントとそれに関連する公衆網へのゲートウェイとの間で、IP パスとして LAN を使用する必要があります。したがって、AAR ダイヤル プランでは、公衆網へのアクセスを集中型ゲートウェイに依存することができません。

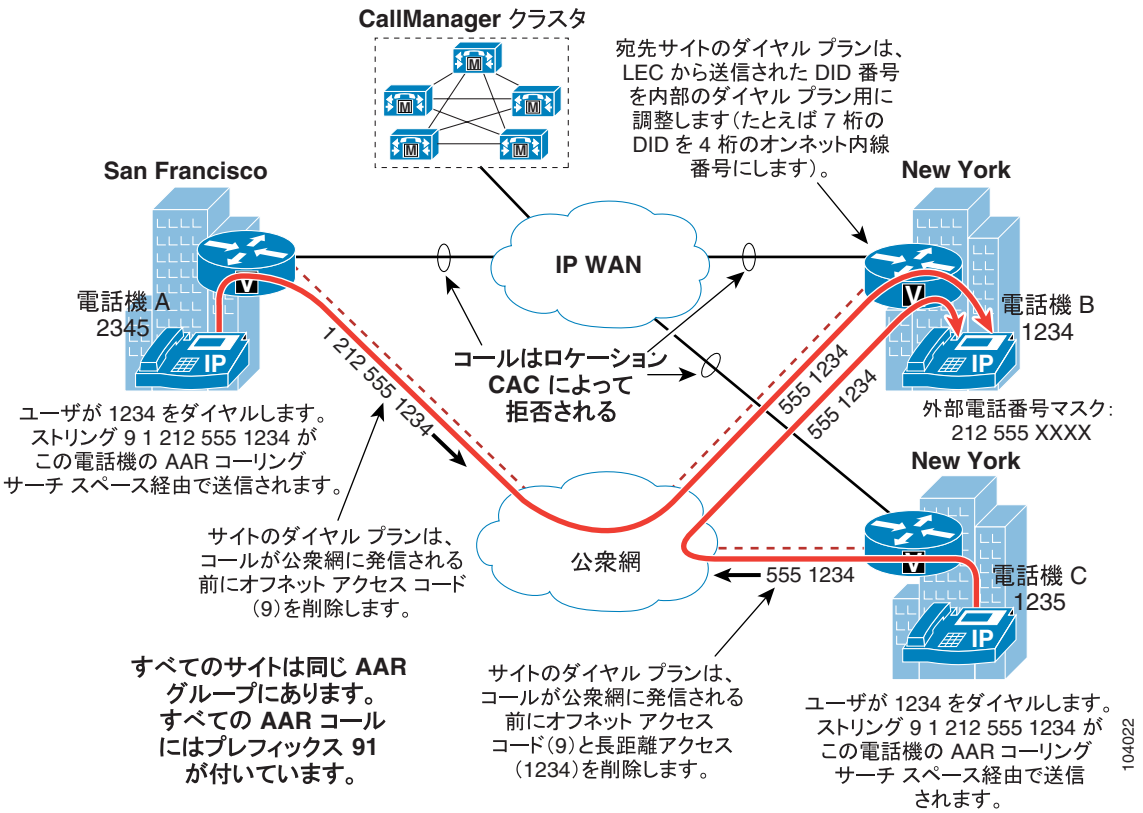
同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項

場合によっては、ローカルエリア ダイヤリングを使用できるように AAR ダイヤル ストリングをローカルに修正する必要があります。たとえば、New York にある 2 つのサイトが、同じエリア コード 212 を共有しているとします（図 10-12 を参照）。この場合は、91 212 555 1234 としてダイヤルされた番号を 9 555 1234 に変換する必要があります。

この変換を実行する最良の方法は、サイト固有のトランスレーション パターン 91212.555XXXX を設定することです（ドットの前の番号を削除して、先頭に 9 を付加します）。このトランスレーション パターンは、New York サイトの AAR コーリング サーチ スペースのメンバー パーティションに

のみ配置します。San Francisco サイトからは、この同じ宛先に 91 212 555 1234 として到達する必要があります。また、New York サイトのダイヤル プランにもこのトランスレーション パターンを配置して、長距離電話としてダイヤルされたローカルに到達可能な番号を適切にルーティングできるようにする必要があります。New York サイトのダイヤル プランでは、9 555 1234 を有効なストリングとして受け付け、このコールを公衆網に送信する前に、ストリングを 555 1234 に変換するようにします。

図 10-12　サイト間 AAR コールにおけるダイヤル番号の変換



（注） AAR 機能は、宛先の電話が到達不能であることが検出されても起動しません。したがって、WAN の障害によって AAR 機能が起動することはありません。

エクステンション モビリティ

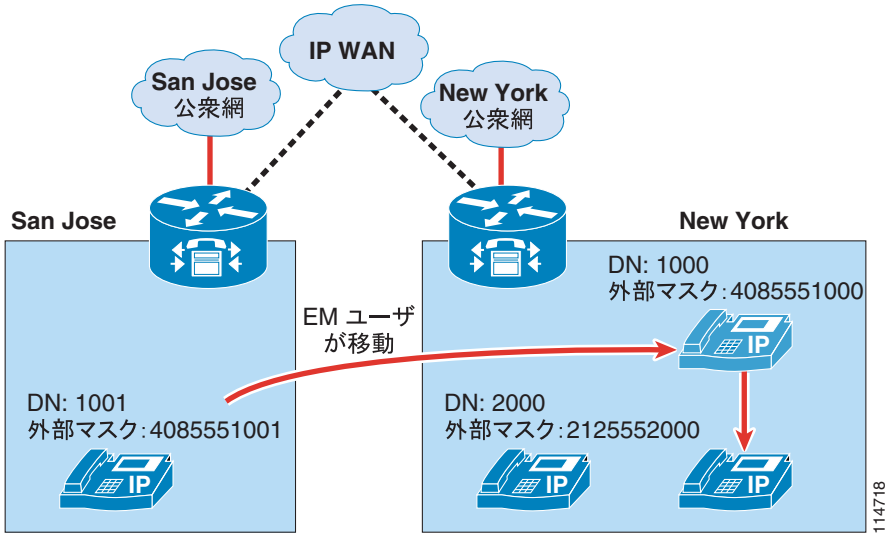
エクステンション モビリティ機能を使用すると、ユーザが IP Phone にログインしたとき、内線番号、短縮ダイヤル、メッセージ待機インジケータ（MWI）ステータス、コール特権を含めて、そのユーザのプロファイルが自動的にその電話機に適用されるようになります。このメカニズムは、それぞれのエクステンション モビリティ ユーザに関連付けられる、デバイス プロファイルを作成することで成り立っています。デバイス プロファイルは、実質的には仮想 IP Phone であり、1 つまたはそれ以上の回線を設定したり、コール特権や短縮ダイヤルなどを定義したりできます。

IP Phone がログアウト状態になっている（つまり、エクステンション モビリティ ユーザがログインしていない）とき、この IP Phone の特性は、デバイス設定ページと回線設定ページによって決まります。ユーザが IP Phone にログインすると、デバイス設定は変更されませんが、既存の回線設定は Cisco Unified CallManager データベースに保存され、ユーザのデバイス プロファイルの回線設定によって置き換えられます。

エクステンション モビリティの重要な利点の 1 つは、ユーザがどこにいるかにかかわらず、同じ Cisco Unified CallManager クラスタによって制御されている IP Phone にユーザがログインできれば、そのユーザに対して、そのユーザ固有の内線番号で到達できることです。集中型コール処理を使用しているマルチサイト配置に対してエクステンション モビリティを適用すると、地理的に互いに分離している複数のサイトに対して、この機能を展開することができます。

ただし、エクステンション モビリティ機能を P.10-28 の「Automated Alternate Routing」の項で説明している AAR 機能と組み合せる場合は、一定の制限事項があります。図 10-13 に示した例について考えます。エクステンション モビリティと AAR を集中型コール処理の Cisco Unified CallManager クラスタに配置していて、San Jose と New York にそれぞれ 1 つのサイトがあります。

図 10-13　エクステンション モビリティと AAR



この例では、通常 San Jose を拠点としているエクステンション モビリティ ユーザが、DN 1000 と DID 番号 (408) 555-1000 を持っているとします。このユーザの外部電話番号マスクは、4085551000 と設定されています。このユーザが New York サイトに移動し、ログインします。さらに、San Jose と New York 間の IP WAN 帯域幅がすべて使用されているとします。

San Jose にいる内線番号 1001 のユーザが 1000 にコールすると、AAR が呼び出され、発信側の AAR コーリング サーチ スペースと着信側の AAR グループに基づいて、914085551000 への新しいコールが、San Jose の電話によって試行されます。このコールは、San Jose のゲートウェイを使用して公衆網にアクセスしますが、DID (408) 555-1000 が同じゲートウェイによって所有されているため、公衆網はコールをこのゲートウェイに戻します。San Jose のゲートウェイは、内線番号 1000 を持つ電話へのコールを確立しようとしますが、この電話は現在 New York にあります。New York にアクセスするための帯域幅を使用できないため、AAR 機能がもう一度呼び出され、次の 2 つのうち、いずれかのシナリオが発生します。

- ゲートウェイの AAR コーリング サーチ スペースに外部公衆網ルート パターンが含まれている場合、ループが開始され、San Jose サイトにあるすべての公衆網トランクが使い果たされる。
- 逆に、ゲートウェイの AAR コーリング サーチ スペースに内部の番号のみが含まれている場合は、コールが失敗し、発信者にはファースト ビジー トーンが聞こえる。この場合は、1 つの公衆網コールが発生して 1 つが受信されるため、コールのセットアップ中、San Jose のゲートウェイでは 2 つの公衆網トランクが使用されます。

ヒント　ここで説明したようなルーティング ループを防止するには、ゲートウェイ設定ページでコーリング サーチ スペースを設定するときに、必ず内部の宛先のみを含め、同じゲートウェイを含んでいるルート グループやルート リストを指すルート パターンを一切含めないようにします。

この例では、エクステンション モビリティが Cisco Unified Communications の動的な側面を利用しているため、サイト間のコール ルーティングで IP ネットワークを使用する必要があることを中心に説明しています。公衆網に定義されている E.164 番号は静的なものであり、公衆網ネットワークはエクステンション モビリティ ユーザの移動を認識しません。AAR 機能は、コール ルーティングを公衆網に依存しているため、ホーム サイト以外のサイトに移動したエクステンション モビリティ ユーザに対して、この機能を使用して到達することはできません。

（注）　ただし、エクステンション モビリティ ユーザが自分のホーム サイトと同じ AAR グループに属するリモート サイトに移動した場合には、使用可能な IP WAN 帯域幅が十分にないとき、そのユーザは AAR 機能を使用して他のサイトへのコールを発信することができます。

ハント リストと回線グループ

「ハント パイロット」は、通常はコール カバレッジや、Skinny Client Control Protocol（SCCP）エンドポイントを通じたコール分配に使用されます。コールの分配には、ハント コンストラクトを使用できます。このハント コンストラクトは、3 層式のアーキテクチャに基づいています。外部コールのルーティングに使用されるアーキテクチャに似たこのアーキテクチャでは、複数層のコール ルーティングと共に、番号操作も可能です。

Cisco Unified CallManager は、着信番号と一致する設定済みハント パイロットを検索し、それを使用して、対応するハント リストを選択します。ハント リストには、コールに使用可能なパスが優先順位順に並べられています。これらのパスは、「回線グループ」と呼ばれます。図 10-14 では、Cisco Unified CallManager Release 4.1 以降のハント コンストラクトの 3 層式アーキテクチャを示しています。

（注）　Cisco CallManager Release 3.3 以前では、コール カバレッジ機能はハント グループによって提供されていました。このグループは、Telephony Call Dispatcher（TCD）サービスによって制御され、Cisco Attendant Console によっても使用されます。Cisco Unified CallManager Release 4.0 では、ハント パイロット、ハント リスト、および回線グループが導入されました。ただし、このリリースでは、ハント パイロット構造はルート パターン構造と組み合せられ、ハント リストはルート リストと組み合せられていました。Cisco Unified CallManager Release 4.1 以降では、これらの構造は独立しています。表 10-3 は、Cisco Unified CallManager Releases 4.0 と 4.1 のハント リストと回線グループ、および Cisco Unified CallManager Releases 3.3 以前で Attendant Console を使用したハント グループの機能比較を示しています。

表 10-3　ルート リスト、ハント リスト、ハント パイロット、ハント グループの機能比較

機能	Cisco Unified CallManager Release 3.3 以前のハント グループ	Cisco Unified CallManager Release 4.0 のルート リストとハント リスト	Cisco Unified CallManager Release 4.1 および 5.0 のハント パイロット
Skinny Client Control Protocol（SCCP）エンドポイント	あり	あり（回線グループ）	あり
SIP エンドポイント	適用対象外	適用対象外	あり（Release 5.0）
ゲートウェイとトランク（オフネットの宛先）	なし	あり（ルート グループ）	なし
トップダウン アルゴリズム	あり	あり	あり
循環アルゴリズム	あり	あり	あり
最長アイドル時間アルゴリズム	あり	あり	あり
ブロードキャスト アルゴリズム	あり	あり	あり
ハント オプション	なし	あり	あり
無応答時の復帰	なし	あり	あり
パフォーマンスの監視（PerfMon）	なし	あり	あり（Release 5.0 を除く）
SCCP ボイスメール ポート（Cisco Unity）	なし	あり（回線グループ）	あり
Simplified Message Desk Interface（SMDI）ボイスメール システム	あり	あり	あり
キューイング	あり	なし	なし
ハント グループとハント パイロットのリンク	あり	なし	あり

比較のために、図 10-14 に Cisco Unified CallManager 4.1 以上のハント パイロットのアーキテクチャを示し、図 10-15 に Cisco Unified CallManager 4.0 のハント パイロットのアーキテクチャを示します。

図 10-14　Cisco Unified CallManager Release 4.1 のハント アーキテクチャの 3 層式アーキテクチャ

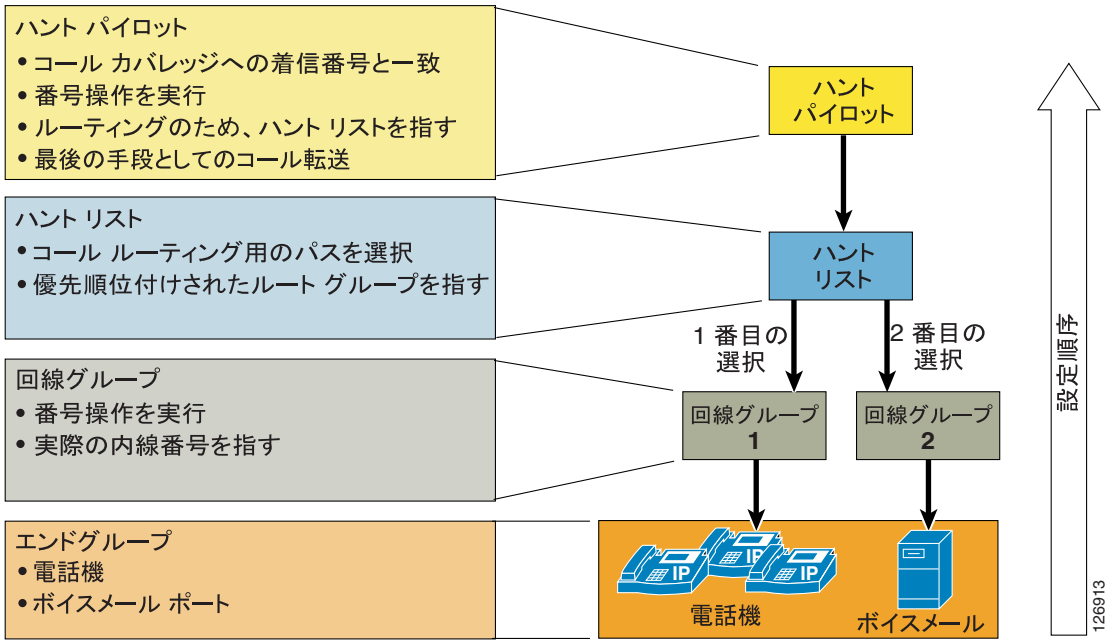
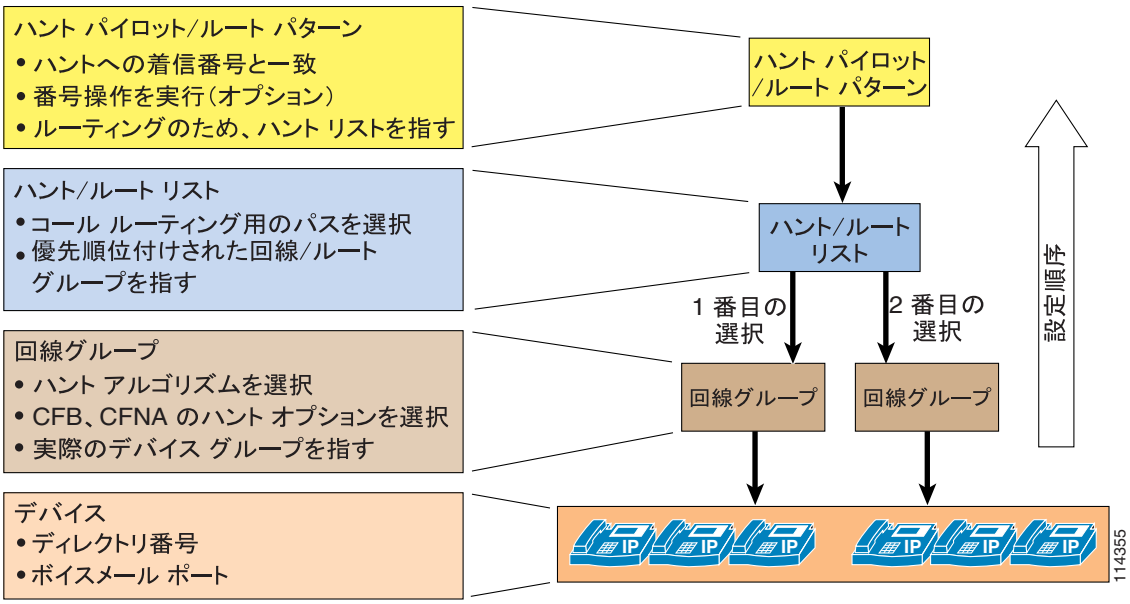


図 10-15　Cisco Unified CallManager Release 4.0 のハント アーキテクチャ



ハント パイロット

ハント パイロットは、コールをディレクトリ番号にルーティングするために Cisco Unified CallManager で設定された、ルート パターンのように数字とワイルドカードを組み合せたストリング（たとえば、9.[2-9]XXXXXX）です。ハント パイロットは、ハント リストを直接指しています。ハント リストは回線グループを指しており、回線グループは、最終的に SCCP エンドポイントを指しています。

Cisco Unified CallManager Release 4.1 以降では、ハンティングが次のいずれかまたは両方の理由で失敗した場合、コールを最終的な宛先に転送することができます。

- すべてのハンティング オプションを使い果たしても、コールはまだ応答されていない。
- タイムアウト期間が満了した。

このコール転送は、Hunt Pilot 設定ページの Hunt Forward Settings セクションで設定します。この転送の宛先は、次のいずれかから選択できます。

- Cisco Unified CallManager の内部コール ルーティング テーブルに含まれている、特定のパターン。
- 個人用プリファレンス。このプリファレンスは、元々の着信番号の Call Forward No Coverage 設定を指しています。

たとえば、個人用プリファレンス オプションを実装するには、Forward No Answer フィールドに従ってコールをハント パイロットへ転送するようにユーザの電話を設定して、コールに応答できるユーザが他にいないかどうか検索できるようにします。すべてのハンティング オプションが使い果たされたか、タイムアウト期間が満了したためにコール ハンティングが失敗した場合、コールを当初の宛先ユーザが設定している宛先に転送することができます。たとえば、ユーザの DN 設定ページにある Forward No Coverage フィールドにボイスメール番号を設定すると、ハンティングが失敗した場合、コールはそのユーザのボイスメール ボックスに送信されます。

（注） Cisco Unified CallManager Release 4.0 は、コール転送をサポートしていません。

ハント パイロットの処理するコールには、次の考慮事項が適用されます。

- コール ピックアップとグループ コール ピックアップは、ハント パイロットが分配するコールではサポートされません。回線グループのメンバーは、回線グループの他のメンバーに提供されたハント パイロット コールについては、メンバー同士が同じコール ピックアップ グループに属している場合でもピックアップできません。
- ハント パイロット番号に基づいて分配されるコールは、回線グループ内のディレクトリ番号に対して設定される、個別の自動転送処理をサポートしていません。このため、Immediate Divert（iDivert）ソフトキーや、ディレクトリ番号に対して設定されている自動転送は、ハント パイロットが分配するコールに対しては機能しません。回線グループの設定でハント オプションとして使用できる自動転送条件のみが、ハント パイロット コールに適用されます。ただし、iDivert ソフトキーや自動転送設定は、ハント パイロットが分配したコールを除く、すべての着信コールで機能します。
- ハント パイロットは、自身の回線グループのメンバーとハント パイロットが別のパーティションに配置されている場合でも、コールを自身の回線グループのいずれかのメンバーに分配できます。ハント パイロットが分配するコールは、すべてのパーティションおよびコーリング サーチ スペース制限を上書きします。

ハント リスト

ハント リストは、コール カバレッジに使用できるパス（回線グループ）が優先順位順に並べられたリストです。ハント リストには次の特性があります。

- 複数のハント パイロットが同一ハント リストを指すことができます。
- ハント リストは、ハント パイロット番号へのコールが行われたときに提供される代替電話機セットとして機能する回線グループが、優先順位順に並べられたリストです。たとえば、特定のサイトにある一連の電話機の中から、コールを受け取る電話機を見つけるために使用できます。コールが受け取られない場合、ハント リストは第 2 のサイトにある電話機を指定する、第 2 の回線グループを通じたコールの提供を試みます。
- ハント リストは、番号操作は一切実行しません。
- 複数のハント リストに、同じ回線グループを含めることができます。

回線グループ

回線グループのメンバーは、Cisco Unified CallManager が制御しているユーザ内線番号です。このため、コールを回線グループのメンバー間に分配するときは、Cisco Unified CallManager がコールを制御します。コールが応答されなかった場合や、内線番号が使用中または未登録の場合は、ハント オプションをコールに適用できます。

回線グループは、コールが分配される順序を制御し、次の特性を持っています。

- 回線グループは、特定の内線番号（通常は、IP Phone 内線番号またはボイスメール ポート）を指しています。
- 1 つの内線番号が複数の回線グループに含まれていることがあります。
- コンピュータ / テレフォニー インテグレーション（CTI）ポートと CTI ルート ポイントは、回線グループに追加できません。したがって、CTI アプリケーション（Cisco Customer Response Solutions（CRS）や IP 音声自動応答装置（IP IVR）など）を通じて制御されるエンドポイントには、コールを分配できません。
- Cisco Unified CallManager は、割り当てられている分配アルゴリズムに従ってコールを各デバイスに分配します。Cisco Unified CallManager は、次のアルゴリズムをサポートしています。
  - トップダウン
  - 循環
  - 最長アイドル時間
  - ブロードキャスト
- No-Answer、Busy、Not-Available のいずれかのイベントが発生すると、分配されたコールを回線グループがハント オプションに基づいて内線番号に転送します。Cisco Unified CallManager は、次のハント オプションをサポートしています。
  - 次のメンバーにアクセスし、その後はハント リスト内の次のグループにアクセスする。
  - 次のメンバーにアクセスするが、次のグループにはアクセスしない。
  - 残りのメンバーをスキップして、次のグループに直接アクセスする。
  - ハンティングを停止する。

ハント アルゴリズムとハント オプションの詳細については、次の Web サイトで入手可能な『*Cisco Unified CallManager Administration Guide*』を参照してください。

http://www.cisco.com

回線グループ デバイス

回線グループ デバイスは、回線グループがアクセスするエンドポイントであり、次のいずれかのタイプに該当します。

- Skinny Client Control Protocol（SCCP）エンドポイント（Cisco Unified IP Phone、VG248、ATA 188 など）
- SIP エンドポイント（Cisco Unified CallManager 5.0 が必要）
- ボイスメール ポート（Cisco Unity）
- H.323 クライアント
- MGCP ゲートウェイに接続されている FXS

時間帯ルーティング

Cisco Unified CallManager Release 4.1 では、Time-of-Day（ToD）ルーティング機能が導入されました。この機能を使用するには、次の要素を設定します。

- 期間
- タイム スケジュール

期間を利用すると、営業開始時刻と終了時刻を設定できます。この開始時刻と終了時刻は、コールをルーティングできる期間を示しています。これらの時刻に加えて、毎週または毎年発生するイベントを設定することもできます。さらに、Start Time オプションと End Time オプションにある No business hours を選択して、休業時間を設定することもできます。このオプションを選択した場合は、すべての着信コールがブロックされます。

タイム スケジュールは、パーティションに割り当てられている特定の期間をグループにまとめたものです。このタイム スケジュールによって、指定した期間中にパーティションがアクティブまたは非アクティブのどちらになっているかが判断されます。一致したパターンやダイヤリング パターンには、そのダイヤリング パターンの配置されているパーティションがアクティブになっている場合のみ到達できます。

図 10-16 では、同じコール パターン（8000）を持つ 2 つのハント パイロットが、2 つのパーティション（RTP_Partition、SJC_Partition）内に設定されています。これらのパーティションには、一連の定義済み期間を保持したタイム スケジュールがそれぞれ割り当てられています。たとえば、RTP の電話には、ハント パイロット 1 を使用することで、月曜日から金曜日の午前 8 時～ 午後 12 時（東部標準時。GMT - 5.00）まで、および日曜日の午前 8 時から午後 5 時まで到達できます。同様に、SJC の電話には、ハント パイロット 2 を使用することで、月曜日から金曜日の午前 8 時～午後 5 時（太平洋標準時。GMT - 8.00）まで、および土曜日の午前 8 時～午後 5 時まで到達できます。この例では、どちらのハント パイロットも 7 月 4 日は非アクティブです。

図 10-16　時間帯ルーティング

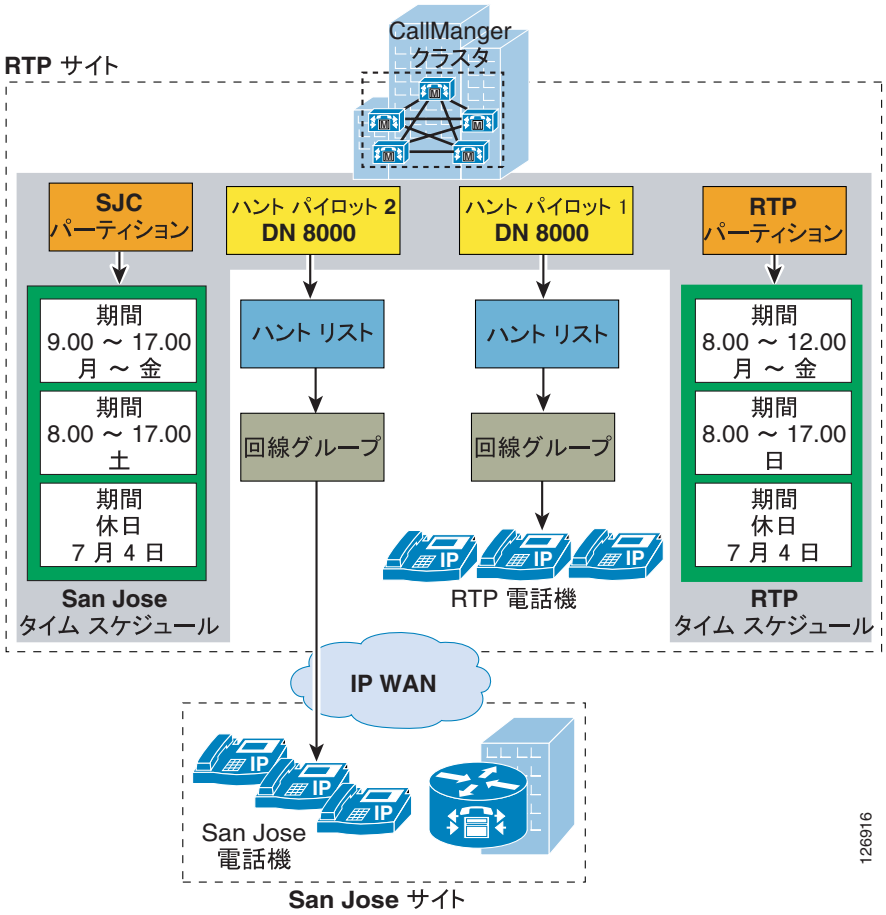


図 10-16 の例では、水曜日の午後 3 時にハント パイロット（8000）に着信したコールは、SJC の電話に転送されます。一方、このハント パイロットに 7 月 4 日にコールした人は、別のパターンが 8000 に一致しない限り、ファースト ビジー トーンを受信します。

H.323 ダイヤル ピアを使用する Cisco IOS でのコール ルーティング

H.323 プロトコルを使用する Cisco IOS ルータ上でのコール ルーティング ロジックは、ダイヤル ピア コンストラクトに依存しています。ダイヤル ピアは、スタティック ルートに似たものです。コールの発信地点と終端地点、およびコールがネットワークで通過するパスを定義しています。ダイヤル ピアは、コールの発信元と宛先のエンドポイントを指定するため、およびコール接続の各コール レッグに適用される特性を定義するために使用します。ダイヤル ピアに含まれている属性によって、ダイヤルされるどの番号をルータが収集し、テレフォニー デバイスに転送するかが決まります。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

ダイヤル ピアを使用したコール ルーティングを理解するための鍵の 1 つは、着信コール レッグと発信コール レッグ、つまり着信ダイヤル ピアと発信ダイヤル ピアという概念です。Cisco IOS ルータを経由する各コールは、2 つのコール レッグを持っていると見なされます。1 つはルータに入るもので、1 つはルータから出るものです。ルータに入るコール レッグが「着信コール レッグ」であり、ルータから出るコール レッグが「発信コール レッグ」です。

コール レッグには、主に次の 2 つのタイプがあります。

- ルータを公衆網、アナログ電話機、または PBX に接続する、従来の TDM テレフォニー コール レッグ
- ルータを他のゲートウェイ、ゲートキーパー、または Cisco Unified CallManager に接続する、IP コール レッグ

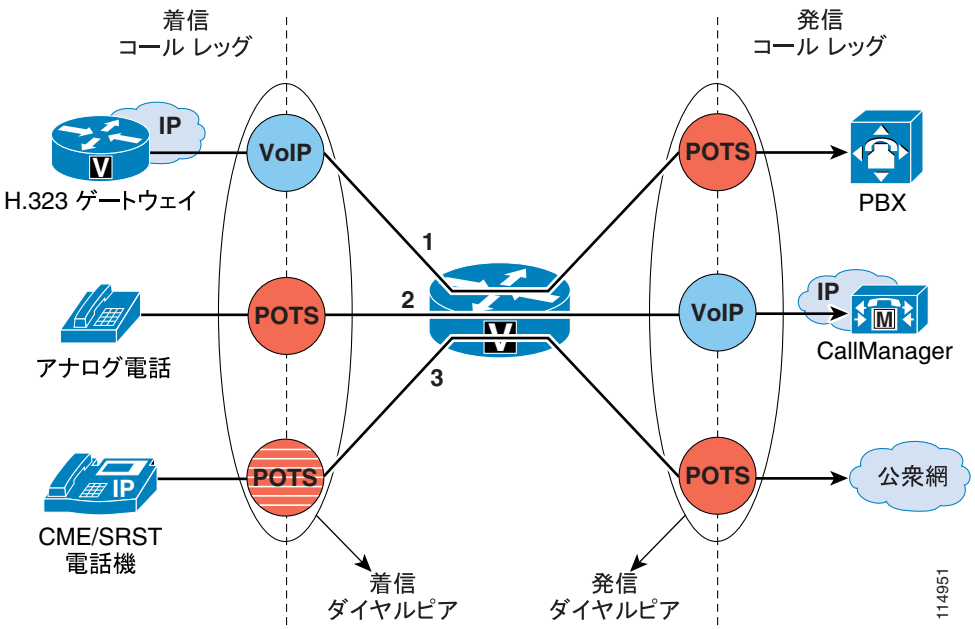
Cisco IOS は、ルータを通過するすべてのコールについて、1 つのダイヤル ピアを各コール レッグに関連付けます。ダイヤル ピアにも、関連付け先となるコール レッグのタイプに応じて、次に示す主に 2 つのタイプがあります。

- 従来の TDM テレフォニー コール レッグに関連付けられる、POTS ダイヤル ピア
- IP コール レッグに関連付けられる、VoIP ダイヤル ピア

図 10-17 では、Cisco IOS ルータを通過する、次の各種コールの例を示しています。

- コール 1 は、IP ネットワークにある別の H.323 ゲートウェイから、ルータに接続されている従来の（たとえば、PRI インターフェイス経由の）PBX までです。このコールに対しては、着信 VoIP ダイヤル ピアと発信 POTS ダイヤル ピアが選択されます。
- コール 2 は、ルータの FXS ポートに接続されているアナログ電話機から、IP ネットワークにある Cisco Unified CallManager クラスタまでです。このコールに対しては、着信 POTS ダイヤル ピアと発信 VoIP ダイヤル ピアがルータによって選択されます。
- コール 3 は、Cisco Unified CallManager Express または SRST の制御する IP Phone から、ルータ上の公衆網インターフェイス（たとえば、PRI インターフェイス）までです。このコールに対しては、自動生成の POTS ダイヤル ピア（ルータ上に設定されている **ephone** に対応します）と発信 POTS ダイヤル ピアが選択されます。

図 10-17　着信ダイヤル ピアと発信ダイヤル ピア



着信コール レッグを着信ダイヤル ピアと対応付けるために、ルータは、セットアップ メッセージ内の情報要素（着信番号 /DNIS と発信番号 /ANI）が 4 つの設定可能ダイヤル ピア属性と一致するかどうか調べることによって、ダイヤル ピアを選択します。ルータは、これらの項目が一致するかどうかを次の順序で調べます。

1. 着信番号と **incoming called-number**
2. 発信番号と **answer-address**
3. 着信番号と **destination-pattern**
4. 着信音声ポートと設定済み音声ポート

ルータで必要となるのは、これらの条件のいずれか 1 つのみ一致することです。すべての属性をダイヤル ピア内に設定する必要はなく、すべての属性がコール セットアップ情報に一致している必要はありません。ルータがダイヤル ピアを選択するために必要な条件は 1 つのみです。ルータは、1 つのダイヤル ピアが一致するとすぐに検索を停止し、コールは設定済みのダイヤル ピア属性に従ってルーティングされます。一致するダイヤル ピアが他にある場合でも、最初に一致したピアのみが使用されます。

ルータが発信ダイヤル ピアを選択する方法は、着信 POTS ダイヤル ピアに **direct-inward-dial**（DID）が設定されているかどうかによって異なります。

- 着信 POTS ダイヤル ピアに DID が設定されていない場合、ルータは 2 段階ダイヤリングを実行し、着信ダイヤル ストリングを 1 桁ずつ収集します。1 つのダイヤル ピアが宛先パターンに一致すると、ルータは一致したダイヤル ピアの設定済み属性を使用して、コールをただちに発信します。
- 着信 POTS ダイヤル ピアに DID が設定されている場合、ルータは着信番号全体を使用して、発信ダイヤル ピアに含まれている宛先パターンに一致するかどうかを調べます。DID を使用する場合は、コールのルーティングに必要な番号がセットアップ メッセージにすべて含まれているため、番号をそれ以上収集する必要がありません。複数のダイヤル ピアがダイヤル ストリングに一致した場合、一致するすべてのダイヤル ピアが「ハント グループ」の形成に使用されます。ルータは、発信コール レッグを確立できるまで、ハント グループに含まれているすべてのダイヤル ピアを使用して確立を試行します。

デフォルトでは、ハント グループ内のダイヤル ピアは、次の基準を使用して、この順序に従って選択されます。

1. 電話番号の最長一致

   この方法では、ダイヤルされた番号と一致している部分が最も長い宛先パターンが選択されます。たとえば、あるダイヤル ピアがダイヤル ストリング 345.... を使用して設定され、2 番目のダイヤル ピアが 3456789 を使用して設定されている場合、ルータはまず 3456789 を選択します。2 つのダイヤル ピアのうち、正確に一致している部分が最も長いためです。

2. 明示的プリファレンス

   この方法では、**preference** ダイヤル ピア コマンドで設定した優先順位を使用します。プリファレンスの数値が小さくなるほど、優先順位が高くなります。最高の優先順位は、プリファレンス順位 0 のダイヤル ピアに与えられます。同じ宛先パターンを持つ複数のダイヤル ピアに対して同じ優先順位が定義されている場合、ダイヤル ピアはランダムに選択されます。

3. ランダム選択

   この方法では、すべての宛先パターンが同等の重みになります。

このデフォルト選択順序を変更することも、**dial-peer hunt** グローバル設定コマンドを使用して、別のダイヤル ピア ハンティング方法を選択することもできます。このほかの選択基準は、「最長待機時間」です。最後に選択された時点から、最も長く待機している宛先パターンを選択します（Cisco Unified CallManager 回線グループの「最長アイドル時間」に相当します）。

Cisco IOS ルータ上で H.323 ダイヤル ピアを設定するときは、次のベスト プラクティスに従ってください。

- 着信公衆網コールが　DNIS　情報に基づいて宛先に直接ルーティングされるようにするには、**direct-inward-dial** 属性を使用して、次のようにデフォルト POTS ダイヤル ピアを作成します。

```
dial-peer voice 999 pots
  incoming called-number .
  direct-inward-dial
  port 1/0:23
```

- ルータを Cisco Unified CallManager クラスタに接続されている H.323 ゲートウェイとして使用する場合は、同じ宛先パターンを持ち、2 つの異なる Cisco Unified CallManager サーバを指す VoIP ダイヤル ピアを少なくとも 2 つ設定して、冗長性を実装します。プライマリとセカンダリの Cisco Unified CallManager サーバ間での優先順位を選択するには、**preference** 属性を使用します。次に **preference** 属性の使用例を示します。

```
dial-peer voice 100 voip
 preference 1

!--- Make this the first choice dial peer.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.2

!--- This is the address of the primary Cisco Unified CallManager.

 dtmf-relay h245-alpha


dial-peer voice 101 voip
 preference 2

!--- This  is the second choice.

 ip precedence 5
 destination-pattern 1...
 session target ipv4:10.10.10.3

!--- This is the address of the secondary Cisco Unified CallManager.

 dtmf-relay h245-alpha
```

ゲートキーパーを使用する Cisco IOS でのコール ルーティング

H.323 ゲートキーパーは、H.323 ネットワークにあるエンドポイント（Cisco Unified CallManager Express および Cisco Unified CallManager のクラスタ、H.323 端末、ゲートウェイ、マルチポイント コントロール ユニット（MCU）など）を管理するためのオプション ノードであり、それらのエンドポイントにコール ルーティング機能とコール アドミッション制御機能を提供します。エンドポイントは、H.323 Registration Admission Status（RAS）プロトコルを使用してゲートキーパーと通信します。

エンドポイントは、起動するとゲートキーパーへの登録を試行します。他のエンドポイントとの通信が必要な場合は、E.164 アドレスや電子メール アドレスなど、自身のシンボリック エイリアスを使用して、コールを開始するための許可を要求します。ゲートキーパーは、そのコールを許可してもよいと判断した場合、宛先の IP アドレスを発信元エンドポイントに返します。この IP アドレスは、宛先エンドポイントの実際の IP アドレスではなく、中継アドレスである場合もあります。たとえば、IP-to-IP ゲートウェイや、コール シグナリングをルーティングするゲートキーパーのアドレスです。

H.323 プロトコル、および H.323 エンドポイントとゲートキーパーとのメッセージ交換の詳細については、次の Web サイトで入手可能な『*Cisco IOS H.323 Configuration Guide*』を参照してください。

http://www.cisco.com

Cisco 2600、3600、3700、2800、3800、および 7200 シリーズのルータはすべて、ゲートキーパー機能をサポートします。冗長性、ロード バランシング、および階層コール ルーティング用に、さまざまな方法で Cisco IOS ゲートキーパーを設定できます。ここでは、ゲートキーパー機能のコール ルーティング機能を中心に説明します。冗長性とスケーラビリティに関する考慮事項については、P.8-22 の「ゲートキーパーの冗長性」を参照してください。コール アドミッション制御に関する考慮事項については、P.9-16 の「Cisco IOS ゲートキーパー ゾーン」を参照してください。

Cisco IOS ゲートキーパーのコール ルーティングは、次のタイプの情報に基づいています。

- 静的に設定されている情報（ゾーン プレフィックスや、デフォルト テクノロジー プレフィックスなど）
- 動的な情報（登録フェーズで H.323 デバイスが提供した E.164 アドレスやテクノロジー プレフィックスなど）
- コールごとの情報（着信番号やテクノロジー プレフィックスなど）

ゾーンは、エンドポイント、ゲートウェイ、MCU などの、ゲートキーパーに登録される H.323 デバイスの集合です。アクティブになることができるゲートキーパーは、ゾーンごとに 1 つのみです。1 つのゲートキーパーには、ローカル ゾーンを 100 個まで定義できます。

H.323 エンドポイントがゲートキーパーに登録すると、エンドポイントはゾーンに割り当てられます。また、処理できるコールの種類（音声、ビデオ、ファックスなど）を指定するテクノロジー プレフィックスとともに、処理を担当している 1 つまたはそれ以上の E.164 アドレスを登録することもできます。

ゾーンごとに、ゲートキーパー上で 1 つまたはそれ以上の「ゾーン プレフィックス」を設定できます。ゾーン プレフィックスは、番号とワイルドカードを含んだストリングであり、ゲートキーパーがコール ルーティングの判断に使用します。ゾーン プレフィックス ストリングでは、次の文字を使用できます。

- 0 ～ 9 までのすべての数字。それぞれが特定の 1 桁に対応
- ドット（.）ワイルドカード。いずれかの 1 桁の 0 ～ 9 までの数字に対応
- * ワイルドカード。1 またはそれ以上の桁の 0 ～ 9 までの数字に対応

ゲートキーパーのコール ルーティング動作を理解するには、メッセージ解析ロジックについて考えると役立ちます。図 10-18 では、アドミッション要求（ARQ）の解析ロジックを示しています。エンドポイントは、コールを初期化するために、ARQ（Admission Request ; アドミッション要求）をゲートキーパーに送信します。ARQ には、宛先つまり着信側の H.323 ID または E.164 アドレスのどちらか、および送信元つまり発信側の E.164 アドレスまたは H.323 ID が含まれています。

ARQ に E.164 アドレスが入っている（Cisco Unified CallManager では、ARQ には常に E.164 アドレスが入っています）場合、ARQ にはテクノロジー プレフィックスが含まれている場合と、含まれていない場合があります。ARQ にテクノロジー プレフィックスが含まれている場合、ゲートキーパーはテクノロジー プレフィックスを着信番号から削除します。ARQ にテクノロジー プレフィックスが含まれていない場合、ゲートキーパーは、デフォルトのテクノロジー プレフィックスが設定されていれば、それを使用します（P.10-47 の「集中型ゲートキーパー設定」の項の **gw-type-prefix** コマンドを参照）。このように取得したテクノロジー プレフィックスは、メモリに格納され、ゲートキーパーはコール ルーティング アルゴリズムに基づく処理を続行します。

次に、ゲートキーパーは、着信番号が設定済みのいずれかのゾーン プレフィックスに一致しないかどうかを調べます。一致する可能性のあるエントリが複数ある場合は、一致する部分の最も長いものが使用されます。一致するゾーン プレフィックスがない場合、未知のプレフィックスを持つコールを受け付けるようにゲートキーパーが設定されているときは、ゲートキーパーは宛先ゾーンが発信元ゾーンと同じであると想定します。

この時点で、ゲートキーパーは選択された宛先ゾーン内を検索して、着信番号に一致する登録済み E.164 アドレスがあるかどうかを調べます。一致が見つかると、コールに関して要求した帯域幅が使用可能になっていて、着信側エンドポイントがゲートキーパーに登録されている場合、ゲートキーパーはアドミッション確認（ACF）を送信します。ACF には、宛先エンドポイントの IP アドレスが入っています。帯域幅が使用不能であるか、着信側エンドポイントが登録されない場合、ゲートキーパーは、発信側エンドポイントに ARJ（Admission Reject ; アドミッション拒否）を戻します。

一致する E.164 アドレスが宛先ゾーン内に登録されていない場合、ゲートキーパーは、以前に格納したテクノロジー プレフィックスを使用して、そのゾーンに登録されているゲートウェイをコールの宛先として選択します。ゲートキーパーが ACF または ARJ のどちらを発信元エンドポイントに送信するかは、帯域幅の可用性とエンドポイントの登録に関する、上と同じ考慮事項に基づいて決まります。

送信元エンドポイントは、ゲートキーパーから ACF を受信した後、ACF で戻された IP アドレスを使用して、直接セットアップ メッセージを宛先エンドポイントに送信できます。

図 10-18　ARQ のゲートキーパー アドレス解決

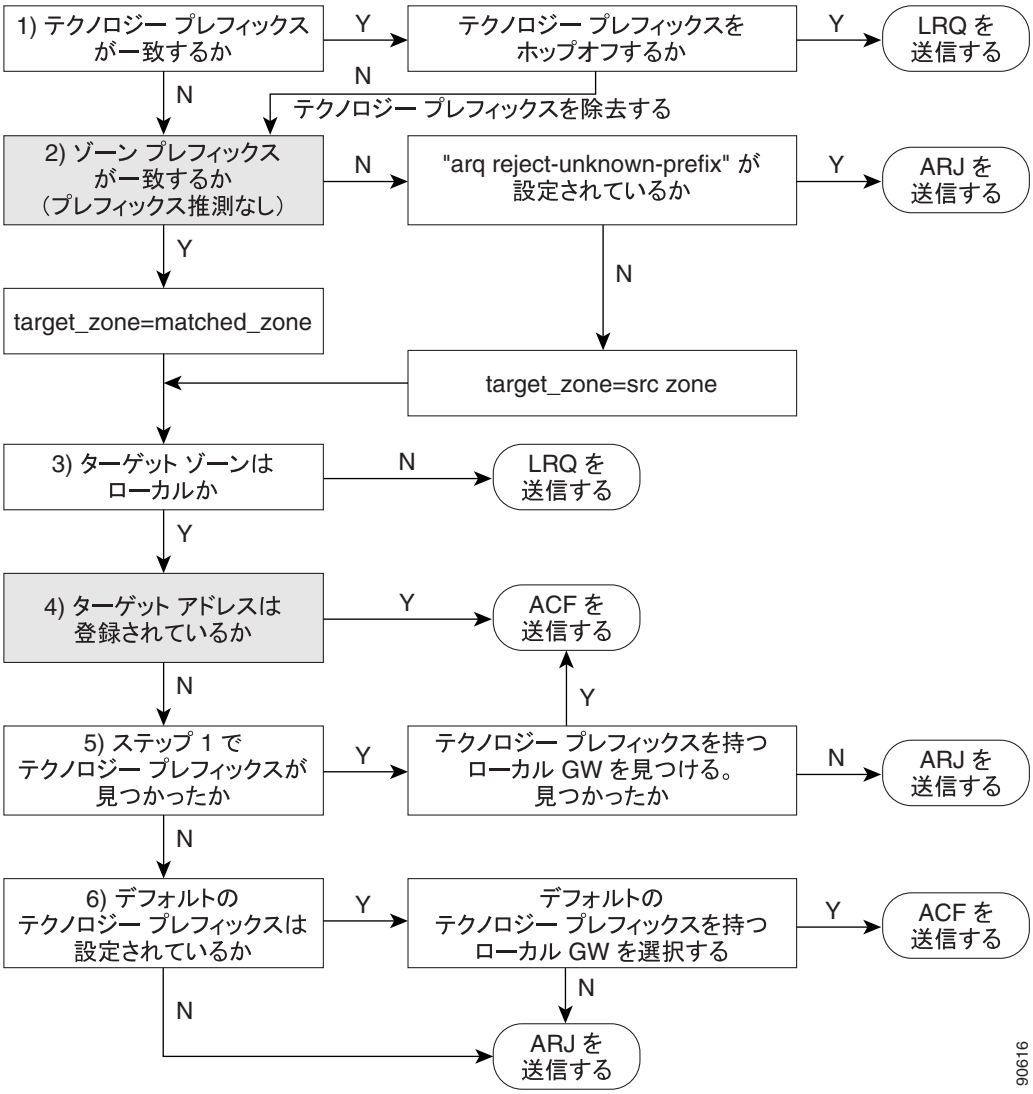
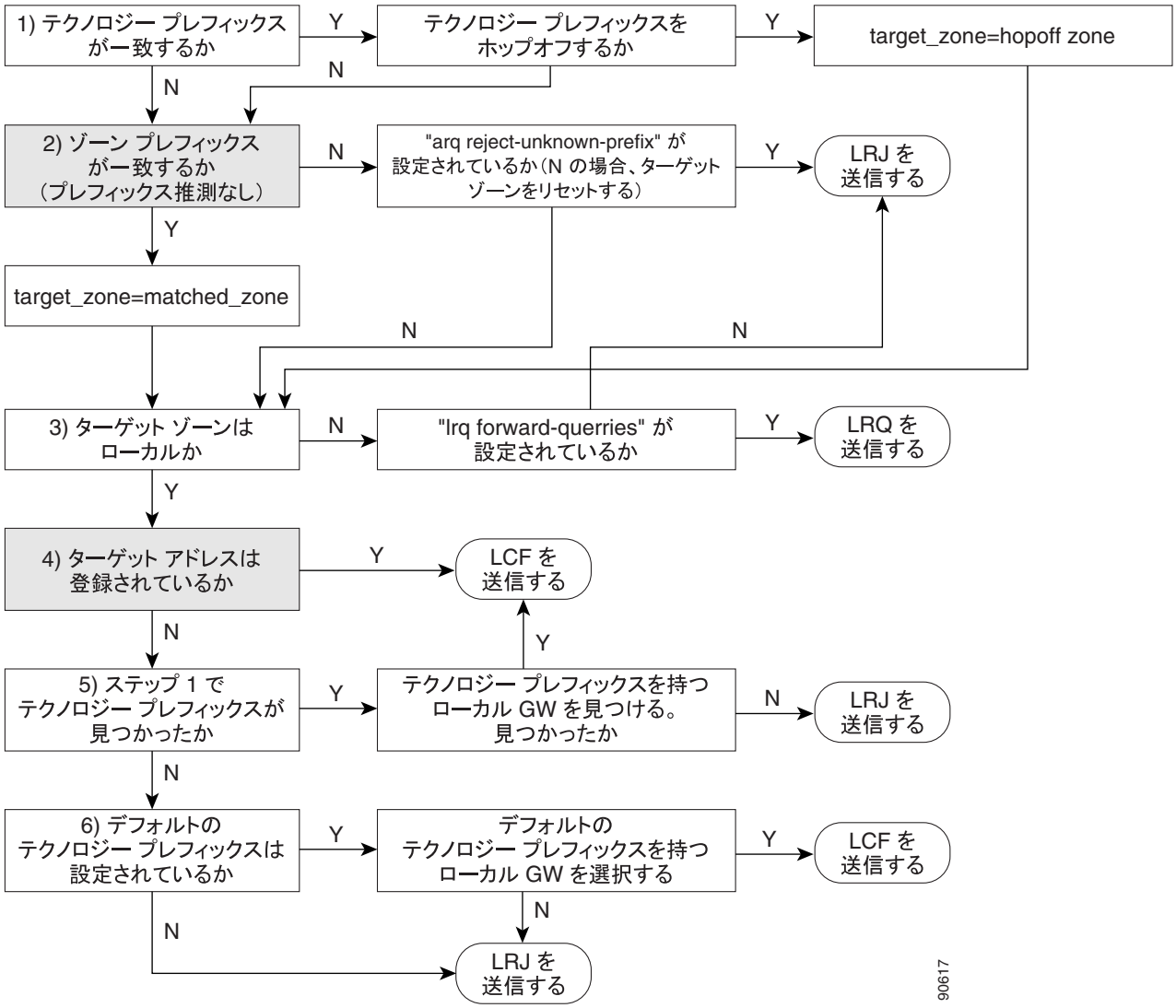


図 10-19 では、ロケーション要求（LRQ）の解析ロジックを示しています。LRQ メッセージは、ゲートキーパー間で交換され、ゾーン（リモート ゾーン）間のコールに使用されます。たとえば、ゲートキーパー A が ARQ をローカル ゾーンのゲートウェイから受信し、その ARQ は、リモート ゾーンのデバイスに対するコール アドミッションを要求しているとします。ゲートキーパー A は、ゲートキーパー B に LRQ メッセージを送信します。ゲートキーパー B は、自身がゾーン間コール要求を許可するように設定されているかどうか、および要求されたリソースが登録されているかどうかに応じて、この LRQ メッセージにロケーション確認（LCF）メッセージまたはロケーション拒否（LRJ）メッセージで応答します。

図 10-19　LRQ のゲートキーパー アドレス解決



従来の Cisco IOS ゲートキーパー機能は、「中継ゾーン」ゲートキーパーという概念を通じて、IP-to-IP ゲートウェイに対応するように拡張されました。配置の例については、P.9-30 の「RSVP 機能のある Cisco IOS Gatekeeper および IP-to-IP ゲートウェイ」を参照してください。

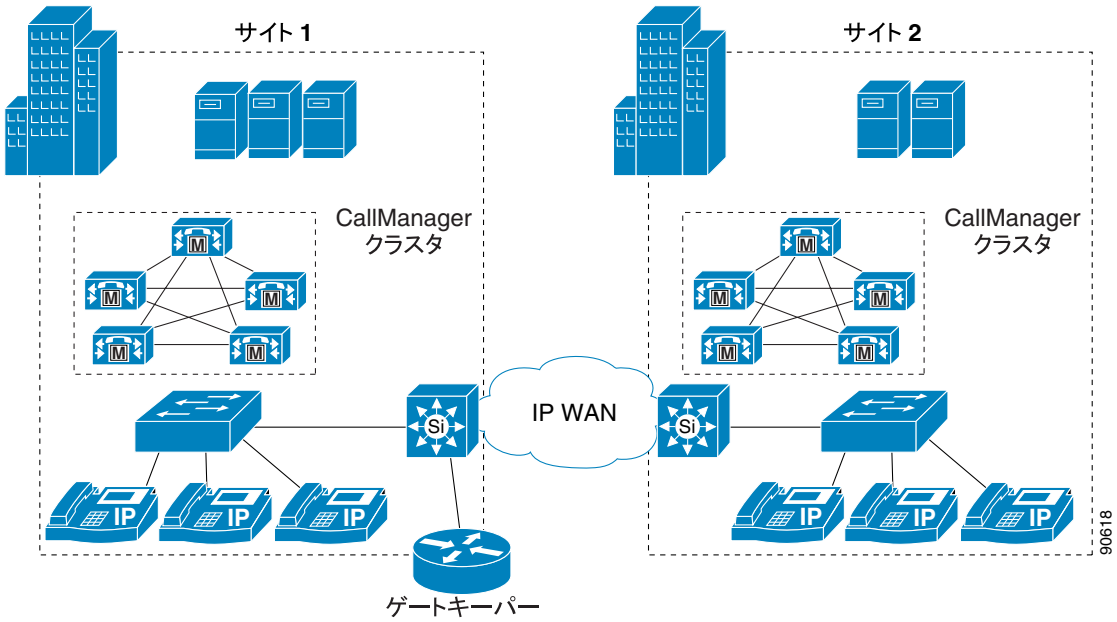
中継ゾーン ゲートキーパーがレガシー ゲートキーパーと異なっている点は、コール ルーティングでの LRQ メッセージと ARQ メッセージの使用方法です。中継ゾーン ゲートキーパーを使用しても、通常のクラスタおよび機能はそのまま使用できます。レガシー ゲートキーパーは、着信する LRQ を着信番号に基づいて検査します。具体的には、LRQ の destinationInfo 部分にある dialedDigits フィールドを検査します。中継ゾーン ゲートキーパーは、着信番号を検査する前に LRQ の発信地点を検査します。LRQ が、中継ゾーン ゲートキーパーのリモート ゾーン設定にリストされているゲートキーパーから送信されている場合、ゲートキーパーは、ゾーンのリモート設定に **invia** キーワードまたは **outvia** キーワードが含まれているかどうかを確認します。設定にこれらのいずれかのキーワードが含まれている場合、ゲートキーパーは中継処理をします。含まれていない場合は、従来の処理をします。

ARQ メッセージの場合、ゲートキーパーは宛先ゾーンに **outvia** キーワードが設定されているかどうかを調べます。**outvia** キーワードが設定されていて、**outvia** キーワードを使用して命名されているゾーンがゲートキーパーに対してローカルである場合は、そのゾーンの IP-IP ゲートウェイがポイントされている ACF が返され、コールは IP-IP ゲートウェイに転送されます。**outvia** キーワードを使用して命名されているゾーンがリモートである場合、ゲートキーパーは、ロケーション要求（LRQ）をリモート ゾーンのゲートキーパーではなく **outvia** ゲートキーパーに送信します。**invia** キーワードは、ARQ の処理では使用されません。

集中型ゲートキーパー設定

単一のゲートキーパーは、クラスタ間のコール ルーティング、および最大 100 の Cisco Unified CallManager クラスタに対するコール アドミッション制御をサポートできます。図 10-20 では、2 つの Cisco Unified CallManager クラスタと単一の集中型ゲートキーパーを備えた分散型コール処理環境を示しています。

図 10-20　2 つのクラスタをサポートする集中型ゲートキーパー



例 10-1 では、図 10-20 のゲートキーパー設定を示しています。

例 10-1　集中型ゲートキーパーの設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone local GK-Site2 customer.com
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth interzone GK-Site1 160
 bandwidth interzone GK-Site2 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、図 10-20 について説明します。

- Cisco Unified CallManager トランク登録をサポートするために、各 Cisco Unified CallManager クラスタにはローカル ゾーンが設定されます。
- ゾーン間とクラスタ間のコール ルーティングを可能にするために、ゾーンごとにゾーン プレフィックスが設定されます。
- サイトごとに帯域幅ステートメントが設定されます。シスコでは、**bandwidth interzone** コマンドを使用することをお勧めします。**bandwidth total** コマンドを使用すると、設定内容によっては問題が発生することがあるためです。帯域幅はキロビット / 秒（kbps）単位で測定されます。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。

  テクノロジー プレフィックスは、発信されているコールのタイプを示しています。テクノロジー プレフィックスとして使用される個々の値は任意のものであり、ネットワーク管理者が定義します。配置全体で常に同じ値を使用する必要があります。

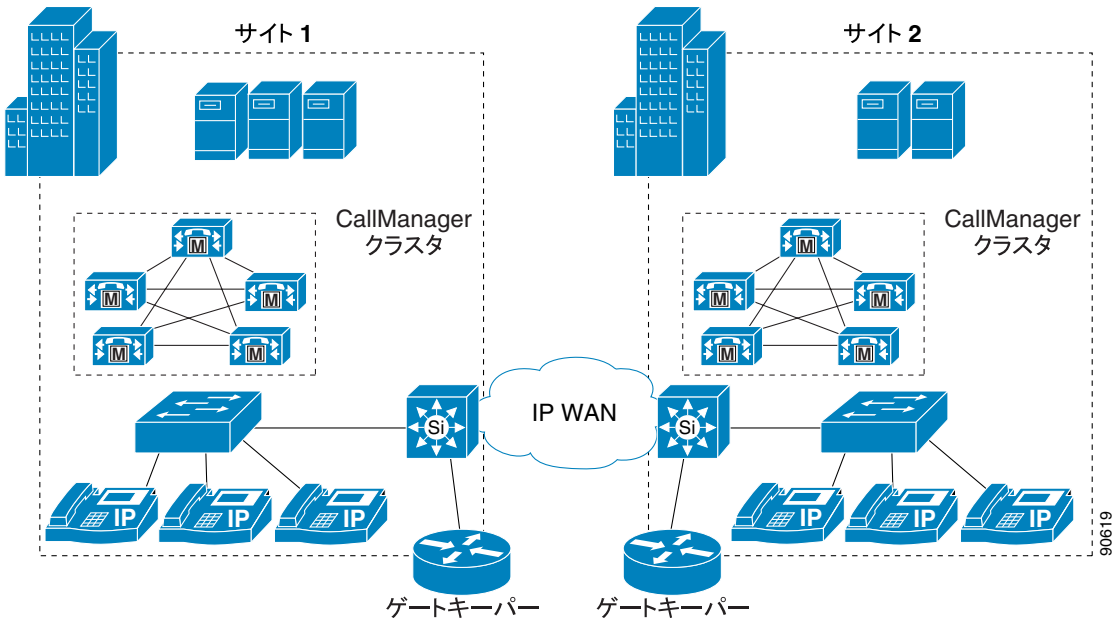
  テクノロジー プレフィックスは、E.164 アドレス（電話番号）のプレフィックスとして送信され、コールが音声であるか、ビデオであるか、その他のタイプであるかを示します。# シンボルは、一般に、プレフィックスと E.164 番号を区別するために使用します。プレフィックスが含まれていない場合、コールのルーティングにはデフォルトのテクノロジー プレフィックスが使用されます。配置全体で 1 つのデフォルト テクノロジー プレフィックスだけが使用される場合があります。

  Cisco IOS ゲートウェイは、プレフィックスが設定されていれば、自動的に発信コールにテクノロジー プレフィックスを追加します。ゲートウェイは、自動的に着信 H.323 コールからプレフィックスを除去します。Cisco Unified CallManager は、ゲートキーパー制御 H.323 トランクの設定ページで指定されているテクノロジー プレフィックスを使用して、ゲートキーパーに登録することができます。ただし、このテクノロジー プレフィックスは、ゲートキーパーに向かう発信コールに自動的に追加されることはありません。また、Cisco Unified CallManager に向かう着信コールから自動的に除去されることもありません。トランスレーション パターンとゲートウェイ コンフィギュレーションを使用して着信番号を操作すると、テクノロジー プレフィックスを必要に応じて追加または除去できます。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

分散型ゲートキーパー設定

帯域幅を節約するため、または WAN 障害時に H.323 ゲートウェイにローカル コール ルーティングをサポートするために、ゲートキーパーを分散させることができます。図 10-21 は、2 つのクラスタと 2 つのゲートキーパーを備えた分散型コール処理環境を示しています。

図 10-21　2 つのクラスタをサポートする分散型ゲートキーパー



例 10-2 は、図 10-21 のサイト 1 に対するゲートキーパー設定を示しています。

例 10-2　サイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408.......
 zone prefix GK-Site2 212.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-2 について説明します。

- ローカル Cisco Unified CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 2 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

例 10-3 は、図 10-21 のサイト 2 に対するゲートキーパー設定を示しています。

例 10-3　サイト 2 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site2 customer.com 10.1.11.100
 zone remote GK-Site1 customer.com 10.1.10.100
 zone prefix GK-Site2 212.......
 zone prefix GK-Site1 408.......
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-3 について説明します。

- ローカル Cisco Unified CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- サイト 1 のゲートキーパーへのコール ルーティング用に、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。
- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

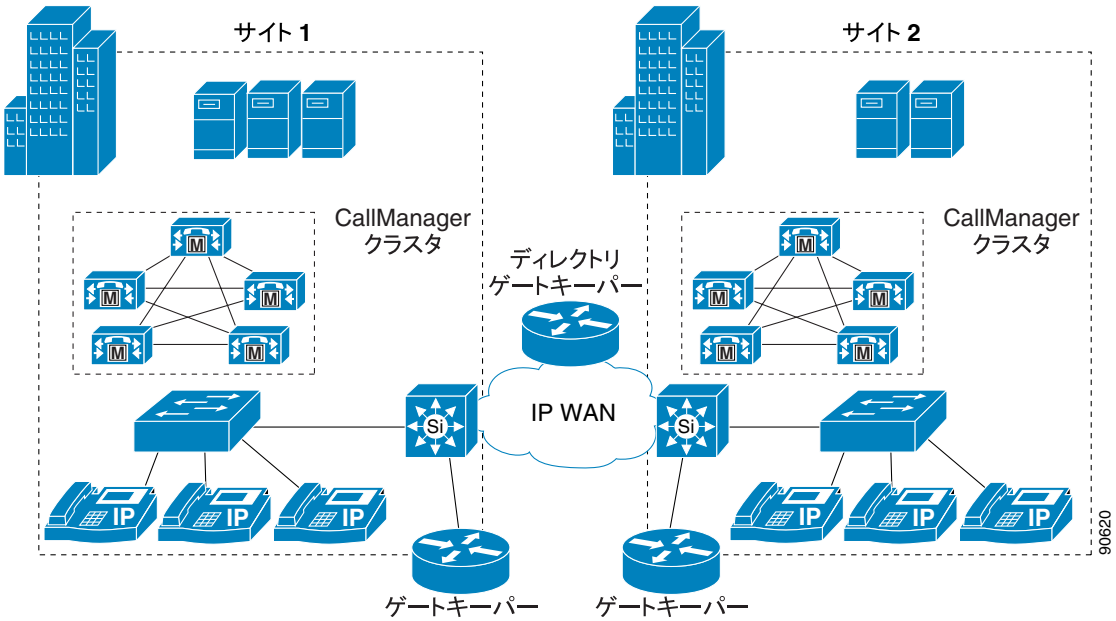
ディレクトリ ゲートキーパーを使用した分散型ゲートキーパー設定

ゲートキーパー ルーティング テーブルを更新するために使用できるゲートキーパー プロトコルがないので、ディレクトリ ゲートキーパーを使用すると、分散型ゲートキーパー設定のスケーラビリティとマネージャビリティの向上に役立ちます。ディレクトリ ゲートキーパーを実装すると、各サイトのゲートキーパー設定が簡単になり、ゾーン間通信の大部分の設定をディレクトリ ゲートキーパーでできるようになります。

ディレクトリ ゲートキーパーがない場合、ゲートキーパーに新しいゾーンを追加するたびに、ネットワーク上のすべてのゲートキーパーに項目を追加する必要があります。しかし、ディレクトリ ゲートキーパーを使用すると、ローカル ゲートキーパーとディレクトリ ゲートキーパーのみで新しいゾーンを追加できます。ローカル ゲートキーパーは、コール要求をローカル側で解決できない場合、ゾーン プレフィックスが一致するディレクトリ ゲートキーパーにその要求を転送します。

図 10-22 では、ローカル コール ルーティング用の分散型ゲートキーパー、およびゲートキーパー間のコール ルーティングをサポートするディレクトリ ゲートキーパーを備えた、Cisco Unified CallManager 分散型コール処理環境を示しています。

図 10-22　ディレクトリ ゲートキーパーを備えた分散ゲートキーパー



例 10-4 では、図 10-22 のサイト 1 に対するゲートキーパー設定を示しています。この例では、サイト 1 とサイト 2 のゲートキーパー設定がほぼ同じなので、ここでは、サイト 1 だけについて説明します。

例 10-4　ディレクトリ ゲートキーパーを使用したサイト 1 のゲートキーパー設定

```
gatekeeper
 zone local GK-Site1 customer.com 10.1.10.100
 zone remote DGK customer.com 10.1.10.101
 zone prefix GK-Site1 408.......
 zone prefix DGK ..........
 bandwidth remote 160
 gw-type-prefix 1#* default-technology
 arq reject-unknown-prefix
 no shutdown
```

ここでは、例 10-4 について説明します。

- ローカル Cisco Unified CallManager クラスタ トランクの登録用に、ローカル ゾーンが設定されます。
- ディレクトリ ゲートキーパー用にリモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のゾーンにゾーン プレフィックスが設定されます。
- ディレクトリ ゲートキーパーのゾーン プレフィックスは、10 個のドットを使用して設定されます。このパターンは、未解決の任意の 10 桁のダイヤル ストリングと一致します。1 つのゾーンに複数のゾーン プレフィックスを設定して、異なる長さのダイヤル ストリングを一致させることができます。ディレクトリ ゲートキーパーのゾーン プレフィックスにもワイルドカード（*）を使用できますが、この方法はコール ルーティングの問題が発生する場合があります。
- ローカル ゾーンとその他の任意のリモート ゾーンとの間の帯域幅を制限するために、**bandwidth remote** コマンドを使用します。
- **gw-type-prefix 1# default-technology** コマンドを使用すると、ローカルで解決されないすべてのコールをローカル ゾーン内でテクノロジー プレフィックス 1# に登録されたデバイスに転送できます。この例では、すべての Cisco Unified CallManager トランクは、1# プレフィックスに登録されるように設定されています。

- **arq reject-unknown-prefix** コマンドは、冗長 Cisco Unified CallManager トランク上にできるコール ルーティング ループを回避します。

例 10-5 では、図 10-22 の例のディレクトリ ゲートキーパー設定を示しています。

例 10-5　ディレクトリ ゲートキーパー設定

```
gatekeeper
 zone local DGK customer.com 10.1.10.101
 zone remote GK-Site1 customer.com 10.1.10.100
 zone remote GK-Site2 customer.com 10.1.11.100
 zone prefix GK-Site1 408*
 zone prefix GK-Site2 212*
 lrq forward-queries
 no shutdown
```

ここでは、例 10-5 について説明します。

- ディレクトリ ゲートキーパー用にローカル ゾーンが設定されます。
- リモート ゲートキーパーごとに、リモート ゾーンが設定されます。
- ゾーン間コール ルーティング用に、両方のリモート ゾーンにゾーン プレフィックスが設定されます。設定を簡単にするために、ゾーン プレフィックスでワイルドカード（*）が使用されます。コールは DGK ゾーンにルーティングされないので、DGK ゾーンにはプレフィックスが必要ありません。
- **lrq forward-queries** コマンドは、ディレクトリ ゲートキーパーが、別のゲートキーパーから受信した LRQ を転送できるようにします。

H.323 ダイヤル ピアを使用する Cisco IOS のコール特権

H.323 を使用する Cisco IOS ベースのシステム（H.323 ゲートウェイ、SRST、および Cisco Unified CallManager Express を含む）にコール特権を実装するには、クラス制限（COR）機能を使用します。この機能は、ネットワークの設計に柔軟性をもたらし、管理者は、すべてのユーザに関して任意のコールをブロックできるようになります（たとえば、米国では 900 番号へのコール）。また、個々の発信者のコール試行に対して、それぞれ別のコール特権を適用できます（一部のユーザには国際通話を許可し、他のユーザには許可しない、など）。

COR 機能の中心となる基本的メカニズムは、着信と発信の「COR リスト」を定義することで成立しています。このリストは既存のダイヤル ピアに関連付けるもので、着信および発信という概念は、Cisco IOS ルータに対してのものです（ダイヤル ピアの場合と同様）。各 COR リストは、メンバーの番号を含めることで定義します。この番号は、Cisco IOS 内に定義済みの単純なタグです。

コールがルータを通過するときには、Cisco IOS ダイヤル ピア ルーティング ロジックに基づいて、着信ダイヤル ピアと発信ダイヤル ピアが選択されます。選択されたダイヤル ピアに COR リストが関連付けられている場合は、コールをルーティングする前に、さらに次のチェックが実行されます。

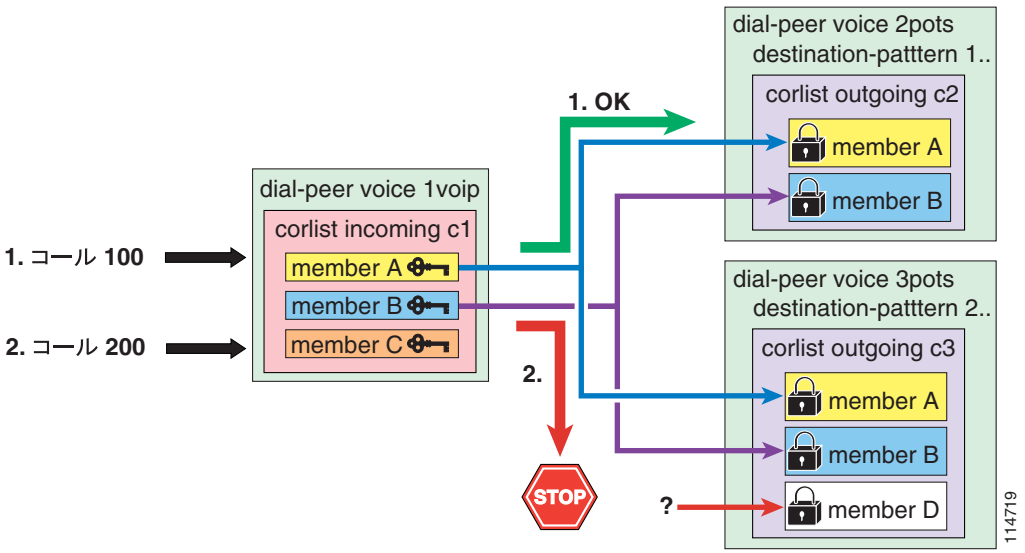
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットである場合、コールは許可されます。
- 発信ダイヤル ピアに関連付けられている発信 COR リストのメンバーが、着信ダイヤル ピアに関連付けられている着信 COR リストのメンバーのサブセットではない場合、コールは拒否されます。

COR リスト ステートメントが一切適用されていないダイヤル ピアが存在する場合は、次のプロパティが適用されます。

- ダイヤル ピア上に着信 COR リストが設定されていない場合は、デフォルトの着信 COR リストが使用されます。デフォルト着信 COR リストは最高の優先順位を持っているため、発信 COR リストの内容にかかわらず、このダイヤル ピアは他のすべてのダイヤル ピアにアクセスできます。
- ダイヤル ピア上に発信 COR リストが設定されていない場合は、デフォルトの発信 COR リストが使用されます。デフォルト発信 COR リストは優先順位が最も低いため、着信 COR リストの内容にかかわらず、他のすべてのダイヤル ピアがこのダイヤル ピアにアクセスできます。

この動作の内容を最もよく表しているのが、図 10-23 に示す例です。この例では、1 つの VoIP ダイヤル ピアと 2 つの POTS ダイヤル ピアが定義されています。

図 10-23　COR の動作の例



この VoIP ダイヤル ピアは、メンバー A、B、C を持つ着信 COR リスト c1 に関連付けられています。着信 COR リストのメンバーは、「鍵」だと考えることができます。

最初の POTS ダイヤル ピアは、宛先パターン 1.. を持っており、メンバー A と B を持つ発信 COR リスト c2 に関連付けられています。2 番目の POTS ダイヤル ピアは、宛先パターン 2.. を持っており、メンバー A、B、D を持つ発信 COR リスト c3 に関連付けられています。発信 COR リストのメンバーは、「錠」だと考えることができます。

コールが成功するには、発信ダイヤル ピアの発信 COR リストにあるすべての「錠」を開けるための「鍵」を、着信ダイヤル ピアの着信 COR リストがすべて持っている必要があります。

図 10-23 に示した例では、宛先が 100 になっている最初の VoIP コールがルータに受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが最初の POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c2 発信 COR リストの錠（A と B）に必要な鍵をすべて持っているため、コールは成功します。

次に、宛先が 200 になっている 2 番目の VoIP コールがルータで受信されます。Cisco IOS コール ルーティング ロジックによって、着信コール レッグが VoIP ダイヤル ピアに、発信コール レッグが 2 番目の POTS ダイヤル ピアに対応付けられます。次に、COR ロジックが適用されます。c1 着信 COR リストは、c3 発信 COR リスト（D）に必要な「鍵」を 1 つ持っていないため、コールは拒否されます。

Cisco IOS で COR 機能を設定するには、次の手順に従います。

ステップ 1　コマンド **dial-peer cor custom** を使用して、COR リスト メンバーとして使用される「タグ」を定義します。

ステップ 2　コマンド **dial-peer cor list** *corlist-name* を使用して、COR リストを定義します。

ステップ 3　COR リストを既存の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けます。このためには、ダイヤル ピアの設定で、コマンド **corlist** {**incoming** | **outgoing**} *corlist-name* を使用します。

Cisco IOS Release 12.2(8)T 以降では、COR 機能を SRST 制御の IP Phone に適用できます。IP Phone は、SRST ルータに対して動的に登録を実行します。このため、SRST では、IP Phone が Cisco Unified CallManager クラスタへの接続を失うときまで、個々の IP Phone について事前には一切把握していません。したがって、COR 機能の SRST 用の設定は、電話の DN に基づいています。SRST ルータに登録するとき、IP Phone は自身の DN をルータに通知して、SRST ルータが IP Phone を適切な COR リストに割り当てられるようにします。

SRST によって制御される IP Phone のための COR を設定するには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* {*corlist-number starting-number – ending-number* | **default**} を **call-manager-fallback** 設定モードで使用します。

このコマンドには、次の制限事項があります。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor** {**incoming** | **outgoing**} ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

COR 機能は、Cisco IOS Release 12.2(8)T 以降を使用する Cisco Unified CallManager Express にも配置できます。個々の IP Phone は、Cisco Unified CallManager Express で具体的に設定されます。したがって、COR リストを IP Phone 自体に直接適用することができます。このためには、コマンド **cor** {**incoming** | **outgoing**} *corlist-name* を各 IP Phone の **ephone-dn** *dn-tag* 設定モードで使用します。

これらの概念を実際に適用する方法の例については、P.10-92 の「H.323 を使用している Cisco IOS でのサービス クラスの構築」の項を参照してください。

Cisco SRST と Cisco Unified CallManager Express の設定の詳細については、次の Web サイトで入手可能な『*Cisco SRST 3.0 System Administrator Guide*』および『*Cisco Unified CallManager Express 3.1 System Administrator Guide*』を参照してください。

http://www.cisco.com

H.323 ダイヤル ピアを使用する Cisco IOS での番号操作

H.323 を実行している Cisco IOS ルータでは、番号操作は音声トランスレーション プロファイルを通じて実行されます。このプロファイルは、音声コールの発信番号（ANI）または着信番号（DNIS）の番号を操作するために、またはコールの番号タイプを変更するために使用されるものです。

音声トランスレーション プロファイルは、Cisco IOS Release 12.2(11)T 以降で使用できます。このプロファイルは、コールが着信ダイヤル ピアに対応付けられる前、またはコールが発信ダイヤル ピアによって転送される前に、電話番号を別の番号に変換するために使用します。たとえば、社内で 5 桁の内線番号をダイヤルすると、別のサイトにいる従業員に到達できるとします。コールが他のサイトに公衆網を通じてルーティングされ、到達する場合は、発信側のゲートウェイで音声トランスレーション プロファイルを使用する必要があります。これによって、5 桁の内線番号が公衆網で認識される 10 桁の形式に変換されます。

音声トランスレーション プロファイルを設定するには、**voice translation-rule** および **voice translation-profile** Cisco IOS コマンドを使用します。これらのコマンドでは、変換の対象となる番号ストリングを正規表現を使用して定義します。次に、この操作を発信番号、着信番号、転送先着信番号のいずれに関連付けるのかを指定します。音声トランスレーション プロファイルを定義したら、次の任意の要素に適用することができます。

- 特定の音声ポート上で終端する、すべての着信 POTS コール レッグ
- ルータに入るすべての着信 VoIP コール レッグ
- 特定の VoIP ダイヤル ピアまたは POTS ダイヤル ピアに関連付けられている発信コール レッグ
- SRST 制御の IP Phone 上で終端する、すべての着信または発信コール レッグ
- SRST 制御のすべての IP Phone によって発信されるコールのための着信コール レッグ

（注） **voice translation-rule** コマンドを使用する音声トランスレーション プロファイルは、以前に **translation-rule** コマンドで提供されていた機能を置き換え、拡張するものです。この新しいコマンドの構文は、以前のコマンドで使用されていた構文とは異なります。詳細については、http://www.cisco.com で入手可能な『*Cisco IOS Voice Command Reference*』（Release 12.2(11)T 以降）の **voice translation-rule** を参照してください。

音声トランスレーション プロファイルの一般的な用途は、IP WAN が使用不可になっていてルータが SRST モードで動作している場合でも、支店サイトからのオンネット サイト間ダイヤリング手順をそのまま維持できるようにすることです。たとえば、中央サイトが San Jose にあり、3 つのリモート サイトが San Francisco、New York、Dallas にある単純な配置について考えます。表 10-4 では、この例の DID 範囲と内部サイト コードを示しています。

表 10-4　変換規則応用例の DID 範囲とサイト コード

	San Jose	San Francisco	New York	Dallas
DID 範囲	(408) 555-1XXX	(415) 555-1XXX	(212) 555-1XXX	(972) 555-1XXX
サイト コード	1	2	3	4

サイト間のコールは、オンネット アクセス コード 8 の次に 1 桁のサイト コードと着信側の 4 桁内線番号をダイヤルすることによって、通常は IP WAN 経由で発生します。IP WAN がダウンしていて Cisco SRST がアクティブな場合にも、これらのダイヤル手順を維持できるようにするには、内部の番号を E.164 番号に再変換してから公衆網に送信する必要があります。次に、San Francisco ルータの設定例を示します。

```
voice translation-rule 1
  rule 1 /^81/ /91408555/
  rule 2 /^83/ /91212555/
  rule 3 /^84/ /91972555/

voice translation-profile on-net-xlate
  translate called 1

call-manager-fallback
  translation-profile outgoing on-net-xlate

dial-peer voice 2 pots
  destination-pattern 91[2-9]..[2-9].....
port 1/0:0
  direct-inward-dial
  forward-digits 11
```

この設定では、San Francisco サイトが SRST モードになっているときにユーザが 831000 をダイヤルすると、ルータは **voice translation-rule 1** の **rule 2** と一致するものと判定し、着信番号を 912125551000 に変換します。この新しい番号が使用され、発信ダイヤル ピア（**dial-peer voice 2**）と一致するものと判定されます。

ダイヤル ピアおよびその設定の詳細については、次の Web サイトで入手可能な『*Cisco IOS Voice, Video, and Fax Configuration Guide, Release 12.2*』の「*Configuring Dial Plans, Dial Peers, and Digit Manipulation*」を参照してください。

http://www.cisco.com

Cisco IOS の正規表現構文の詳細については、次の Web サイトで入手可能な『*Regular Expressions*』ドキュメントを参照してください。

http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800ca7e6.html

設計上の考慮事項

この項では、マルチサイト配置について、ダイヤル プランの設計に関する次の考慮事項について説明します。

- P.10-57 の「マルチサイト配置用の設計ガイドライン」では、すべてのマルチサイト配置モデルに当てはまるガイドラインとベスト プラクティスを示します。
- P.10-60 の「ダイヤル プラン アプローチの選択」では、定型オンネット ダイヤリングおよび可変長オンネット ダイヤリングのダイヤル プランを作成するためのさまざまなアプローチを紹介し、この 2 番目のオプションについては、分割アドレッシングとフラット アドレッシングを紹介します。
- P.10-78 の「Cisco Unified CallManager 5.0 を使用する電話機でのダイヤル パターン認識の配置」では、SIP ダイヤル規則を利用して、SIP 電話機が特定のダイヤリング パターンを認識できるようにする方法について説明します。
- 次の各項では、3 つのダイヤル プラン アプローチについて詳しく分析し、それぞれの設定ガイドラインを示します。
  - 定型オンネット ダイヤル プランの配置（P.10-62）
  - 分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置（P.10-64）
  - フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置（P.10-70）
- 次の各項では、Cisco Unified CallManager でサービス クラスを設定する方法について、2 つの代替方法を示します。
  - 従来のアプローチによる Cisco Unified CallManager のサービス クラスの構築（P.10-80）
  - 回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築（P.10-84）
- P.10-92 の「H.323 を使用している Cisco IOS でのサービス クラスの構築」では、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを実装する方法を説明します。
- P.10-96 の「コール カバレッジの配置」では、ハント リストと回線グループを使用して Cisco Unified CallManager にコール カバレッジ機能を実装する場合の、ガイドラインとベスト プラクティスを示します。

マルチサイト配置用の設計ガイドライン

あらゆるマルチサイト IP テレフォニー配置に対して、次のガイドラインとベスト プラクティスが共通して適用されます。複数の Cisco Unified CallManager クラスタが関係する配置については、P.10-59 の「分散型コール処理配置に関する追加の考慮事項」の項も参照してください。

- ルーティング ループを防止するには、どの公衆網ゲートウェイのコーリング サーチ スペースにも、外部ルート パターンを含むパーティションが含まれていないことを確認してください。
- 地域通信事業者（LEC）との間で DID 範囲を取り決めるときは、サイト内で重複が発生しない DID 範囲を選択するようにしてください。たとえば、サイト内で 4 桁ダイヤリングを使用していて、1,000 個の DID ブロックが 2 つ必要な場合、ブロック (408)555-1XXX と (408)999-1XXX は 4 桁番号に短縮すると重複し、着信変換と発信変換が実行されるとさらに複雑な状態になります。
- 緊急番号をダイヤルする方法は、複数用意します。たとえば、北米の場合には、911 と 9.911 の両方を Cisco Unified CallManager で緊急ルート パターンとして設定します。
- Automated Alternate Routing（AAR）を配置する場合は、IP Phone 上に設定されている外部電話番号マスクが、各種 AAR グループによって付加されるどのプレフィックスとも競合しないようにする必要があります。たとえば、複数の国にわたる配置の場合、0 などの国内アクセス コードは、それらがグローバル E.164 アドレスの一部でない限り、マスクに含めないでください。

- クラスタ内の宛先に対するオンネット コールを、強制的に公衆網としてダイヤルさせることができます。このためには、各サイトの E.164 DID 範囲に一致するトランスレーション パターンを追加し、このパターンによって、宛先内線番号に一致するように番号を操作します。ただし、適切な AAR を必ず設定してください。次のいずれかの方法を使用して、IP WAN が帯域幅外になったときに自動公衆網フェールオーバーができるようにします。
  - 「オンネット強制」トランスレーション パターンを含んだパーティションを除外し、公衆網を指す標準ルート パターンを含んだパーティションを含むように、AAR コーリング サーチ スペースを設定します。
  - * などの特殊文字をプレフィックスとして番号に付加する AAR グループを設定し、*9.! や *9.!#（または *0.! や *0.!#）などの追加ルート パターンを標準パーティション内に設定します。

  2 番目の方法を使用することをお勧めします。この方法では、AAR 用の追加コーリング サーチ スペースを定義する必要がないためです。また、追加の * ルート パターンによって、AAR を呼び出さなくても「オンネット強制」設定を上書きして公衆網経由でコールを発信したり、宛先番号が SRST モードの支店内にあるときに公衆網を通じたコールを強制したりすることができる、AAR 用の優れたトラブルシューティング ツールおよびテスト ツールが提供されるためです。
- N 個のサイトがある集中型コール処理クラスタでは、次のいずれかの方法を使用することで、テールエンド ホップオフ（TEHO）を実装できます。
  - 集中型フェールオーバーを使用する TEHO

    この方法では、N 個のルート パターンをグローバル パーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、中央サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。
  - ローカル フェールオーバーを使用する TEHO

    この方法では、N 個のルート パターンを N セット、サイト固有のパーティション内に設定します。各パターンが、適切なリモート サイト ルート グループを最初の選択肢として保持し、ローカル サイト ルート グループを 2 番目の選択肢として保持しているルート リストを指すようにします。

  2 番目の方法では、リモート ゲートウェイや IP WAN が使用不可になった場合に、最も優れたフェールオーバー シナリオを実現できる一方で、ダイヤル プランが非常に複雑になります。最初の方法では、必要になるのは N 個のルート パターンと N 個のルート リストであるのに対して、少なくとも N^2 個のルート パターンと N^2 個のルート リストが必要になるためです。
- 国内の番号計画で許容される場合は、長距離電話としてダイヤルされたローカル公衆網コールを捕捉し、適切な省略形式に変換するための追加トランスレーション パターンを各サイトに設定することをお勧めします。このトランスレーション パターンには、サイト内の電話からのみアクセスできるようにします。このように設定することで、AAR 設定も簡潔化できます（P.10-30 の「同じローカル ダイヤリング エリアに複数のサイトがある場合の特別な考慮事項」を参照）。
- Multilevel Precedence and Preemption（MLPP）機能を使用して、緊急コールに高い優先順位を割り当てないでください。緊急時のコールは、IP テレフォニー システムに緊急コールとして表示されない場合もあります。また、メインの緊急サービス ルーティング番号に新たにコールが発信された場合、既存の緊急コールが終了する恐れがあります。たとえば、緊急時に通常の 10 桁の番号へコールを発信し、医療専門家に連絡することが必要になる場合があります。このコールのプリエンプション処理により、進行中の緊急通信が中止され、緊急時の処理が遅延することがあります。また、救急隊員からの着信コールも MLPP でプリエンプション処理される危険性があります。

(注) 多数のゲートウェイ、ルート パターン、トランスレーション パターン、およびパーティションを含む非常に大きなダイヤル プランをもつ CiscoUnified CallManager クラスタでは、Cisco CallManager Service の初回始動時に、初期化に長い時間がかかる場合があります。デフォルトの時間内にシステムが初期化されない場合、サービス パラメータを変更して、設定の初期化時間を延長してください。サービス パラメータの詳細については、Cisco Unified CallManager Administration オンライン ヘルプの「Service Parameters」を参照してください。

分散型コール処理配置に関する追加の考慮事項

分散型コール処理配置（つまり、複数の Cisco Unified CallManager クラスタを含んでいるマルチサイト配置）のダイヤルプランを設計する場合は、前の項で説明した考慮事項に加えて、次のベストプラクティスに従ってください。

- DID 範囲を複数の Cisco Unified CallManager クラスタにわたって分割することは避けます。分割した場合、経路の集約が不可能になり、クラスタ間ルーティングが非常に困難になります。各 DID 範囲は、それぞれ単一の Cisco Unified CallManager クラスタに配置してください。
- 1 つのリモート サイト内にある複数のデバイスを、静的ロケーションに基づいたコール アドミッション制御を使用して複数の Cisco Unified CallManager クラスタに分割することは避けます。静的ロケーション ベースのコール アドミッション制御が意味を持つのは、1 つのクラスタ内のみです。それぞれ別のクラスタに属している複数のデバイスを同じリモート サイトに配置すると、クラスタ間で使用可能な帯域幅を分割する必要があるため、IP WAN 帯域幅が効率よく使用されなくなります。各リモート サイトは、それぞれ単一の Cisco Unified CallManager クラスタに配置してください。Cisco Unified CallManager 5.0 では、RSVP をロケーションのコール アドミッション制御メカニズムとして設定できるため、単一サイトの合計 WAN 帯域幅を、さまざまなクラスタに属する電話機間で効率よく共有できます。RSVP ベースのコール アドミッション制御を最も効率よく使用するには、リモート サイト内にあるすべての電話機を、Cisco Unified CallManager 5.0 クラスタに設定する必要があります。
- Cisco Unified CallManager クラスタ間でのコール ルーティングには、ゲートキーパー制御クラスタ間トランクを使用します。このようにすると、ネットワーク内でクラスタを簡単に追加および修正できるようになり、他のクラスタをすべて再設定しなくても済みます。
- Cisco Unified CallManager とゲートキーパー間の接続には、冗長性を持たせます。このためには、ゲートキーパー クラスタを使用するか、複数のサーバが設定された Cisco Unified CallManager グループを使用しているデバイス プールに対して、クラスタ間トランクを割り当てます。
- コールをゲートキーパーに送信するときは、着信番号を完全な E.164 アドレスへと展開します。このようにすると、IP WAN が使用不可になった場合の公衆網フェールオーバーが簡単になります。これは、コールを公衆網ゲートウェイ経由で再ルーティングするための追加の番号操作が必要ないためです。また、リモート サイトごとのダイヤル長情報を使用してローカル（発信側）Cisco Unified CallManager を設定する必要がなくなります。
- ゲートキーパー内に、Cisco Unified CallManager クラスタごとにゾーンを 1 つ設定します。クラスタ（ゾーン）ごとに、そのクラスタの所有するすべての DN 範囲に一致するゾーン プレフィックス ステートメントを追加します。
- 次のガイドラインに従うと、複数の Cisco Unified CallManager クラスタにわたってテールエンド ホップオフ（TEHO）を実装することができます。
  - 関係する E.164 範囲の個々のルート パターンを、送信元（発信元）Cisco Unified CallManager クラスタに追加します。これらのパターンでは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持するルート リストを指すようにします。
  - Cisco IOS ゲートキーパー設定に、関係するすべての E.164 範囲のゾーン プレフィックス ステートメントを追加します。これらのステートメントでは、適切な Cisco Unified CallManager クラスタを指すようにします。

— 宛先 Cisco Unified CallManager クラスタに含まれているクラスタ間トランク コーリング サーチ スペースに、ローカル公衆網番号に一致するルート パターンを備えたパーティションを含めます。また、必要に応じて番号操作を適用します（たとえば、コールを公衆網に送信する前にエリア コードを除去します）。

分散型コール処理配置の Cisco IOS ゲートキーパーを設定する方法の詳細については、P.8-22 の「ゲートキーパーの設計上の考慮事項」を参照してください。

ダイヤル プラン アプローチの選択

P.10-3 の「プランニングの考慮事項」で紹介したように、IP テレフォニー システムの内部宛先用のダイヤル プランには、主に次の 2 つのアプローチがあります。

- 定型オンネット ダイヤル プラン：個々の内部宛先には、発信者が同じサイトにいるか、別のサイトにいるかにかかわらず、同じ方法でダイヤルします。
- 可変長オンネット ダイヤル プラン：内部宛先がサイト内にある場合、複数のサイトにわたっている場合とは別の方法でダイヤルします。通常、サイトの内部でやり取りされるコールの場合は 4 桁または 5 桁の省略ダイヤリングを使用し、複数サイトにわたるコールの場合は、完全な E.164 アドレスを使用するか、オンネット アクセス コード、サイト コード、内線番号をこの順序で使用します。

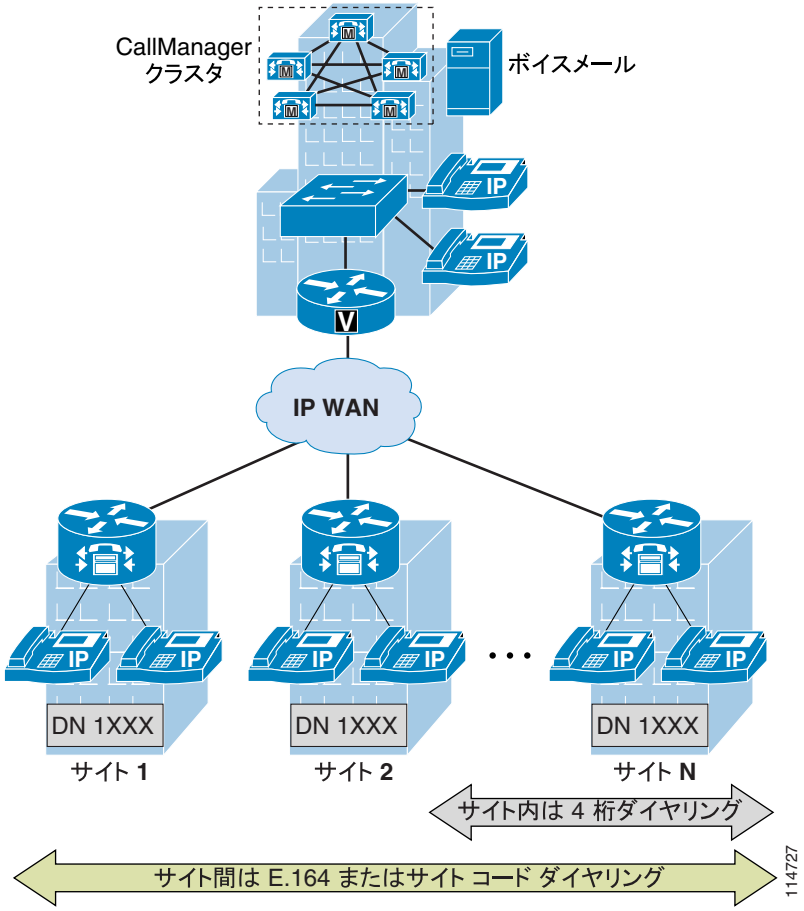
どちらのアプローチが最適かを判断するには、次の基本的な設計上の質問について検討すると役立ちます。

- IP テレフォニー システムによってサービスされるサイトは、最終的にいくつあるか。
- サイト間または支店間の発信パターンは何か。
- サイト内で、および別のサイトに到達するために、ユーザは何をダイヤルするか。
- オンネットサイト間コールに適用されるコール制限はあるか。
- ほとんどのサイト間コールで使用される転送ネットワークは何か（公衆網または IP WAN）。
- CTI アプリケーションが使用されている場合、それは何か。
- サイト コードを使用して、オンネット ダイヤリング構造を標準化する予定はあるか。

定型オンネット ダイヤル プランは、設計と設定が最も簡単です。ただし、このプランが最も適しているのは中小規模の配置であり、サイトおよびユーザの数が大きくなるほど、実用には適さなくなります。このプランについては、P.10-62 の「定型オンネット ダイヤル プランの配置」の項で詳しく説明および分析しています。

可変長オンネット ダイヤル プランは、スケーラビリティが優れていますが、設計と設定も複雑になります。図 10-24 では、可変長オンネット ダイヤル プラン アプローチを使用する大規模配置について、一般的な要件を示しています。

図 10-24　大規模マルチサイト配置の一般的なダイヤリング要件



Cisco Unified CallManager で可変長オンネット ダイヤル プランを実装する方法には、主に次の 2 つがあります。

- 分割アドレッシング

  内部の内線番号は、配置されているサイトに応じて、複数のパーティションに配置します。この方法は、通常はサイト間コールの E.164 アドレスに基づいています。詳細については、P.10-64 の「分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項を参照してください。

- フラット アドレッシング

  内部の内線番号を、すべて同じパーティションに配置します。この方法は、通常はサイト間コールのオンネット サイト コードに基づいています。詳細については、P.10-70 の「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項を参照してください。このアプローチは、サイト間コールに完全な E.164 アドレスを使用している場合でも使用できることがあります。P.10-76 の「サイト コードを使用しない配置に関する特別な考慮事項」の項を参照してください。

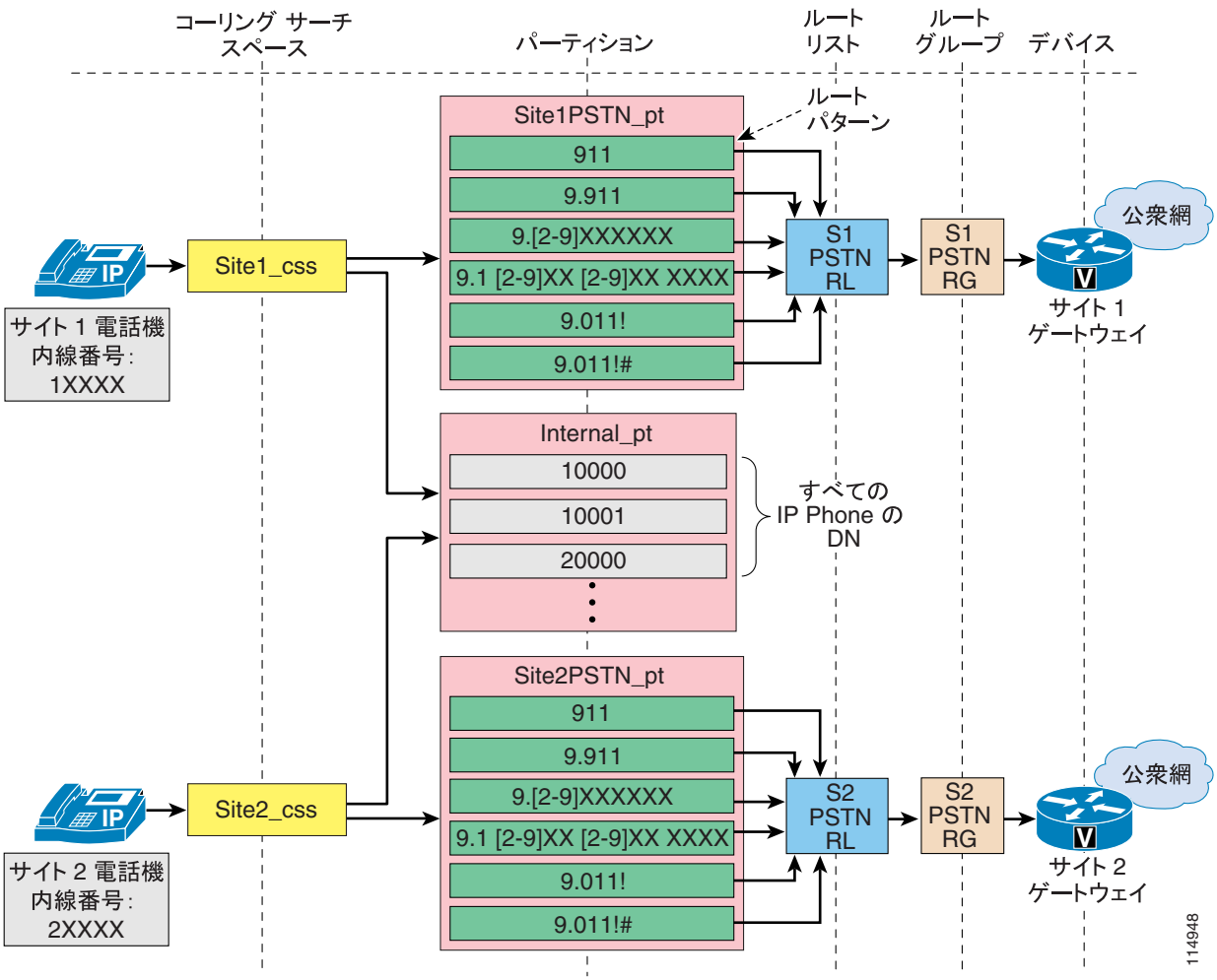
定型オンネット ダイヤル プランの配置

定型オンネット ダイヤル プランを実装するには、次のガイドラインに従います。

- 省略ダイヤルを使用して、すべての電話を一意に識別する。
- すべての電話 DN を単一のパーティションに配置する。
- 各サイトで、選択したサービス クラス アプローチに従って、公衆網ルート パターンを 1 つまたはそれ以上のサイト固有パーティションに配置する。

図 10-25 では、単一 Cisco Unified CallManager クラスタ配置での実装例を示しています。

図 10-25　定型オンネット ダイヤル プランの配置の例



次の両方の条件に当てはまる場合は、このアプローチを使用します。

- 内部内線番号の識別用に選択した桁数を考慮したとき、使用可能な DID 範囲どうしが重複していない。
- IP テレフォニー システムによって処理されるサイトの数は、長期的に見て大幅に増加することがない。

次の各項では、定型オンネット ダイヤル プランのフレームワークで使用される各種のコールについて、実装の詳細およびベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-63）
- 発信公衆網コールと IP WAN コール（P.10-63）
- 着信コール（P.10-63）
- ボイスメール コール（P.10-64）

クラスタ内でのサイト間コール

すべての内部 DN に対して、あらゆるデバイスのコーリング サーチ スペースから直接到達することができるため、すべてのオンネット コール（サイト内およびサイト間）が自動的に使用可能になります。Cisco Unified CallManager で特に設定する必要はありません。

発信公衆網コールと IP WAN コール

公衆網コールは、サイト固有のパーティションとルート パターンを使用することで可能になります。このため、緊急コールと市内電話は、ローカルの支店ゲートウェイを通じてルーティングすることができます。長距離電話と国際コールは、企業のポリシーに応じて、同じ支店ゲートウェイを通じてルーティングすることも（図 10-25 を参照）、中央ゲートウェイを通じてルーティングすることもできます。この 2 番目の方法で必要になるのは、サイトごとの追加ルート リストのみです。このリストには、中央サイト ゲートウェイを指す第 1 位ルート グループ、およびローカル支店ゲートウェイを指す第 2 位ルート グループ（省略可）を含めます。

別の Cisco Unified CallManager クラスタや Cisco Unified CallManager Express への省略ダイヤリングも、ゲートキーパーを通じて使用できます。これらの IP WAN コールについては、ゲートキーパーに送信する前に、トランスレーション パターンを通じて省略ストリングを完全な E.164 に展開することをお勧めします。

緊急コール

緊急コールの処理に Cisco Emergency Responder を使用する場合は、コールを Cisco Emergency Responder へ送信するために使用される CTI ルート ポイントを含むパーティションを、図 10-25 に示したようなサイト固有の 911 パターンではなく、すべての支店内にあるすべての電話機のコーリング サーチ スペースに含める必要があります。内部パーティション内での DN の重複は許容されないので、Cisco Emergency Responder は発信側の電話機を識別できます。Cisco Emergency Responder に関する考慮事項の詳細については、P.11-1 の「緊急サービス」の章と、次の Web サイトで入手可能な Cisco Emergency Responder 製品資料を参照してください。

http://www.cisco.com

着信コール

着信公衆網コールで必要となるのは、Cisco Unified CallManager に設定されている内線番号の長さに合せて、余分な桁を除去することのみです。この操作は、ゲートウェイの設定によって、またはゲートウェイのコーリング サーチ スペースに含まれているトランスレーション パターンを通じて実行できます。

ボイスメール コール

各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Cisco Unified CallManager 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。

ただし、ユーザが公衆網からボイスメール システムにアクセスする場合は、ユーザを訓練して、ボイスメール ボックスにアクセスするときに 8 桁の内線番号を入力してもらうようにする必要があります。

分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置

分割アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、複数のパーティション（サイトごとに 1 パーティション）に分かれている各サイトの電話に対して省略 DN を定義し、グローバル パーティションに含まれている一連のトランスレーション パターン（サイトごとに 1 トランスレーション パターン）を利用して、サイト間コール ルーティングを実行します。

この方法を使用すると、サイトの内部では省略ダイヤリング（通常は 4 桁または 5 桁）をサポートし、サイト間では完全な E.164 ダイヤリングをサポートするという重要な要件を満たすことができます。ただし、ダイヤル プランが複雑になるという代償もあります。

（注） これらの配置は、「重複ダイヤル プラン」または「重複内線番号のあるダイヤル プラン」とも呼ばれます。それぞれのサイトで定義した省略 DN が、通常は互いに重複しているためです。

表 10-5 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 10-5　分割アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Phones_pt	サイト 1 の電話 DN（省略形式）
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Translations_pt	クラスタ内でのサイト間コールのためのトランスレーション パターン
…	…	…
SiteN_css	SiteNPhones_pt	サイト N の電話 DN（省略形式）
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Translations_pt	クラスタ内でのサイト間コールのためのトランスレーション パターン

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- サイト コードを使用するグローバル オンネット番号計画を使用する予定がない。

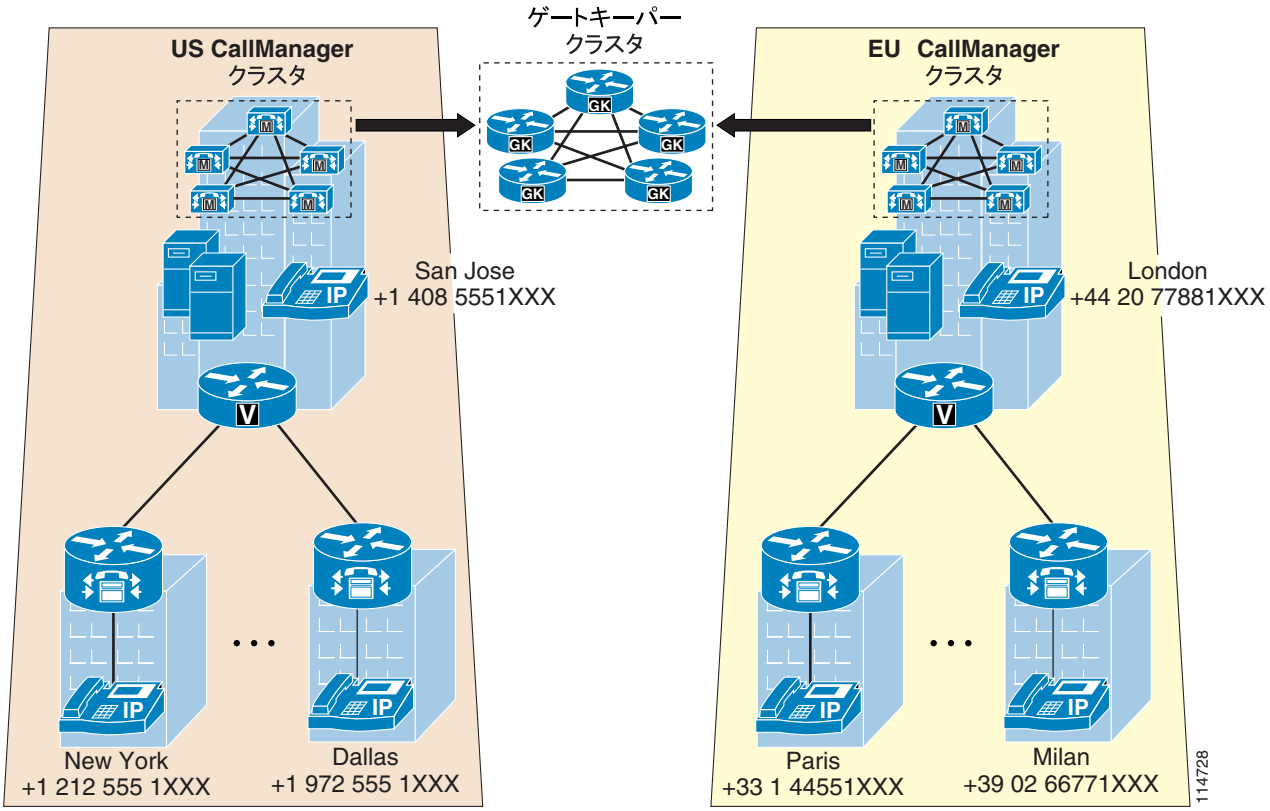
（注）　このアプローチは、サイト コードを使用するオンネットの内部内線番号計画がある場合にも使用できますが、そのようなシナリオでは、P.10-70 の「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」の項で説明しているフラット アドレッシング アプローチに従うことをお勧めします。ダイヤル プランの構造を大幅に簡素化でき、システムの管理とトラブルシューティングが容易になるためです。

- オンネットのサイト間コールに対して、ポリシーによる制約を適用する必要がある（つまり、一部またはすべてのユーザが他のオンネット サイトにダイヤルすることを不許可にする）。
- サイト間コールは、常に公衆網を介してルーティングされる（P.2-11 の「集中型コール処理のバリエーションとしての Voice Over the PSTN」の項を参照）。
- CTI ベースのアプリケーションは、サイト間では使用しない。

（注）　CTI ベースの一部のアプリケーション（Cisco Emergency Responder など）は、Cisco Attendant Console と同様に重複内線番号をサポートしていないため、分割アドレッシング アプローチを使用して配置することができません。Cisco Personal Assistant や Cisco Unified CallManager Assistant など、その他のアプリケーションは追加のダイヤル プラン設定を必要とします。重複内線番号が存在している場合、このダイヤル プラン設定は複雑なものになり、場合によっては正常に機能しない可能性があります。これらのアプリケーションを配置する予定がある場合は、次の項で説明するフラット アドレッシング アプローチを選択することをお勧めします。

分割アドレッシング アプローチを配置する方法をわかりやすくするために、図 10-26 に示す架空の顧客ネットワークについて考えます。このネットワークは、米国内にメイン サイト（San Jose）と多くの小規模支店サイト（New York と Dallas）があり、トポロジは、欧州のメイン サイト（London）と小規模支店サイト（Paris と Milan）に類似しています。ユーザ数、管理上の必要性、およびネットワーク トポロジに基づいて、集中型コール処理を使用する Cisco Unified CallManager クラスタが 2 つ配置されています。1 つは米国で、1 つは欧州です。Cisco IOS ゲートキーパー クラスタを使用して、2 つのクラスタ間での E.164 アドレス解決とコール アドミッション制御を提供しています。可変長オンネット ダイヤル プランが必要なことも決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間では完全な E.164 ダイヤリングを使用します。

図 10-26　大規模なマルチサイト配置の例



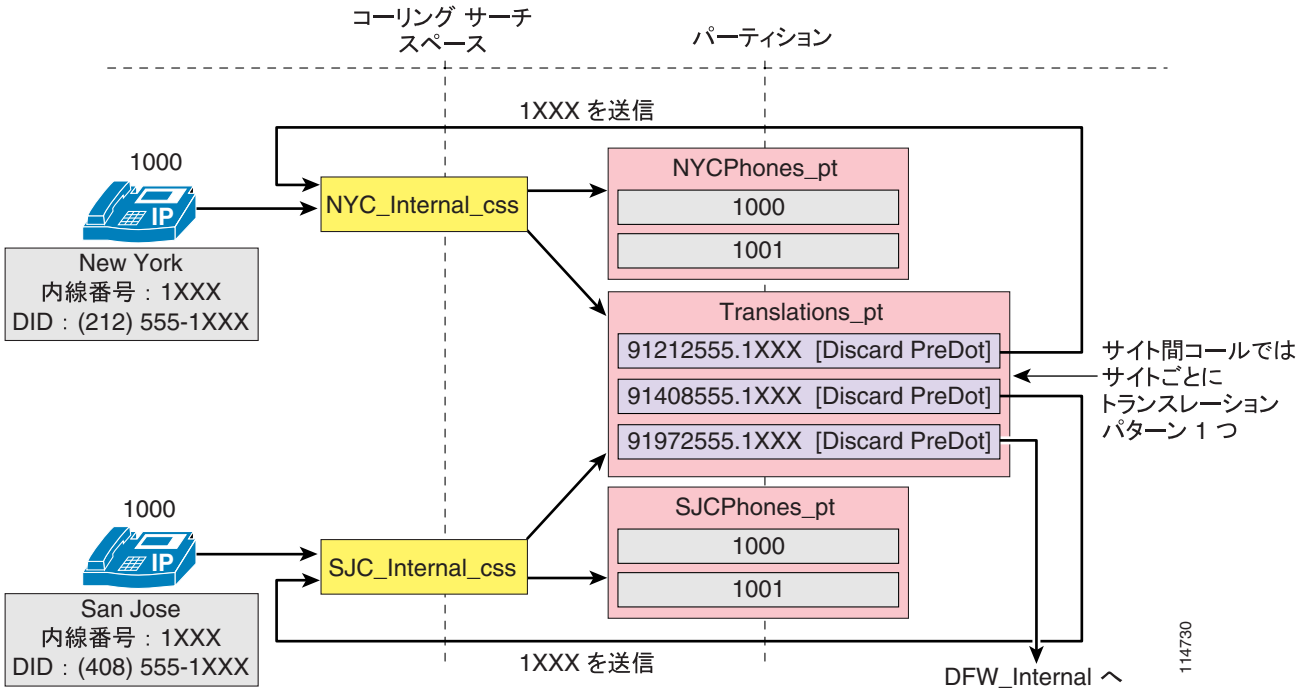
次の各項では、図 10-26 の米国（US）クラスタを例にとって、分割アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-67）
- 発信公衆網コールと IP WAN コール（P.10-67）
- 着信コール（P.10-69）
- ボイスメール コール（P.10-69）

クラスタ内でのサイト間コール

図 10-27 では、US クラスタでのサイト間コールの設定例を示しています。

図 10-27　分割アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってトランスレーション パターンを使用してください。

- サイトごとに 1 つのトランスレーション パターンを定義し、すべてのトランスレーション パターンを Translations_pt パーティションに入れる。
- 各パーティションは、公衆網サイト コード（この例では 9）を含めて、サイトの E.164 アドレス範囲と一致する必要がある。
- 変換後に得られる着信番号は、サイトの内線番号（この例では 1XXX）と一致する必要がある。
- 変換後にコールが送信されるコーリング サーチ スペースには、宛先サイトの IP Phone の DN が入っているパーティションが含まれている必要があります。

発信公衆網コールと IP WAN コール

各種の公衆網コールをどのようにルーティングするかに応じて（集中型ゲートウェイと分散型ゲートウェイ）、設定が異なります。図 10-28 の例では、国内公衆網コールはすべてローカル支店ゲートウェイを通じてルーティングされます。国際コールは、欧州クラスタの制御するサイトへのコールを代行受信するために、まずゲートキーパーを通じてルーティングされ、次にローカル公衆網ゲートウェイを通じてルーティングされます。

図 10-28　分割アドレッシング法における発信の公衆網コールと IP WAN コール

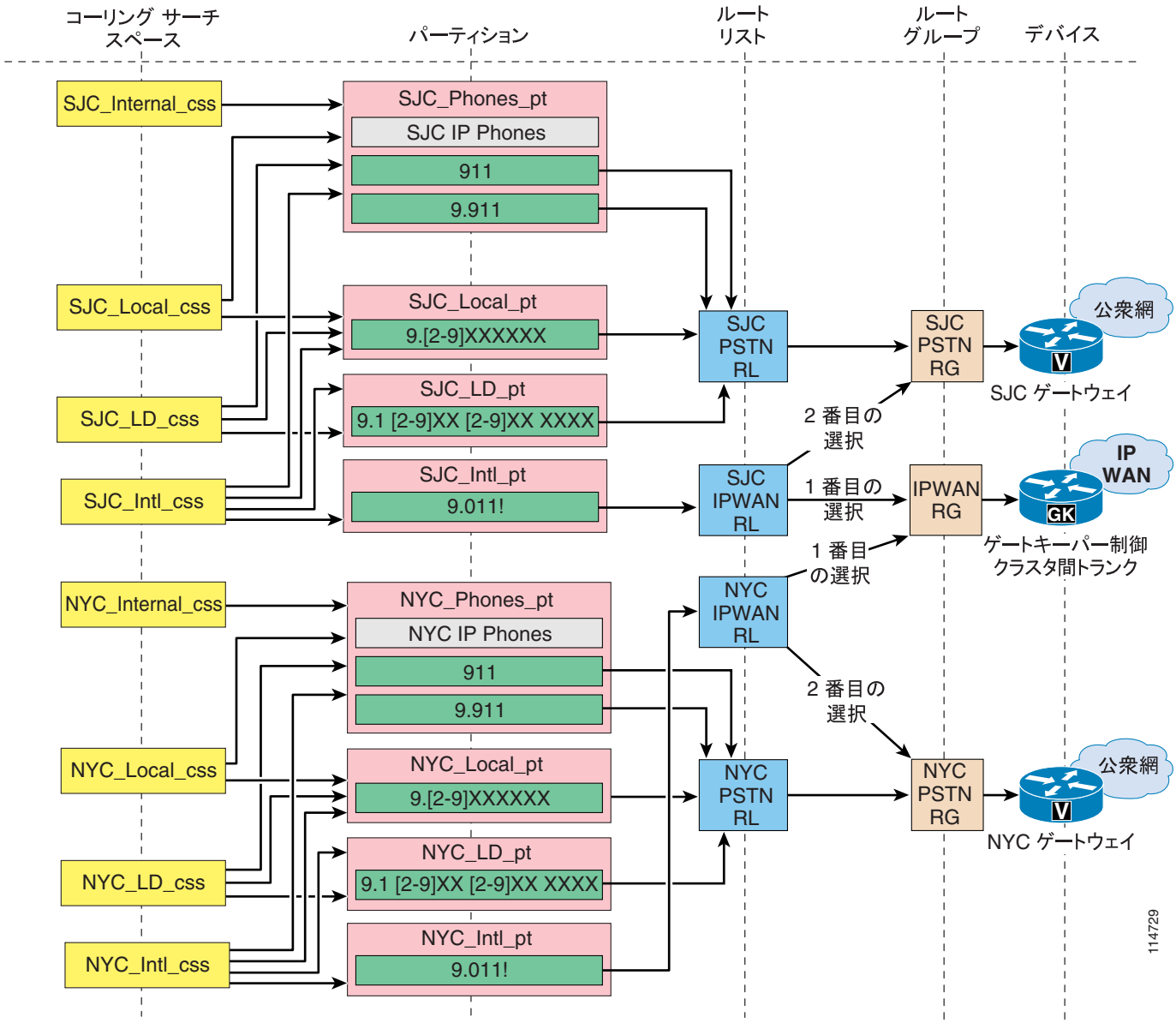


図 10-28 に示すように、発信の公衆網コールと IP WAN コールについては、内部アドレッシングが分割されていても特に考慮事項はありません。

（注） 図 10-28 では、従来のアプローチに従ってサービス クラスを構築しています。ただし、回線 / デバイス アプローチを分割アドレッシング アプローチと組み合せることもできます。サービス クラス アプローチとエンドポイント アドレッシング アプローチはそれぞれ独立しており、互いを置き換えることはできません。

着信コール

着信の公衆網コールまたは IP WAN コールを適切な内線に送信するには、上記で説明されている Translations_pt パーティション内のトランスレーション パターンを再使用できます。Translations_pt パーティションだけが入っているコーリング サーチ スペースに、すべての公衆網ゲートウェイを割り当て、すでに定義されているトランスレーション パターンと一致させるために、ゲートウェイが、着信ダイヤル番号の前に 9 または 91 をプレフィックスとして付けることを確認するだけで十分です。この方法は、公衆網が各電話機の完全修飾番号をゲートウェイに送信し、着信ダイヤル番号の前に 91 が付いている場合に、Cisco Unified CallManager には Translations_pt パーティションにあるグローバル トランスレーション パターンと一致する番号が渡されることが前提になっています。

ボイスメール コール

ボイスメール統合では、分割アドレッシング アプローチに関する次の要件に特に注意する必要があります。

- ボイスメール ボックスに固有の ID が必要です。つまり、IP Phone の内線番号はボイスメール ボックスとして使用できません。固有の番号を取得するには、番号操作が必要です。
- ボイスメール システムからの MWI（メッセージ待機インジケータ）メッセージは、固有でない内線番号がある場合でも、適切な IP Phone に到達できなければなりません。

最初の項目は、Voice Mail Profile Configuration ページの Voice Mail Box Mask フィールドを使用して、Cisco Unified CallManager で処理されます。このパラメータを設定すると、ボイスメール システムと情報を交換し、ユーザを固有に識別できます。たとえば、Voice Mail Box Mask パラメータをユーザに関連した完全な E.164 番号に設定できます。

2 番目の項目は、オンクラスタ パーティション内のトランスレーション パターンを再使用することによって処理されます。ボイスメール システムが完全な E.164 番号を使用して設定されている場合、以前に Translations_pt パーティションで定義されたトランスレーション パターンと一致させ、適切なサイト間通信を確保するために、E.164 番号の前に 9 を付けることができます。このように、完全な E.164 番号をもつボイスメール システムからの MWI メッセージは、特定のパーティション内の適切な内線番号に変換されます。たとえば、ボイスメール ポートを設定するときに、ボイスメール システムによってダイヤルされる E.164 番号に 9 をプレフィックスとして付加するトランスレーション パターンのみが入った VM_Translations_pt パーティションを含んでいるコーリング サーチ スペースを使用します。このトランスレーション パターンのコーリング サーチ スペースには、Translations_pt パーティションが含まれています。このパーティションによって、定義済みのトランスレーション パターンを通じて、すべての内線番号へのアクセスが提供されます。

（注） このアプローチには、Cisco Unified CallManager 内の 2 つのサービス パラメータの設定が必要です。Cisco CallManager サービス内の MultiTenantMwiMode パラメータを True に設定し、CMI（Cisco Messaging Interface）サービス内の ValidateDNs パラメータを False に設定する必要があります。

フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置

フラット アドレッシングを使用する可変長オンネット ダイヤル プランを実装するには、電話の DN を、オンネット アクセス コード、サイト コード、および内線番号を含んだ一意のストリング（たとえば、8-123-1000）として定義します。これらの DN を同じグローバル パーティションに配置すると、サイト コードを使用したサイト間コールを使用できるようになり、サイト固有のパーティション内にトランスレーション パターンを定義すると（サイトごとに 1 トランスレーション パターンと 1 パーティション）、サイトの内部では省略ダイヤリングを使用できるようになります。

サイト内でユーザが通常ダイヤルしている 4 桁または 5 桁の番号を使用して、Directory Number 設定ページの Line Text Label パラメータを設定すると、この内部構造をエンドユーザから見えないようにすることができます。AAR を使用可能にし、ユーザが自分の DID 番号を IP Phone のディスプレイで見られるようにするには、外部電話番号マスクについても、対応する公衆網番号を使用して設定する必要があります。

表 10-6 では、各サイトでのコーリング サーチ スペースとパーティションの基本的な関係を示しています。ただし、サービス クラスの実装に必要となる追加の要素は考慮に入れていません。

表 10-6　フラット アドレッシングを使用する可変長ダイヤル プランのコーリング サーチ スペースとパーティション

コーリング サーチ スペース	パーティション	パーティションの内容
Site1_css	Site1Translations_pt	サイト 1 の省略ダイヤリングのためのトランスレーション パターン
	Site1PSTN_pt	サイト 1 の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）
…	…	…
SiteN_css	SiteNTranslations_pt	サイト N の省略ダイヤリングのためのトランスレーション パターン
	SiteNPSTN_pt	サイト N の公衆網ルート パターン（サービス クラスに基づいて、他にもパーティションが必要）
	Internal_pt	すべての IP Phone の DN（一意形式）

次の条件に 1 つ以上当てはまる場合は、このアプローチを使用します。

- オンネットのサイト間コールで、ダイヤリング制限が必要ない。
- サイト コードを使用するグローバル オンネット番号計画を使用する予定がある。
- サイト間コールは、通常は IP WAN を通じてルーティングされる。
- CTI ベースのアプリケーションをサイト間で使用する。

（注） オンネットのサイト間コールにダイヤリング制限を適用する必要がある場合や、サイト　コードを使用するオンネット番号計画を使用する予定がない場合は、それらのニーズに対応可能なこのアプローチの変型について、P.10-76 の「サイト コードを使用しない配置に関する特別な考慮事項」の項を参照してください。

このアプローチには、次の考慮事項が適用されます。

- サイト内の 4 桁コールの宛先番号は、IP Phone のディスプレイでは一意の内部 DN へと展開されます。
- Placed Calls ディレクトリでは、ユーザがダイヤルしたとおりに元の 4 桁のストリングが表示されます。
- 発信番号、および Missed Calls ディレクトリと Received Calls ディレクトリの番号は、一意の内部 DN として表示されます。
- IP WAN が使用不可になって支店の電話が SRST モードになっている場合でも、4 桁ダイヤリング機能をそのまま使用できるようにするには、SRST ルータの **call-manager-fallback** 設定に変換規則を適用する必要があります。
- 支店の電話が SRST モードになっている場合、一意の内部 DN を IP Phone のディスプレイ上で 4 桁番号としてマスクする Line Text Label は、使用できません。代わりに、ユーザには完全な内部 DN が表示されます。

フラット アドレッシング アプローチを配置する方法をわかりやすくするために、図 10-26 に示す架空の顧客ネットワークについてもう一度考えます。この場合、可変長オンネット ダイヤル プランが必要になることは決定していて、各サイトの内部では 4 桁ダイヤリングを使用し（各サイトで 1XXX 内線番号範囲を利用）、サイト間のダイヤリングでは、オンネット アクセス コード（この例では 8）、3 桁のサイト コード、および 4 桁の内線番号で構成される 8 桁のストリングを使用します。3 桁のサイト コードは、米国にあるサイトの場合は NANP エリア コードから生成され、欧州にあるサイトの場合は E.164 国コードとサイト識別子から生成されます。表 10-7 では、選択されたサイト コードを示しています。

表 10-7　図 10-26 の顧客ネットワークのサイト コード

	San Jose	New York	Dallas	London	Paris	Milan
サイト コード	408	212	972	442	331	392

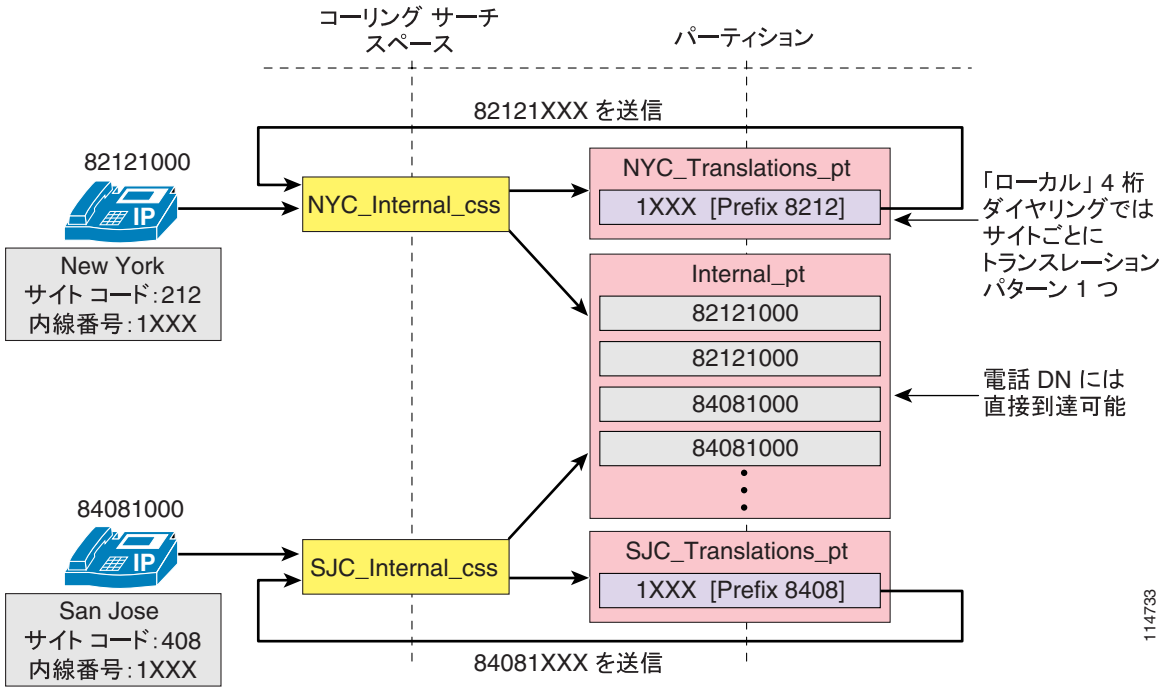
次の各項では、この例の US クラスタを使用して、フラット アドレッシング アプローチのフレームワークで使用される各種のコールについて、実装の詳細とベスト プラクティスを分析します。

- クラスタ内でのサイト間コール（P.10-72）
- 発信公衆網コールと IP WAN コール（P.10-73）
- 着信コール（P.10-76）
- ボイスメール コール（P.10-76）
- サイト コードを使用しない配置に関する特別な考慮事項（P.10-76）

クラスタ内でのサイト間コール

図 10-29 では、US クラスタでのサイト間コールの設定例を示しています。

図 10-29　フラット アドレッシング法におけるクラスタ内部のサイト間コール



サイトとパーティション間の接続性をサポートするために、次のガイドラインに従ってください。

- オンネット アクセス コード 8 を含めて、一意の DN をすべてグローバル パーティション（この例では Internal_pt）に配置します。
- サイトごとにパーティションを 1 つ作成し、それぞれのパーティションの中に、4 桁番号をそのサイトの完全修飾 8 桁番号に展開するトランスレーション パターンを配置して、サイト内部で省略ダイヤリングを使用できるようにします。
- 各サイトで、Internal_pt パーティションとローカル トランスレーション パーティションの両方を電話のコーリング サーチ スペースに含めます。

Cisco Unified CallManager に設定されている DN にオンネット アクセス コードを含めると、すべての電話から直接アクセスできるパーティションの中にすべての内部内線番号を配置できるようになり、同時に、IP Phone 上のすべてのコール ディレクトリの中に、直接にリダイヤル可能な番号が確実に入力されます。

（注） ただし、オンネット アクセス コードとサイト コードの組み合せが、どのサイトのローカル省略ダイヤリング範囲とも重複しないようにする必要があります。

発信公衆網コールと IP WAN コール

各種の公衆網コールをどのようにルーティングするかに応じて（集中型ゲートウェイと分散型ゲートウェイ）、設定が異なります。

欧州（EU）クラスタへのサイト間コールに対してオンネット接続を提供するには、次のオプションがあります。

オプション 1：8 桁番号のみ

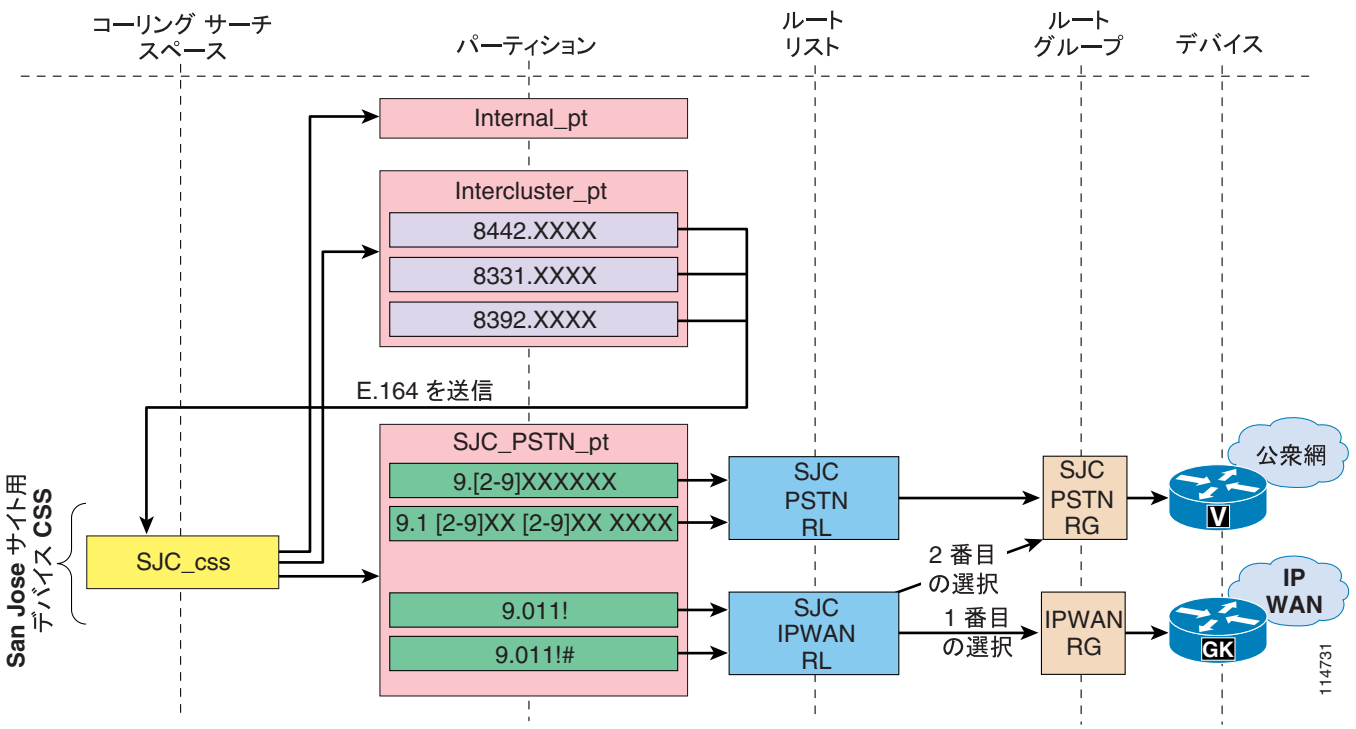
このオプションでは、単一のルート パターンを利用します。このパターンはすべての 8 桁範囲（8XXXXXXX）に一致し、ゲートキーパー制御クラスタ間トランクのみを含んだルート リストまたはルート グループを指しています。ゲートキーパーは、サイト コードをゾーン プレフィックスとして使用するように設定します。

このソリューションは、他のクラスタのサイト コードや E.164 範囲に関する情報が必要ないため、簡潔で保守が容易です。ただし、IP WAN が使用不可になった場合、自動公衆網フェールオーバーは提供されません。ユーザは、公衆網アクセス コードと宛先の E.164 アドレスを使用して、手動で再ダイヤルする必要があります。

オプション 2：8 桁番号と E.164 アドレス（集中型公衆網フェールオーバーを使用）

このオプションでは、図 10-30 に示すように、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換するグローバルな一連のトランスレーション パターンを使用します。これらのトランスレーション パターンでは、中央サイト（この場合は San Jose）のコーリング サーチ スペースを使用するので、コールは中央サイトの公衆網パーティションにある国際公衆網ルート パターンに一致します。各サイトの国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

図 10-30　IP WAN コールに集中型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



(注)　図 10-30 の設定例は、サービス クラスを構築するための回線 / デバイス アプローチが使用されていることを前提としています。ただし、従来のアプローチを使用する場合も同じ考慮事項が適用されます。

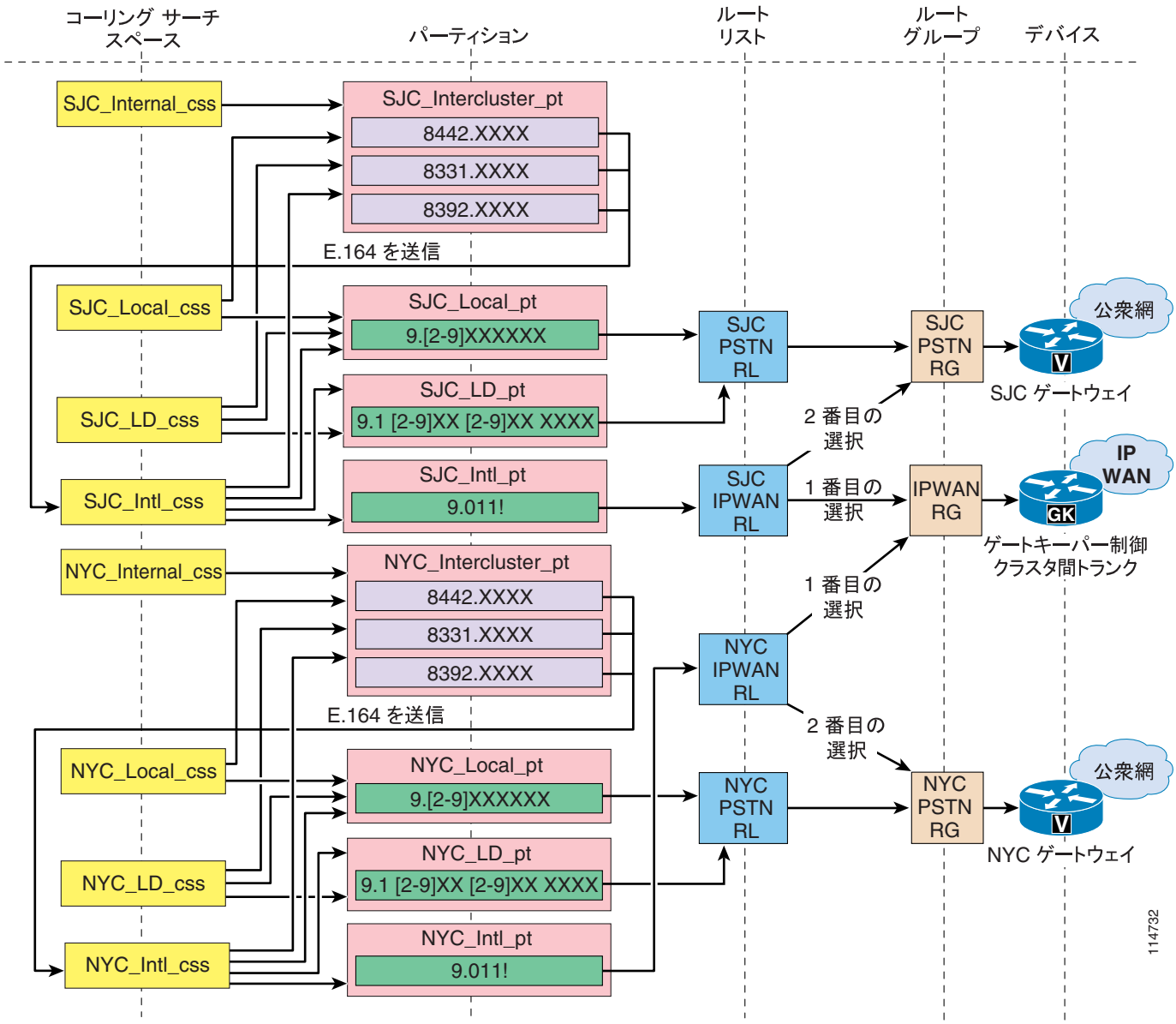
このソリューションは、オプション 1 で説明したソリューションよりもわずかに設定および保守作業が増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守する必要があるためです。その一方で、IP WAN が使用不可になった場合には、自動公衆網フェールオーバーが提供されます。公衆網フェールオーバーは、中央サイトのゲートウェイのみを使用して提供されます。このため、IP WAN 帯域幅の使用効率は最適なものにはなりません。

また、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、自動的にオンネットになります。

オプション 3：8 桁番号と E.164 アドレス（分散型公衆網フェールオーバーを使用）

このオプションでは、図 10-31 に示すように、サイトごとに一連のトランスレーション パターンを使用します。各セットは、欧州の 8 桁範囲に一致し、それらを対応する E.164 番号に変換します。これらのトランスレーション パターンでは、発信元サイトのコーリング サーチ スペースを使用するので、コールは発信元サイトの公衆網パーティションにある国際公衆網ルート パターンに一致します。各サイトの国際公衆網ルート パターンは、IP WAN ルート グループを最初の選択肢として保持し、ローカル公衆網ルート グループを 2 番目の選択肢として保持しているルート リストを指しています。ゲートキーパーは、E.164 アドレスをゾーン プレフィックスとして使用するように設定します。

図 10-31　IP WAN コールに分散型公衆網フェールオーバーを使用する、フラット アドレッシング法における発信の公衆網コールと IP WAN コール



このソリューションは、オプション 2 で説明したソリューションよりも設定および保守作業がかなり増えます。これは、他のクラスタのサイト コードと E.164 範囲に関する情報を設定し、保守して、クラスタ内の各リモート サイトでこの設定作業を繰り返す必要があるためです。その一方で、IP WAN が使用不可になった場合には、ローカル サイトのゲートウェイを使用して自動公衆網フェールオーバーが提供されるため、IP WAN 帯域幅の使用効率は最適なものになります。

このソリューションでも、公衆網コールとしてダイヤルされた欧州サイトへのコールは、IP WAN が使用可能な場合、ローカル ゲートウェイを使用する自動公衆網フェールオーバーによって、オプション 2 と同様に自動的にオンネットになります。

着信コール

着信公衆網コールでは、8 桁の内部番号を取得して宛先の電話に到達するには、E.164 番号を操作する必要があります。この要件は、次の方法のいずれかで満たすことができます。

- Cisco Unified CallManager の Gateway Configuration ページにある Num Digits フィールドと Prefix Digits フィールドを設定して、必要な番号を除去してプレフィックスを付加するようにします。
- クラスタ内でオンネット サイト間コールを強制するトランスレーション パターンを設定した場合は、公衆網アクセス コードをゲートウェイ上の着信番号にプレフィックスとして付加するだけで、それらのパターンを再利用することができます。
- H.323 ゲートウェイを使用している場合は、コールを Cisco Unified CallManager に送信する前に、ゲートウェイ内の変換規則を使用して番号を操作できます。

3 番目のアプローチは、支店が SRST モードになっている場合、設定済みの変換規則を再利用して IP Phone に着信公衆網接続を提供できる利点があります。

ボイスメール コール

8 桁の各内線番号は、いずれもシステム内部では一意です。したがって、この内線番号を使用してボイスメール システム内にボイスメール ボックスを設定することができます。ボイスメール システムにコールを送信するために、または Cisco Unified CallManager 内のメッセージ待機インジケータ（MWI）をオンにするために、変換を実行する必要はありません。ユーザは、メールボックス番号の入力を求められたときに、8 桁のオンネット番号を使用する必要があることに注意してください。

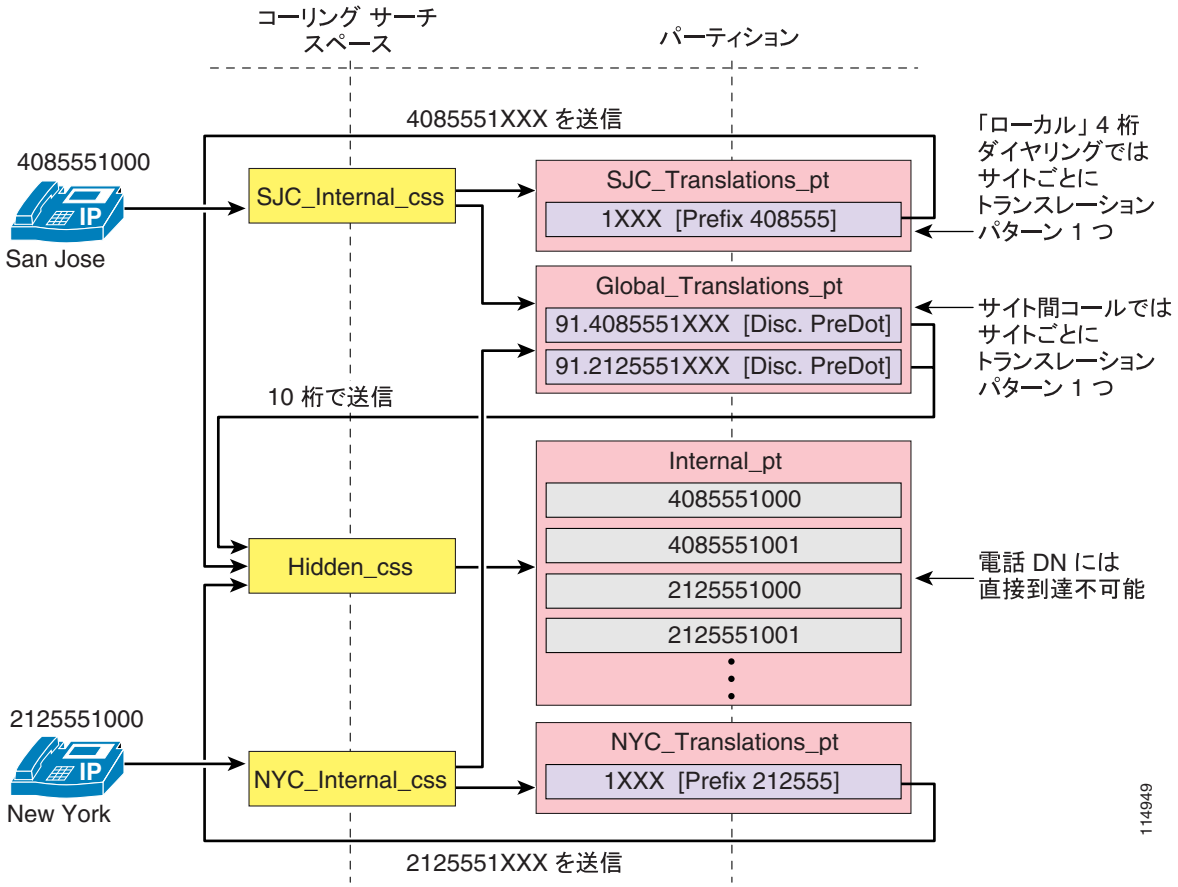
サイト コードを使用しない配置に関する特別な考慮事項

このシナリオは、フラット アドレッシング アプローチの変型であり、サイト コードに基づいてオンネット番号計画を定義することに依存しません。このシナリオでは、サイト内コールは 4 桁番号としてダイヤルします。その一方で、サイト間コールは通常の公衆網コールとしてダイヤルするため、コールは Cisco Unified CallManager によって代行受信され、IP WAN を通じてルーティングされます。

このメカニズムを実装するには、図 10-32 に示すように、次のガイドラインに従います。

- 電話 DN は、完全な E.164 アドレスとして定義し、すべて同じパーティション（この例では Internal_pt）に配置します。
- 電話のコーリング サーチ スペースは、Internal_pt パーティションに直接アクセスできないように設定します。代わりに、Global_Translation_pt というグローバル パーティションを指すようにします。このパーティションには、サイトごとに 1 パーティション、または DID 範囲を含めます。
- 公衆網アクセス コードと国コード（たとえば 91）を除去するトランスレーション パターンを設定し、コールを Hidden_css コーリング サーチ スペースを通じて Internal_pt パーティションに送信します。
- 各サイトの内部では、トランスレーション パターン（サイトごとに 1 パーティションと 1 トランスレーション パターン、または DID 範囲）を含んだサイト固有のパーティションを通じて、省略 4 桁ダイヤリングを提供できます。

図 10-32　サイト コードを使用せずにフラット アドレッシングを使用する可変長ダイヤル プラン



この応用設定では、サイト間コールにダイヤリング制限を課すことができます。たとえば、あるユーザ グループが他のサイトにコールすることを禁止する必要がある場合は、そのグループのコーリング サーチ スペースに Global_Translation_pt パーティションを含めないようにします。ただし、このアプローチを選択する場合は次の要素に注意してください。

- トランスレーション パターンの形式が、さらに複雑になります。
- 実質上オンネット公衆網コールを強制することになるため、AAR を設定して、IP WAN の帯域幅が十分にない場合でも公衆網経由でコールを発信できるようにしてください。詳細については、P.10-57 の「マルチサイト配置用の設計ガイドライン」を参照してください。
- 「発信履歴」ディレクトリには、ユーザがダイヤルしたとおりに番号ストリングが表示されます。たとえば、ユーザが 1000 をダイヤルして電話機 4085551000 へのコールが発信された場合、「発信履歴」のディレクトリには 1000 が表示されます。これにより、ダイヤル ストリングを編集しなくても番号を直接リダイヤルできます。
- 「不在履歴」と「発信履歴」のディレクトリには、電話機にコールが提供されたときに表示されたとおりの電話番号が表示されます。提供される発信番号は、トランスレーション パターンの Calling Number の設定パラメータと、発信側電話機の回線設定によって異なります。
- 図 10-32 に示した設定では、公衆網コールがすべてのサイトで同じ方法によってダイヤルされることを前提としています。単一の国内で閉じている配置は、通常はこの条件を満たしています。複数の国にわたる配置では、サイト間コールを代行受信するために、国ごとに一連の追加トランスレーション パターンが必要です。
- 複数の国にわたる配置では、可変長の内部 DN を取り扱うという複雑さもあります。E.164 アドレスは、国によって（場合によっては、1 つの国の中でも）長さが異なるためです。

Cisco Unified CallManager 5.0 を使用する電話機でのダイヤル パターン認識の配置

SIP 電話機のダイヤル パターン認識機能では、企業内のユーザから予測される一般的なダイヤリングの傾向を考慮する必要があります。一般に、ほとんどの企業では次のパターンの組み合せが使用されます。

- 同じサイト内でのコールのための省略ダイヤリング パターン（定型オンネット ダイヤル プランの場合、省略ダイヤリング パターンがサイト間コールに使用される場合があります）
- サイト コードとオンネット アクセス コード（たとえば 8）を使用しているときに可変オンネット ダイヤル プランで一般的に使用されるサイト間ダイヤリング パターン
- ローカル コール用のオフネット ダイヤリング パターン
- 長距離コール用のオフネット ダイヤリング パターン
- 緊急コール パターン（オフネット アクセス コードありとなし）
- 国際コール用のオフネット ダイヤリング パターン

表 10-8 と表 10-9 は、次のダイヤル プラン特性を持つ企業で採用できる SIP ダイヤル規則の例を示しています。

- 省略ダイヤリングは 4 桁（サイト間コールに省略ダイヤリングが使用されるかどうかは無関係）
- サイト間コールではオンネット アクセス コードとして 8 を使用し、その後にサイト コードと DN を表す 7 桁が続く
- 緊急ダイヤリングは 911 および 9911 として許可
- ローカルの 7 桁コールでは 9 をオフネット アクセス コードとして使用し、その後に 7 桁が続く
- ローカルの 10 桁コールはで 9 をオフネット アクセス コードとして使用し、その後に 10 桁が続く
- 長距離コールは 91 と 10 桁をダイヤル
- 国際コールは、9011 の後に不定の桁数が続き、ダイヤリングを # で終了可能

パターン認識は、桁間タイムアウトや Dial キー操作の必要なく、Cisco Unified CallManager に自動的に転送されるユーザ番号入力の収集の自動化だけに関係しています。サービス クラスの実施はすべて、Cisco Unified CallManager の中から選択された各種のコーリング サーチ スペースによって処理されます。すべての電話機を SIP ダイヤル規則を使用して設定し、たとえば、一部の電話機に無制限のサービス クラスが割り当てられていなくても国際ダイヤリングを認識できるようにするのは、その理由からです。

上記のダイヤル プラン特性は、フラット アドレッシングを使用する代表的な可変長オンネット ダイヤル プランです（P.10-70 の「フラット アドレッシングを使用する可変長オンネット ダイヤル プランの配置」を参照）。パターン認識の観点から見ると、このダイヤル プランは、定型オンネット ダイヤル プラン、および分割アドレッシングを使用する可変長オンネット ダイヤル プランと互換性があります（P.10-62 の「定型オンネット ダイヤル プランの配置」および P.10-64 の「分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置」を参照）。

表 10-8 と表 10-9 の各パターンに対して、同等の Cisco Unified CallManager 表記のパターンを示してあります。これらの表は、7905_7912 と 7940_7960_OTHER の両方のケースについて、SIP ダイヤル規則を示しています。

（注） 7905_7912 の SIP ダイヤル規則は 128 文字までに制限され、7940_7060_OTHER の SIP ダイヤル規則は 8K（8,192）文字までに制限されています。

表 10-8　7940_7960_OTHER ダイヤル規則

説明	パターン	タイムアウト	効果
省略形の 2XXX	2...	0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の省略ダイヤリング パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Cisco Unified CallManager に送信されます（timeout = 0）。
省略形の 3XXX	3...	0	
省略形の 4XXX	4...	0	
省略形の 5XXX	5...	0	
省略形の 6XXX	6...	0	
省略形の 7XXX	7...	0	
サイト間ダイヤリングの 8.XXXXXXX	8,.....	0	8 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。その後、すぐに Cisco Unified CallManager への転送が行われます（timeout = 0）。
緊急の 911	9,11	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 11 が収集されます。その後、すぐに Cisco Unified CallManager への転送が行われます（timeout = 0）。
緊急の 9.911	9,911	0	9 が認識されると 2 次ダイヤル トーンが再生され、番号 911 が収集されます。その後、すぐに Cisco Unified CallManager への転送が行われます（timeout = 0）。
ローカル公衆網の 7 桁	9,.....	3	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 7 桁が収集されます。ローカル公衆網の 10 桁ダイヤリングが設定されていると、ユーザは 3 秒のタイムアウトの間にダイヤリングを続行できます。
ローカル公衆網の 10 桁	9,.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Cisco Unified CallManager への転送が行われます（timeout = 0）。
長距離	9,1.....	0	9 が認識されると 2 次ダイヤル トーンが再生され、さらに 10 桁が収集されます。その後、すぐに Cisco Unified CallManager への転送が行われます（timeout = 0）。
6 秒の桁間タイムアウトによる国際ダイヤル	9,011*	6	9 が認識されると 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。
ダイヤリングの終わりとして # を使用した国際ダイヤル	9,011*#	0	9 が認識されるとすぐに 2 次ダイヤル トーンが再生され、その後、011 と不定の桁数が収集され、# によって終了します。Cisco Unified CallManager にすぐに転送されます（timeout = 0）。
オペレータ	0	0	0 が検出されると Cisco Unified CallManager にすぐに転送されます（timeout = 0）。

表 10-9　7905_7912 ダイヤル規則

説明	パターン	効果
省略形の 2XXX	2...t0	これら 6 個の範囲の組み合せは、すべてのサイトで使用できる 4 桁の省略ダイヤリング パターンを表します。[2-7]XXX と一致するいずれかのストリングがダイヤルされると、そのストリングはすぐに、Cisco Unified CallManager に送信されます（t 0）。
省略形の 3XXX	3...t0	
省略形の 4XXX	4...t0	
省略形の 5XXX	5...t0	
省略形の 6XXX	6...t0	
省略形の 7XXX	7...t0	
サイト間ダイヤリングの 8.XXXXXXX	8.......t0	番号 8 とそれに続く 7 桁が収集された後、すぐに Cisco Unified CallManager に転送されます（t0）。
緊急の 911	911t0	番号 911 が収集され、すぐに Cisco Unified CallManager に転送されます（t0）。
緊急の 9.911	9911t0	番号 9911 が収集され、すぐに Cisco Unified CallManager に転送されます（t0）。
ローカルの 7 桁と LD	9.......t4>#....t1	番号 9 とそれに続く 7 桁が収集され、さらに 4 秒間に最大 4 桁までダイヤルできます。さらに 4 桁を入力した場合、それらは 1 秒後に Cisco Unified CallManager に送信されます。# は、9 と 7 桁が入力された後の終了文字として認識されます。
国際	9011>#t6-	番号 9 011 と、それに続く不定の桁数が収集されます。ユーザは、不完全なストリングへのコールをトリガすることなく、6 秒のタイムアウトの間にダイヤリングを一時停止できます。# を終了文字として使用できます。
オペレータ	0	0 が検出されると Cisco Unified CallManager にすぐに転送されます（timeout = 0）。

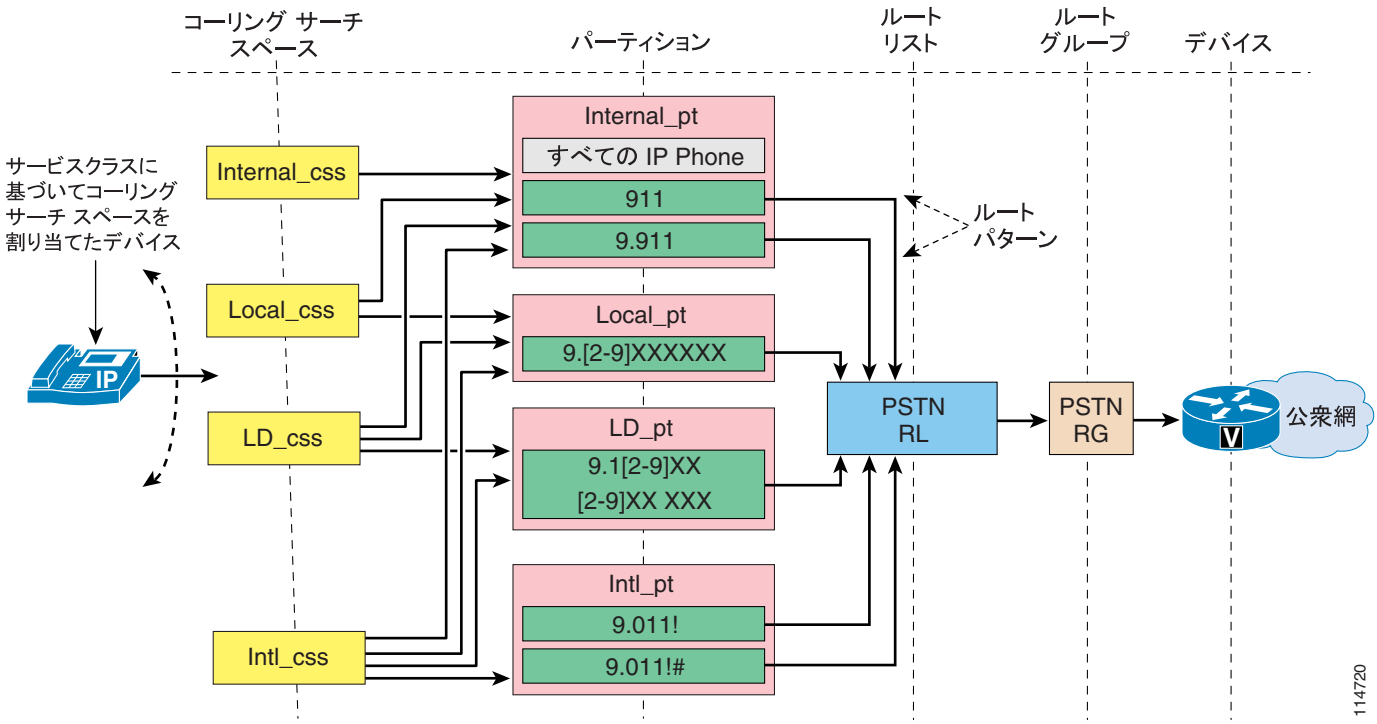
従来のアプローチによる Cisco Unified CallManager のサービス クラスの構築

Cisco Unified CallManager では、次のようにパーティションおよびデバイス コーリング サーチ スペースを外部ルート パターンと組み合せると、IP テレフォニー ユーザにサービス クラスを定義することができます。

- 外部ルート　パターンをコール可能な宛先に関連したパーティションに置きます。1 つのパーティションにすべてのルート パターンを含めることができますが、コール可能な宛先に応じてルート パターンをパーティションに関連付けると、より高度なコール制限ポリシーを実現できます。たとえば、同じパーティションにローカル ルート パターンと国際ルート パターンを入れる場合、すべてのユーザは、ローカルの宛先と海外の宛先の両方と通信できます。ただし、これは好ましくない場合があります。ルート パターンは、さまざまなサービス クラスの到達可能性ポリシーに従って、それぞれのパーティションに分類することをお勧めします。
- 各コーリング サーチ スペースがそのコール制限ポリシーに関連したパーティションのみに到達できるように設定します。たとえば、ローカル コーリング サーチ スペースが内部パーティションとローカル パーティションを指定するように設定します。その結果、このコーリング サーチ スペースに割り当てられるユーザは、内部コールおよびローカル コールしか発信できません。
- Cisco Unified CallManager のデバイス ページで電話機を設定して、これらのコーリング サーチ スペースを電話機に割り当てます。このように設定すると、デバイス上に設定されているすべての回線が自動的に同じサービス クラスを受信します。

図 10-33 では、単純な単一サイト配置の例を示しています。

図 10-33　従来のアプローチを使用するサービス クラスの基本的な例



このアプローチでは、デバイス コーリング サーチ スペースが次の 2 つの論理機能を実行します。

- パスの選択

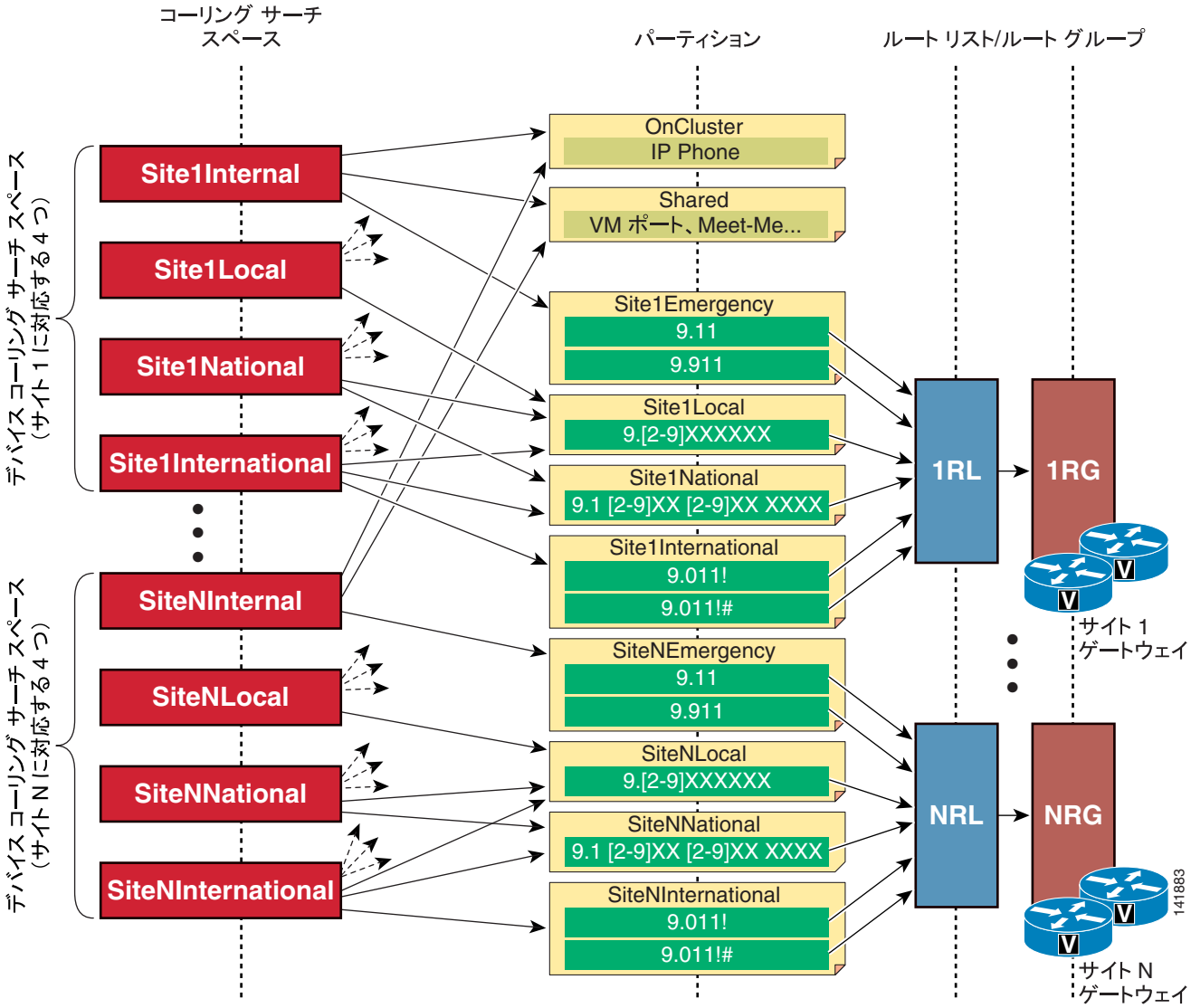
  コーリング サーチ スペースは、特定のパーティションを含んでいます。このパーティションは、ルート リストとそれに関連したルート グループを通じて、特定の公衆網ゲートウェイを指している特定のルート パターンを含んでいます。

- サービス クラス

  特定のパーティションのみをデバイス コーリング サーチ スペースに含めて、他のパーティションを含めないようにすると、特定のユーザ グループに対して実質上のコール制限が適用されます。

結果として、このアプローチを集中型コール処理のマルチサイト配置に適用する場合は、パーティションとコーリング サーチ スペースを各サイトに複製する必要があります。これは、図 10-34 に示すように、サイトごとにサービス クラスを作成し、同時に、ローカル支店ゲートウェイから発信される公衆網コールをルーティングする必要があるためです。

図 10-34　従来のアプローチで必要となるコーリング サーチ スペースとパーティション



集中型コール処理を使用するマルチサイト配置に対してこのダイヤル プラン アプローチを適用する場合は、さらに次のガイドラインに従ってください。

- サイト間のオンネット ダイヤリングを構成するために、すべての IP Phone の DN をすべてのサイトのコーリング サーチ スペースからアクセス可能なオンクラスタまたは内部のパーティションに置きます。これは、IP Phone の DN が重複している場合は不可能であることに注意してください。重複内線番号を使用するダイヤル プランの詳細については、P.10-64 の「分割アドレッシングを使用する可変長オンネット ダイヤル プランの配置」を参照してください。
- 各リモート サイトに、独自のパーティションとルート パターンのセットを指定します。リモート サイトごとのパーティション数は、ルート パターンに関連したコール制限ポリシー数によって異なります。
- 各サイトに、そのサイトの IP Phone 用に独自のコーリング サーチ スペースのセットを指定します。このコーリング サーチ スペースは、適切なローカル ルート パターン パーティションと共に、オンクラスタ パーティションも指定します。
- 企業の自動転送制限ポリシーによっては、サイト固有のデバイス コーリング サーチ スペースの 1 つを Forward All コーリング サーチ スペースに再利用することができます。

必要なコーリング サーチ スペースの合計数とパーティションの合計数を計算するには、通常は次の公式を使用してください。

合計パーティション数 =（サービス クラス数）*（サイト数）+（すべての IP Phone の DN 用に 1 パーティション）

合計コーリング サーチ スペース数 =（サービス クラス数）*（サイト数）

（注） これらの値は、最低限必要となるパーティション数とコーリング サーチ スペース数を表しています。特殊なデバイスやアプリケーションには、他のコール処理エージェント用のオンネット パターンと同様に、追加のパーティションやコーリング サーチ スペースが必要になることがあります。

従来のアプローチにおけるエクステンション モビリティの考慮事項

エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、その電話機へのログイン（またはログアウト）中の機能の 1 つになります。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

エクステンション モビリティを使用する場合、サービス クラスを構築するための従来のアプローチでコール制限を適用するには、次のガイドラインを考慮してください。

- 各サイトで、すべての IP Phone のデバイス コーリング サーチ スペースを、公衆網緊急サービスのみを（ローカル ゲートウェイを使用して）指すように設定します。
- エクステンション モビリティに使用される IP Phone がログアウト状態になっている場合の回線コーリング サーチ スペースを、内部番号のみを指すように設定します。
- 各エクステンション モビリティ ユーザについて、デバイス プロファイル内の回線コーリング サーチ スペースを、個々のユーザのサービス クラスで許可されている内部番号と追加公衆網ルート パターンを（ここでも、企業ポリシーに従って適切なゲートウェイを使用して）指すように設定します。

通常はサイト 1 を拠点としているエクステンション モビリティ ユーザが、サイト 2 の IP Phone にログインすると、公衆網コールのパス選択が次のように変更されます。

- 緊急コールは、サイト 2 の公衆網ゲートウェイを使用して正しくルーティングされます。緊急サービスは、サイト 2 にある IP Phone のデバイス コーリング サーチ スペースによって提供されるためです。
- この他のすべての公衆網コールは、エクステンション モビリティ ユーザのプロファイル（具体的には、デバイス プロファイル内に設定されている回線コーリング サーチ スペース）に従ってルーティングされます。これは、通常、これらの公衆網コールが 2 つの WAN リンクを通過し、サイト 1 のゲートウェイを使用して公衆網にアクセスすることを意味します。

この動作を修正し、エクステンション モビリティ ユーザが別のサイトにローミングしている場合でも、公衆網コールが常にローカル公衆網ゲートウェイを通じてルーティングされるようにするには、次のいずれかの方法を使用します。

- ローカル公衆網ルート パターンは、デバイス コーリング サーチ スペースに含めて、デバイス プロファイル内の回線コーリング サーチ スペースからは削除します。この方法によって、ローカルの公衆網コールは、同じ場所にある支店ゲートウェイを通じてルーティングされるようになります。ただし、同時に、ユーザは IP Phone にログインしなくてもこれらのコールをダイヤルできるようになります。長距離電話と国際コールについては、エクステンション モビリティ ユーザのデバイス プロファイルに従ってルーティングされます。したがって、このソリューションが適しているのは、通常これらのコールが中央ゲートウェイを通じてルーティングされている場合のみです。

- 各ユーザに対して、ユーザがローミングするサイトごとに 1 つずつ、複数のデバイス プロファイルを定義します。各デバイス プロファイルの設定では、回線コーリング サーチ スペースが、そのサイトのローカル ゲートウェイを使用する公衆網ルート パターンを指すようにします。ローミングするユーザおよびローミング先となるサイトが非常に多い場合、この方法は設定と管理の負荷が大きくなります。
- 次の項（P.10-84 の「回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築」）で説明する回線 / デバイス アプローチを実装します。

（注）

Cisco Emergency Responder を使用する場合は、デバイスに設定するサイト固有のコーリング サーチ スペースに、Cisco Emergency Responder を指す 911 CTI ルート ポイントを含むパーティションを含める必要があります。その同じパーティションに、同じ 911 CTI ルート ポイントを指すトランスレーション パターン 9.911 も含めると、ユーザは 9911 をダイヤルして救急サービスに連絡することができます。

回線 / デバイス アプローチによる Cisco Unified CallManager のサービス クラスの構築

前の項で説明した従来のアプローチは、集中型コール処理を使用した大規模なマルチサイト配置に適用する場合、結果的にパーティションとコーリング サーチ スペースの数が非常に多くなることがあります。このような構成にする必要があるのは、デバイス コーリング サーチ スペースを使用して、パス選択（外部コールにどの公衆網ゲートウェイを使用するか）とサービス クラスの両方を決定しているためです。

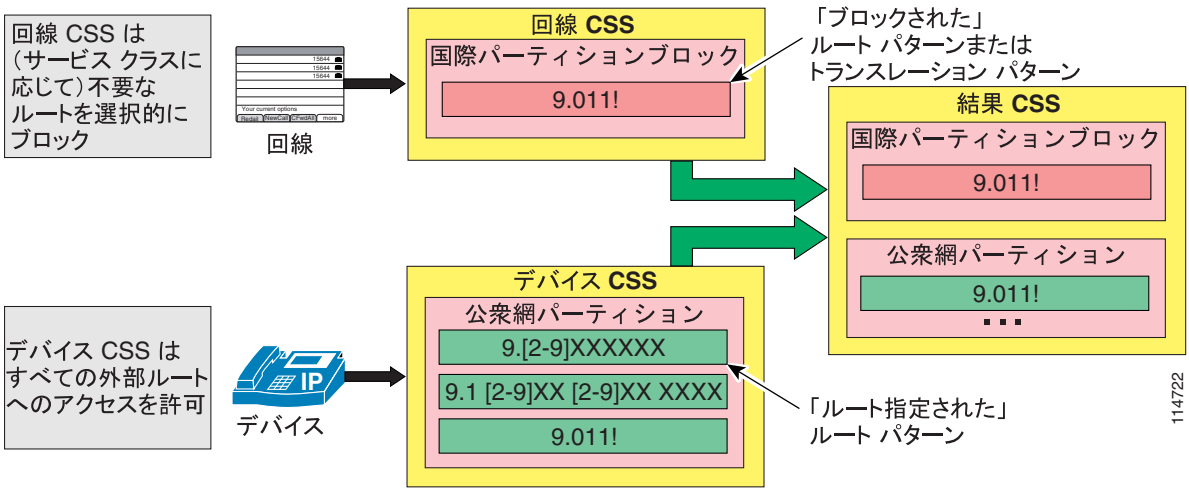
これらの 2 つの機能を回線コーリング サーチ スペースとデバイス コーリング サーチ スペースに分配すると、必要となるパーティションとコーリング サーチ スペースの総数を大幅に減らすことができます。この手法を「回線 / デバイス アプローチ」と呼びます。

所定の各 IP Phone の回線コーリング サーチ スペースとデバイス コーリング サーチ スペースが Cisco Unified CallManager でどのように組み合されているか、および回線コーリング サーチ スペースのパーティションが、結果のコーリング サーチ スペースでどのようにして最初に表示されるのか（P.10-22 の「Cisco Unified CallManager におけるコール特権」を参照）に注目すると、回線 / デバイス アプローチでは、一般に次の規則を適用できます。

- デバイス コーリング サーチ スペースは、コール ルーティング情報（たとえば、どのゲートウェイを公衆網コール用に選択するか）を提供するために使用します。
- 回線コーリング サーチ スペースは、サービス クラス情報（たとえば、どのコールを許可するか）を提供するために使用します。

これらの規則がどのように適用されるのかをわかりやすくするために、図 10-35 に示す例について考えます。このデバイス コーリング サーチ スペースは、国際番号を含めて、すべての公衆網番号へのルート パターンが入ったパーティションを保持しています。このルート パターンは、ルート リストおよびルート グループを通じて、公衆網ゲートウェイを指しています。

図 10-35　回線 / デバイス アプローチにおける重要な概念



同時に、回線コーリング サーチ スペースは、トランスレーション パターンが 1 つのみ入ったパーティションを保持しています。このパターンは国際番号に一致し、ブロック パターンとして設定されています。

したがって、結果のコーリング サーチ スペースには、国際番号に一致する 2 つの同一パターンが保持されています。最初に表示されるのは、回線コーリング サーチ スペースに含まれているブロック パターンです。結果として、この回線からの国際通話はブロックされます。

回線コーリング サーチ スペースでは、トランスレーション パターンの代わりに、ルート パターンを使用してコールをブロックすることもできます。ブロック ルート パターンを設定するには、まず、使用されていない IP アドレスを使用して「ダミー」ゲートウェイを作成し、そのゲートウェイを「ダミー」ルート リストおよびルート グループに配置します。次に、ダミー ルート リストを指すようにルート パターンを設定します。コールをブロックするルート パターンとトランスレーション パターンの主な違いは、ブロックされている番号をエンドユーザがダイヤルしようとしたときの対応です。次に例を示します。

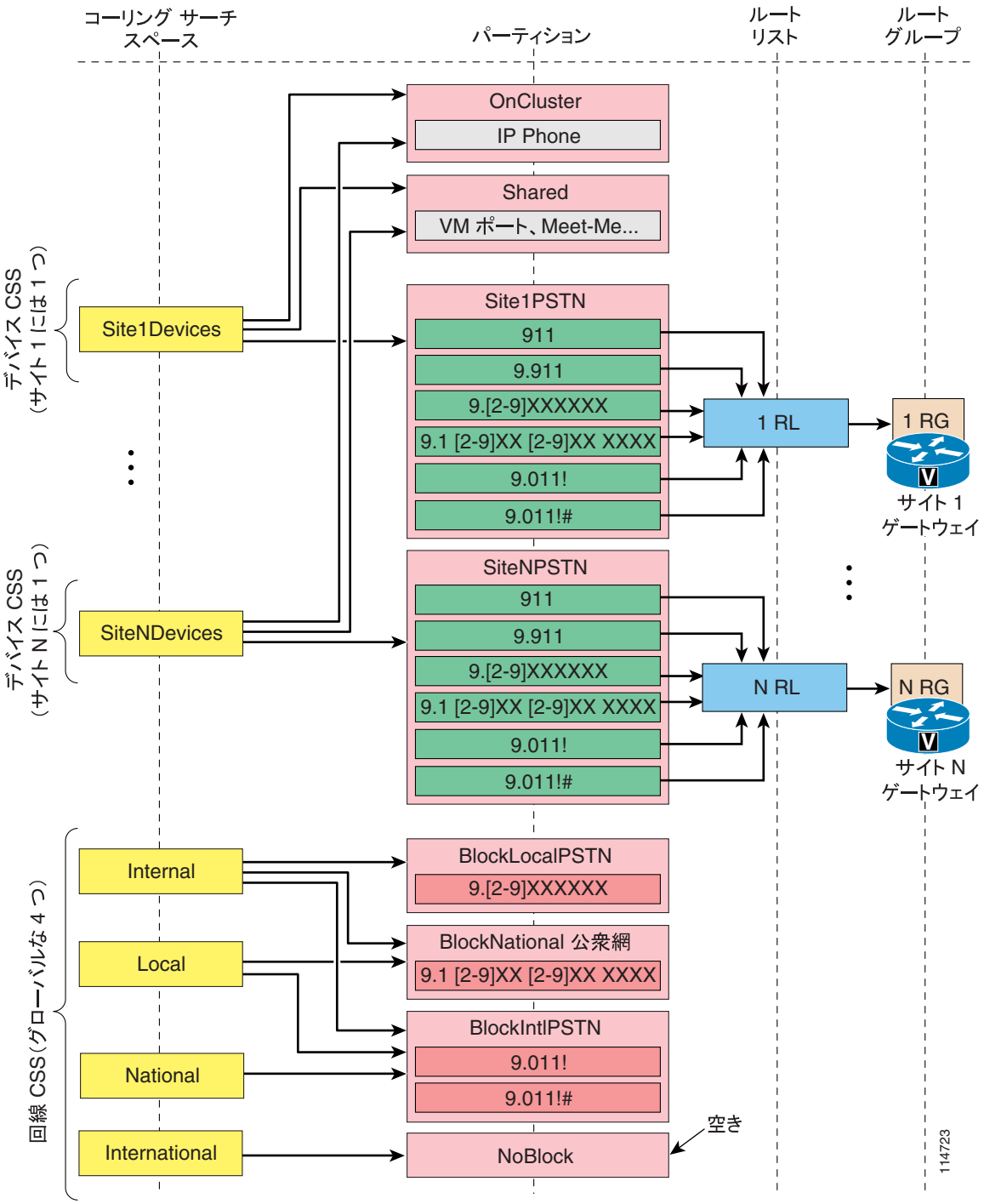
- トランスレーション パターンを使用した場合、エンドユーザは番号を最後までダイヤルできます。ダイヤルが完了した時点でのみ、ユーザにファースト ビジー トーンが再生されます。
- ルート パターンを使用した場合は、エンドユーザのダイヤルしている番号が許可パターンに一致する可能性がなくなると、その時点ですぐにファースト ビジー トーンが再生されます。この動作は、SCCP を実行している IP Phone、または SIP を実行し、電話機に SIP ダイヤル規則が設定されていないタイプ B の IP Phone を前提にしています。

集中型コール処理を使用するマルチサイト配置に対して回線 / デバイス アプローチを実装する場合は、さらに次のガイドラインに従ってください。

- サイトごとに無制限のコーリング サーチ スペースを作成し、電話機のデバイス コーリング サーチ スペースに割り当てます。このコーリング サーチ スペースには、電話機のロケーションに適したゲートウェイ（たとえば、同じ場所に配置されている緊急サービス用の支店ゲートウェイと、長距離電話用の中央ゲートウェイ）にコールをルーティングするルート パターンを備えたパーティションが含まれていなければなりません。
- ユーザのダイヤリング権限に含まれていないタイプのコールに対するブロック トランスレーション / ルート パターンを備えたパーティションを含むコーリング サーチ スペースを作成し、ユーザの回線に割り当てます。たとえば、ユーザが国際コール以外のすべてのタイプのコールを利用できる場合、そのユーザの回線は、9.011! ルート パターンをブロックするコーリング サーチ スペースを使用して設定する必要があります。

図 10-36 は、N 個のサイトがあるマルチサイト配置に対して、これらのガイドラインを適用する方法の例を示しています。

図 10-36　回線 / デバイス アプローチで必要となるコーリング サーチ スペースとパーティション



この方法の利点として、サイトごとに必要なサイト固有の無制限コーリング サーチ スペースが支店に 1 つのみであるという点があります。ダイヤリング権限は、ブロック ルート パターン（サイトに依存しない）の使用により実装されるので、同じセットのブロック コーリング サーチ スペースをすべての支店で使用できます。

結果として、必要なコーリング サーチ スペースの合計数とパーティションの合計数を計算するには、次の公式を使用できます。

合計パーティション数 =（サービス クラス数）+（サイト数）+（すべての IP Phone の DN 用に 1 パーティション）

合計コーリング サーチ スペース数 =（サービス クラス数）+（サイト数）

（注） これらの値は、最低限必要となるパーティション数とコーリング サーチ スペース数を表しています。特殊なデバイスやアプリケーションには、他のコール処理エージェント用のオンネット パターンと同様に、追加のパーティションやコーリング サーチ スペースが必要になることがあります。

（注） Cisco Emergency Responder を使用する場合は、911 CTI ルート パターンと 9.911 トランスレーション パターンをグローバルな On-Cluster パーティションに含めることができます。

サイトの数が多い集中型コール処理配置に対して回線 / デバイス アプローチを適用すると、必要となるパーティションとコーリング サーチ スペースの数が大幅に減少します。たとえば、100 のリモート サイトと 4 つのサービス クラスがある配置の場合、従来のアプローチでは、少なくとも 401 のパーティションと 400 のコーリング サーチ スペースが必要です。回線 / デバイス アプローチでは、105 のパーティションと 104 のコーリング サーチ スペースしか必要ありません。

ただし、回線 / デバイス アプローチが成立するのは、特定サービス クラスの使用を制限する必要のある公衆網コールのタイプ（たとえば、市内電話、長距離電話、国際コール）を、グローバルに識別できる場合です。使用している国の国内番号計画が原因で、コール タイプをグローバルに識別することができない場合、このアプローチの効果は、（設定の省力化に関しては）上の公式に示したものよりも小さくなります。

たとえば、フランスでは、番号計画は 5 桁のエリア コード（01 ～ 05、および携帯電話の 06 エリア コード）に基づいており、この後に 8 桁の加入者番号が続きます。ここで重要となる特徴は、各公衆網宛先に到達するとき、同じローカルエリアからコールするときも、別のエリアからコールするときも、必ず同じ番号（たとえば、Paris の番号は 01XXXXXXXX、Nice の番号は 02XXXXXXXX など）をダイヤルすることです。つまり、「長距離電話」であるかどうかは、発信者がどのエリアにいるかに応じて変化します。このため、1 つのパーティションと 1 つのルート パターンでは、長距離電話へのアクセスをブロックできません。たとえば、発信者が Paris にいる場合、014455667788 へのコールは市内電話ですが、発信者が Nice や Lyon にいる場合は長距離電話です。

このような場合は、市内電話と長距離電話が同じ方法でダイヤルされるエリアごとに 1 つずつ、一連のブロック用コーリング サーチ スペースとパーティションを追加設定する必要があります。フランスの例では、表 10-10 に示すように、各エリア コードに対して 1 つずつ、5 組のブロック用コーリング サーチ スペースとパーティションを追加で定義する必要があります。

表 10-10　フランス国内番号計画に適用される回線 / デバイス アプローチ

コーリング サーチ スペース	パーティション	ブロック ルート パターン
Internal_css	BlockAllNational_pt	0.0[1-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local01_css	BlockLD01_pt	0.0[2-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local02_css	BlockLD02_pt	0.0[13-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local03_css	BlockLD03_pt	0.0[124-6]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local04_css	BlockLD04_pt	0.0[1-356]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
Local05_css	BlockLD05_pt	0.0[1-46]XXXXXXXX
	BlockIntl_pt	0.00!, 0.00!#
LD_css	BlockIntl_pt	0.00!, 0.00!#
Intl_css	NoBlock_pt	なし

回線 / デバイス アプローチのガイドライン

Cisco Unified CallManager 5.0 では、回線設定ページに Secondary Calling Search Space for Forward All が新たに導入されました。このコーリング サーチ スペースが回線の Forward All コーリング サーチ スペースと連結されることにより、回線 / デバイス ダイヤル プラン アプローチを使用して、Forward All 動作に同じ回線から発信される通常のコールと同じサービス クラスを提供できます。連結の順序は、Forward All コーリング サーチ スペースが先で、その後に Secondary Calling Search Space for Forward All が続きます。

回線 / デバイス アプローチを使用する場合は、次のガイドラインを考慮してください。

- Forward Busy および Forward No Answer のコーリング サーチ スペースは、回線またはデバイスのコーリング サーチ スペースと連結されません。
- Forward Busy および Forward No Answer コーリング サーチ スペースは、ボイスメール パイロット番号およびポートに到達できる、グローバル コーリング サーチ スペースに設定します。
- Forward All コーリング サーチ スペースは、企業のポリシーに従って設定します。
  - 転送コールが無制限の特権を持つ必要がある場合は、サイト固有のデバイス　コーリング サーチ スペースに一致するように Forward All コーリング サーチ スペースを設定します（エクステンション モビリティを使用する場合の追加の考慮事項については、P.10-89 の「回線 / デバイス アプローチにおけるエクステンション モビリティの考慮事項」を参照）。
  - 転送コールを内部番号のみに制限する必要がある場合は、Forward All コーリング サーチ スペースを、内部番号にのみ到達可能なグローバル コーリング サーチ スペースに設定します。
  - 転送されるコールを通常のコールと同じサービス クラスにする必要がある場合は、回線に設定したものと同じコーリング サーチ スペースを Forward All に設定し、デバイスに設定したサイト固有のコーリング サーチ スペースを Secondary Calling Search Space for Forward All に設定します。

（注） SIP を実行するタイプ A の IP Phone は、電話機から開始される Rerouting Calling Search Space for Forward All 動作を使用します。Cisco Unified CallManager のユーザ ページまたは管理ページから開始される Forward All 動作は、上記の連結されたコーリング サーチ スペースを使用します。

（注） Cisco Unified CallManager 5.0 より前のバージョンで、転送コールに中間的な制限を適用する必要がある場合は（ローカル公衆網番号へのアクセスに適用し、国際番号には適用しないなど）、サイト固有の追加のコーリング サーチ スペースが必要になるため、回線 / デバイス アプローチの効果は小さくなります。このような場合は、従来のアプローチを選択することをお勧めします。

- このアプローチが機能するには、回線コーリング サーチ スペース内に設定するブロック パターンの詳細度が、デバイス コーリング サーチ スペース内に設定したルート パターンと少なくとも同等になっている必要があります。エラーが発生することを避けるために、ブロックの対象となるパターンは、可能な場合にはルーティングを許可するパターンよりも詳細に設定することをお勧めします。@ ワイルドカード内に定義されるパターンは非常に詳細なものになるため、このワイルドカードの取り扱いには十分に注意してください。
- オンネット DN がダイヤルされると、AAR が呼び出されます。これらの DN へのアクセスは、上で説明したものと同じプロセスで制御できます。AAR は、再ルーティングされるコールには別のコーリング サーチ スペースを使用します。ほとんどの場合、AAR コーリング サーチ スペースは、サイト固有の無制限デバイス コーリング サーチ スペースと同じものでかまいません。このコーリング サーチ スペースは、エンドユーザによって直接ダイヤルされることがないためです。

（注） 回線とデバイスの優先順位は、CTI デバイス（CTI ルート ポイントと CTI ポート）に関しては逆になります。これらのデバイスの場合、結果のコーリング サーチ スペースでは、デバイス コーリング サーチ スペースに含まれているパーティションが、回線コーリング サーチ スペースよりも前に配置されます。そのため、パターン選択を連結の順序だけに頼らず、ブロックされるパターンの精度が許可されるパターンの精度よりも、すべてのケースで確実に高くなるよう注意しなければ、回線 / デバイス アプローチを Cisco IP SoftPhone などの CTI デバイスに適用できません。

回線 / デバイス アプローチにおけるエクステンション モビリティの考慮事項

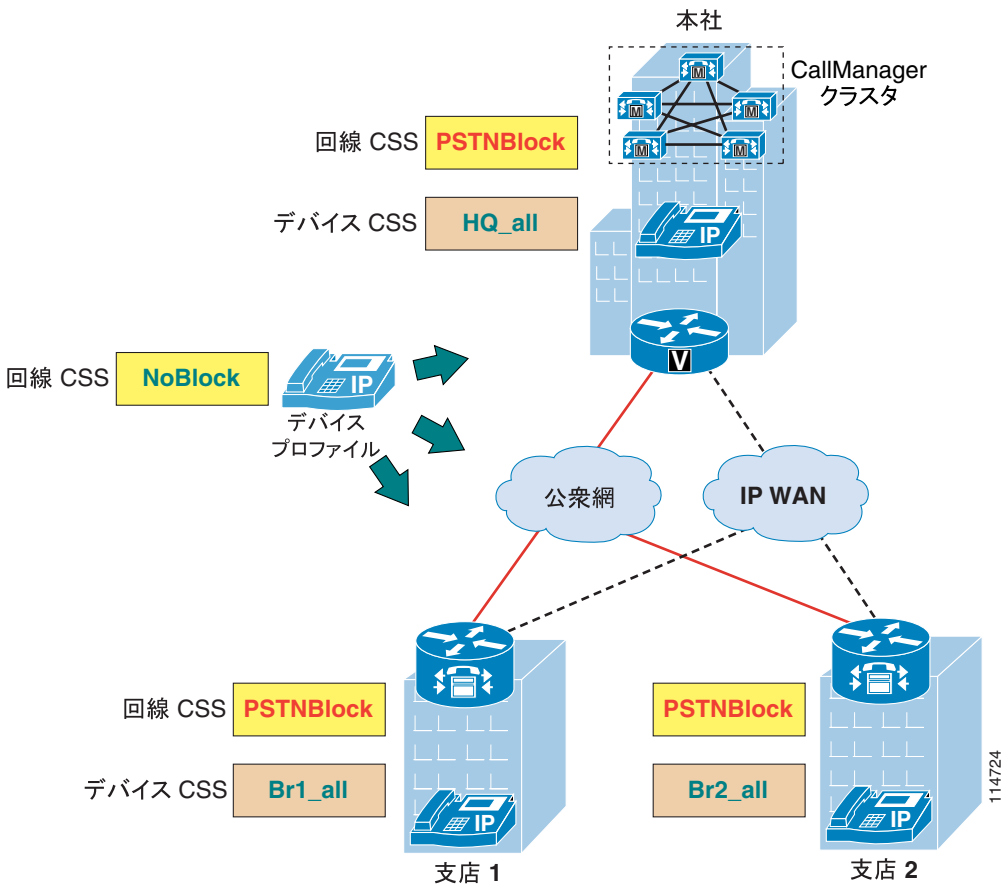
エクステンション モビリティ機能を使用する場合、電話機のダイヤル制限は、回線 / デバイス アプローチを使用することによって、その電話機へのログイン（またはログアウト）中の機能の 1 つとして自然な方法で実装できます。ログアウトされた電話機は、他の電話機やサービス（たとえば、米国では 911）のコールを制限する必要があります。一般に、公衆網を通じた市内または市外通話へのアクセスは制限されます。逆に、ユーザがログインしている電話機は、そのユーザのダイヤリング権限に応じてコールを許可し、それらのコールを適切なゲートウェイ（たとえば、同じ場所に配置されているローカル コール用の支店ゲートウェイ）にルーティングする必要があります。

サービス クラスの構築に回線 / デバイス アプローチを使用する場合は、前の項で説明したものと同じ規則を、エクステンション モビリティのデバイス プロファイル コンストラクトに適用するだけで済みます。エクステンション モビリティ使用時にコール制限を適用するには、次のガイドラインを考慮してください。

- 一致する可能性のあるすべての公衆網ルート パターンが入っていて、それらのパターンを適切にルーティングする（たとえば、緊急コールと市内電話にはローカル ゲートウェイを使用し、長距離電話には中央ゲートウェイを使用する）サイト固有のパーティションを指すように、各サイトのすべての IP Phone のデバイス コーリング サーチ スペースを設定します。
- ユーザがログインしていないときでも許可されるコール（たとえば、内部内線番号と緊急サービス）以外のコールをすべてブロックするブロック トランスレーション / ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、すべての IP Phone の回線コーリング サーチ デバイス（または、デフォルト ログアウト デバイス プロファイルの回線コーリング サーチ スペース）を設定します。
- エクステンション モビリティ ユーザごとに、特定のサービス クラスに対して許可しない公衆網コールを選択してブロックする（たとえば、国際コールのみをブロックする）ブロック トランスレーション / ルート パターンを備えたグローバル コーリング サーチ スペースを指すように、回線コーリング サーチ スペースをデバイス プロファイル内に設定します。一部のユーザに無制限のコール特権を与える必要がある場合は、それらのユーザを空のパーティションを備えた回線コーリング サーチ スペースに割り当てます。

エクステンション モビリティに回線 / デバイス アプローチを使用することの主な利点は、図 10-37 に示すように、集中型コール処理を使用するマルチサイト配置において、ユーザがホーム サイト以外の支店サイトにある IP Phone にログインしている場合でも、適切なコール ルーティングが保証されることです。

図 10-37　回線 / デバイス アプローチを使用したエクステンション モビリティ



この章ですでに説明したように、デバイス プロファイル内に設定した回線コーリング サーチ スペースは、ユーザがエクステンション モビリティを通じてログインすると、物理 IP Phone 上に設定されている回線コーリング サーチ スペースを置き換えます。コール ルーティングはデバイス コーリング サーチ スペースによって正しく処理されるため、ログイン操作は、単に電話のロックを解除するために使用されます。ログイン操作によって、（ブロック パターンを含んでいる）電話の回線コーリング サーチ スペースが削除され、（この単純化した例では、ブロック パターンを保持していない）デバイス プロファイルの回線コーリング サーチ スペースに置き換えられます。

コール ルーティングがすべてデバイス コーリング サーチ スペースの内部で実行されるのに対して、回線コーリング サーチ スペースは、単にブロック パターンを導入するだけです。このため、ユーザは、ホーム サイト以外のサイトにログインした場合、そのサイトのローカル ダイヤリング手順を自動的に継承します。たとえば、電話の DN は 8 桁番号として定義されているものの、各サイトの内部では、ローカル トランスレーション パターンによって 4 桁ダイヤリングが提供されているとします。この場合、別のサイトにローミングしたユーザは、ホーム サイトにいる同僚に 4 桁のみダイヤルして到達することはできなくなります。4 桁の番号は、ユーザがログインしたホスト サイトの規則に従って変換されるためです。

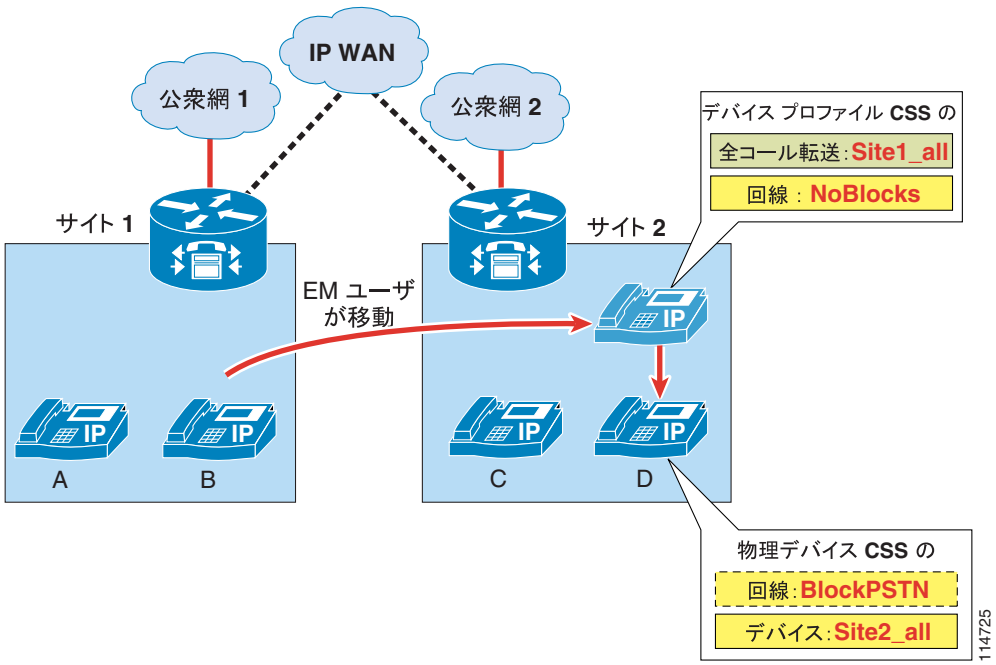
つまり、回線 / デバイス アプローチをエクステンション モビリティに使用する場合は、エンドユーザがログイン先サイトのダイヤリング手順に従う必要があります。

自動転送の考慮事項

エクステンション モビリティを使用する集中型コール処理環境に対して回線/デバイス コーリング サーチ スペース アプローチを適用する場合、ユーザがすべてのコールを外部公衆網番号に転送できるようにする必要があるときは、自動転送の動作に注意する必要があります。

図 10-38 では、エクステンション モビリティ ユーザが通常はサイト 1 を拠点としていて、そのデバイス プロファイルでは、無制限に公衆網コールを発信し、すべての着信コールを任意の公衆網番号に転送することが許可されています。

図 10-38　回線 / デバイス アプローチを使用したエクステンション モビリティにおける自動転送の考慮事項



P.10-26 の「自動転送コーリング サーチ スペース」の項で説明したように、Forward All コーリング サーチ スペースは、回線およびデバイスのコーリング サーチ スペースとは連結されないため、Site1_all に設定する必要があります。Site1_all は、サイト 1 のゲートウェイを使用するすべての公衆網ルートを含んでいます。

このユーザがサイト 2 に移動して電話機 D にログインすると、ユーザのデバイス プロファイルに従って、このプロファイルの回線コーリング サーチ スペースと Forward All コーリング サーチ スペースが物理デバイスに適用されます。直接公衆網コールの場合、使用されるコーリング サーチ スペースは、回線とデバイスのコーリング サーチ スペースを連結したものです。電話 D のデバイス コーリング サーチ スペース（Site2_all）は、サイト 2 のゲートウェイを正しく指しています。

このユーザが、すべてのコールを公衆網番号に転送するように電話を設定すると、転送されるすべてのコールは、Site1_all コーリング サーチ スペースを使用します。Site1_all は、サイト 1 のゲートウェイを指したままです。この状態になると、次のような動作が発生します。

- 着信公衆網コールは、サイト 1 のゲートウェイで IP ネットワークに入り、同じゲートウェイ内で公衆網にヘアピンされます。
- サイト 1 の電話（電話 A など）から発信されるコールは、サイト 1 のゲートウェイを通じて公衆網に正しく転送されます。
- サイト 2 の電話（電話 C など）から発信されるコールは、WAN を経由してサイト 1 に到達し、サイト 1 のゲートウェイを通じて公衆網にアクセスします。同じ Cisco Unified CallManager クラスタ内の他のサイトから発信されるコールに対しても、同じ動作が適用されます。

ネットワークを設計し、ユーザをトレーニングするときは、この動作に注意してください。

（注）

Cisco Unified CallManager 5.0 では、User Device Profile の回線設定ページに Secondary Calling Search Space for Forward All が新たに導入されました。このコーリング サーチ スペースは、User Device Profile の回線コーリング サーチ スペースと連結されます。これらのコーリング サーチ スペースはどちらも、最終的にデバイス プロファイルが使用される電話機のコーリング サーチ スペースから独立しています。したがって、Forward All 動作は、プロファイルが使用されるデバイスのサイト固有のコーリング サーチ スペースが提供するコール ルーティングに基づいたものにはなりません。連結の順序は、Forward All コーリング サーチ スペースが先で、その後に Secondary Calling Search Space for Forward All が続きます。

H.323 を使用している Cisco IOS でのサービス クラスの構築

次のシナリオでは、H.323 プロトコルを実行している Cisco IOS ルータにサービス クラスを定義する必要があります。

- 集中型コール処理を使用する Cisco Unified CallManager マルチサイト配置
- Cisco Unified CallManager Express 配置

集中型コール処理を使用する Cisco Unified CallManager マルチサイト配置では、通常、サービス クラスは Cisco Unified CallManager でパーティションとコーリング サーチ スペースを使用して実装します。ただし、支店サイトと中央サイト間の IP WAN 接続が失われた場合は、Cisco SRST が支店 IP Phone の制御を取得し、パーティションとコーリング サーチ スペースに関する設定は、IP WAN 接続が復旧するまですべて使用できなくなります。したがって、SRST モードで動作している支店ルータ内にサービス クラスを実装することが望ましくなります。

同様に、Cisco Unified CallManager Express 配置の場合も、ルータには IP Phone 用のサービス クラスを実装するメカニズムが必要です。

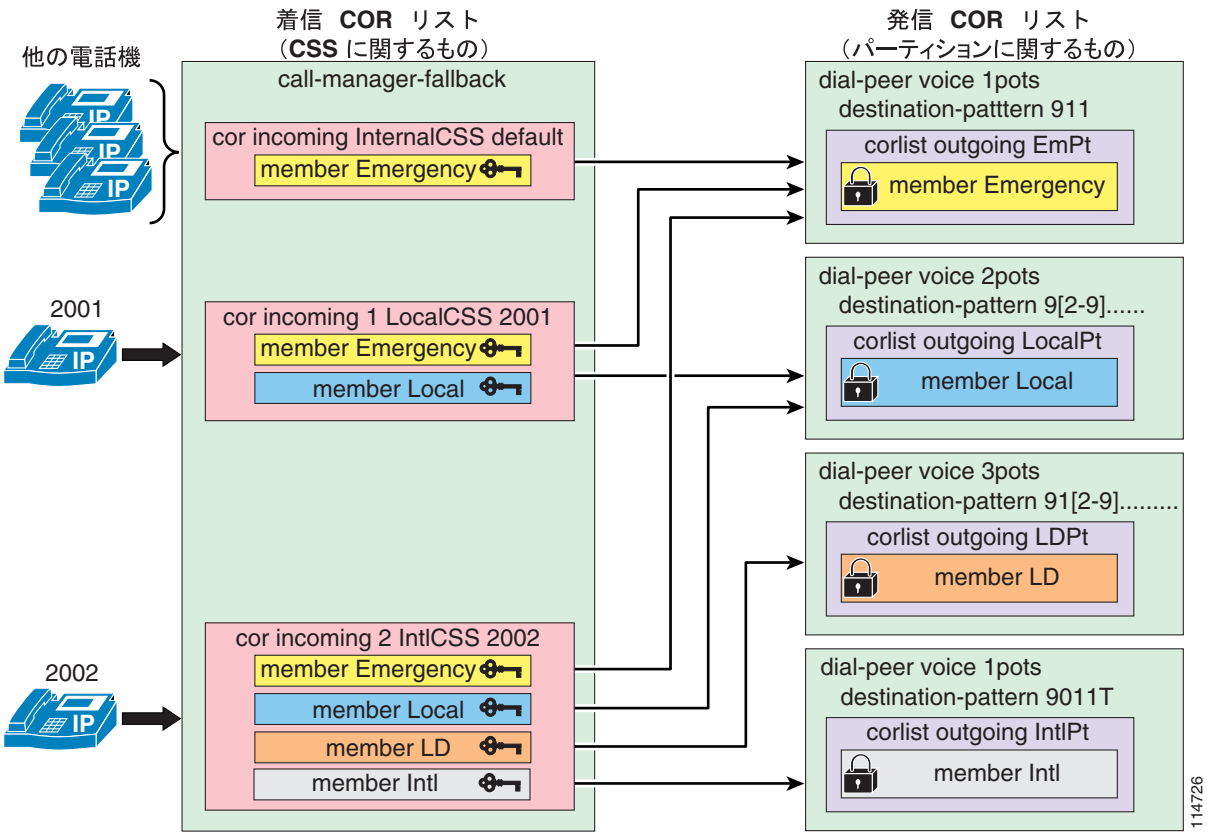
どちらの事例でも、制限クラス（COR）機能を使用して、サービス クラスを Cisco IOS ルータ内に定義します（COR の詳細については、P.10-52 の「H.323 ダイヤル ピアを使用する Cisco IOS のコール特権」を参照）。

次の主要ガイドラインに従うと、COR 機能を調整して、Cisco Unified CallManager のパーティションとコーリング サーチ スペースという概念を再現することができます。

- 区別する必要のあるコールのタイプごとに、タグを定義する。
- 各コール タイプをルーティングするそれぞれの POTS ダイヤル ピアに対して、メンバー タグを 1 つだけ含んだ、「基本的な」発信 COR リスト（パーティションに相当）を割り当てる。
- 各種のサービス クラスに属している IP Phone に対して、メンバー タグのサブセットを含んだ、「複雑な」着信 COR リスト（コーリング サーチ スペースに相当）を割り当てる。

図 10-39 では、SRST に基づいた実装例を示しています。DN が 2002 の IP Phone は、無制限の公衆網アクセスを許可され、DN が 2001 の IP Phone は、ローカル公衆網アクセスのみを許可されています。その他のすべての IP Phone は、内部番号と緊急サービスにのみアクセスできるように設定されています。

図 10-39　COR を使用した Cisco SRST 用サービス クラスの構築



次の手順では、図 10-39 のような Cisco IOS ソリューションの実装例とガイドラインを示します。

ステップ 1　**dial-peer cor custom** コマンドを使用して、各種コールの内容をわかりやすく表しているタグを定義します（この例では、Emergency、VMail、Local、LD、Intl）。

```
dial-peer cor custom
  name Emergency
  name VMail
  name Local
  name LD
  name Intl
```

ステップ 2　**dial-peer cor list** コマンドを使用して、パーティションとして使用される基本的な COR リストを定義します。各リストには、タグを 1 つのみメンバーとして含めます。

```
dial-peer cor list EmPt
  member Emergency

dial-peer cor list VMailPt
  member VMail

dial-peer cor list LocalPt
  member Local

dial-peer cor list LDPt
  member LD

dial-peer cor list IntlPt
  member Intl
```

ステップ 3　**dial-peer cor list** コマンドを使用して、コーリング サーチ スペースとして使用される比較的複雑な COR リストを定義します。各リストには、必要となるサービス クラスに従って、タグのサブセットをメンバーとして含めます。

```
dial-peer cor list InternalCSS
  member Emergency
  member VMail

dial-peer cor list LocalCSS
  member Emergency
  member VMail
  member Local

dial-peer cor list LDCSS
  member Emergency
  member VMail
  member Local
  member LD

dial-peer cor list IntlCSS
  member Emergency
  member VMail
  member Local
  member LD
  member Intl
```

ステップ 4　**corlist outgoing** *corlist-name* コマンドを使用して、基本的な「パーティション」COR リストを、対応する POTS ダイヤル ピアに割り当てる発信 COR リストとして設定します。

```
dial-peer voice 100 pots
  corlist outgoing EmPt
  destination-pattern 911
  no digit-strip
  direct-inward-dial
  port 1/0:23

dial-peer voice 101 pots
  corlist outgoing VMailPt
  destination-pattern 914085551234
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 102 pots
  corlist outgoing LocalPt
  destination-pattern 9[2-9]......
  forward-digits 7
  direct-inward-dial
  port 1/0:23

dial-peer voice 103 pots
  corlist outgoing LDPt
  destination-pattern 91[2-9]..[2-9]......
  forward-digits 11
  direct-inward-dial
  port 1/0:23

dial-peer voice 104 pots
  corlist outgoing IntlPt
  destination-pattern 9011T
  prefix-digits 011
  direct-inward-dial
  port 1/0:23
```

ステップ 5　**cor incoming** コマンドを **call-manager-fallback** 設定モードで使用して、「コーリング サーチ スペース」として機能する複雑な COR リストを、各種の電話 DN に割り当てる着信 COR リストとして設定します。

```
call-manager-fallback
  cor incoming InternalCSS default
  cor incoming LocalCSS 1 3001 - 3003
  cor incoming LDCSS 2 3004
  cor incoming IntlCSS 3 3010
```

SRST 用の COR を配置する場合は、次の制限事項に注意してください。

- Cisco IOS Release 12.2(8)T 以降で使用可能な SRST バージョン 2.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 5（デフォルト ステートメント含まず）です。
- Cisco IOS Release 12.3(4)T 以降で使用可能な SRST バージョン 3.0 では、**call-manager-fallback** で許容される **cor incoming** ステートメントの数は、最大で 20（デフォルト ステートメント含まず）です。

したがって、デフォルト以外の特権を持つユーザの電話 DN が連続しておらず、SRST サイトが比較的大きい場合は、SRST モードのサービス クラスの数を減らして、これらの制限値を超えずにすべての DN に対応できるようにする必要があります。

上の例は Cisco SRST に基づいていますが、Cisco Unified CallManager Express 配置にも同じ概念を適用することができます。ただし、次の考慮事項があります。

- Cisco Unified CallManager Express を使用している場合は、サービス クラスを表現している COR リスト（コーリング サーチ スペースに相当するもの）を個々の IP Phone に直接割り当てることができます。割り当てるには、**cor** {**incoming** | **outgoing**} *corlist-name* コマンドを **ephone-dn** *dn-tag* 設定モードで使用します。
- COR リストの設定されていない IP Phone は、COR の一般規則に従って、発信 COR リストの内容に関係なくすべてのダイヤル　　ピアに無制限にアクセスできます。Cisco　　Unified CallManager Express は、すべての電話にデフォルトの制限を適用する、**cor incoming** *corlist-name* **default** コマンドに相当するメカニズムを備えていません。

コール カバレッジの配置

コール カバレッジ機能は、多くの IP テレフォニー配置で重要となる機能です。顧客サービスを重視する多くの企業では、顧客のコールを適切なサービス部門に迅速にルーティングすることが必須になります。この項では、ハント パイロット、ハント リスト、および回線グループに基づいたハンティング メカニズムを使用して、Cisco Unified CallManager Release 4.1 でコールを分配する場合の設計ガイドラインを中心に説明します。ここでは、次のトピックを主に扱います。

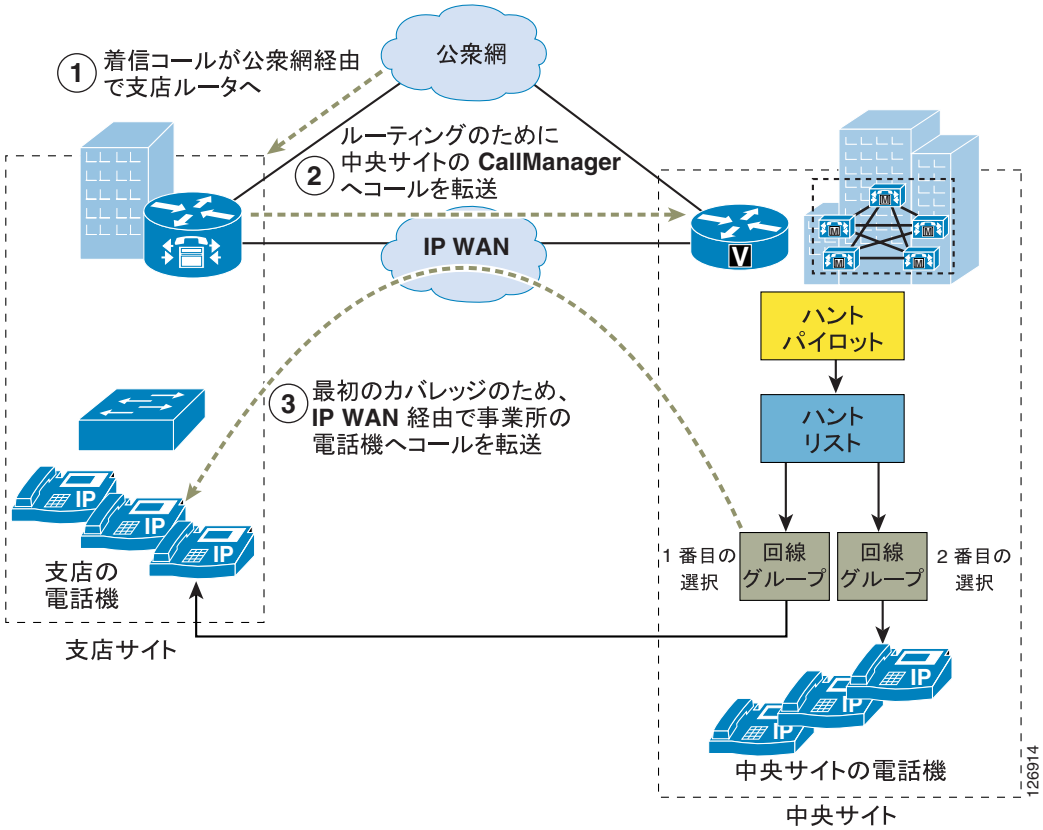
- マルチサイト集中型コール処理モデルへのコール カバレッジの配置（P.10-96）
- マルチサイト分散型コール処理モデルへのコール カバレッジの配置（P.10-98）

（注） コール カバレッジ機能自体はコール キューを提供せず、発信側には、コールの宛先が見つかるまでリングバック トーンが送信されます。プロンプトや Music On Hold などを提供するため、シスコでは Cisco Unified Customer Voice Portal（CVP）などの多数のコンタクト センター テクノロジーを用意しています。シスコから入手可能なコンタクト センター テクノロジーの詳細については、http://www.cisco.com/go/srnd で入手可能な資料を参照してください。

マルチサイト集中型コール処理モデルへのコール カバレッジの配置

図 10-40 では、マルチサイトの集中型コール処理配置における、ハント リストの設定例を示しています。この例では、最初にリモート オフィスのオペレータを通じてハント パイロット コールが分配されることを前提としています。コールは、応答されなかった場合やコール アドミッション制御によって拒否された場合、中央サイトのオペレータまたはボイスメールにルーティングされます。

図 10-40　集中型コール処理配置における複数のサイト間でのコール カバレッジ



集中型の IP テレフォニー システムでは、Automated Alternate Routing（AAR）や Survivable Remote Site Telephony（SRST）などの機能を有効にすることで、高い可用性を実現できます。AAR 機能や SRST 機能を有効にした上でコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- 自動代替ルーティング（AAR）

  回線グループのメンバーは、複数のロケーションおよびリージョンに割り当てることができます。ロケーションを通じて実装したコール アドミッション制御は、想定どおりに動作します。ただし、ハント パイロットから分配されているコールは、WAN の帯域幅が不足していたためにいずれかの回線グループ メンバーへのコールが Cisco Unified CallManager によってブロックされた場合には、AAR を使用して再ルーティングされることはありません。代わりに、Cisco Unified CallManager はコールを使用可能な次のメンバーまたは回線グループに分配します。

  （注） ハント　パイロットによって分配されるコールは、Cisco Unified CallManager　Release 4.1(3) の AAR を使用できます。ただし、AAR を使用するのは、回線グループ内でボイスメール ポートを使用している場合のみにすることを強くお勧めします。

- Survivable Remote Site Telephony（SRST）
  - Cisco Unified CallManager がハント パイロットのコールを受信したとき、その回線グループ メンバーの一部が、SRST モードで動作しているリモート サイトにある場合、Cisco Unified CallManager はそれらのメンバーをスキップし、使用可能な次の回線グループ メンバーにコールを分配します。Cisco Unified CallManager から見ると、SRST モードで動作しているメンバーは未登録であり、ハント パイロットのコールは未登録メンバーには転送されません。

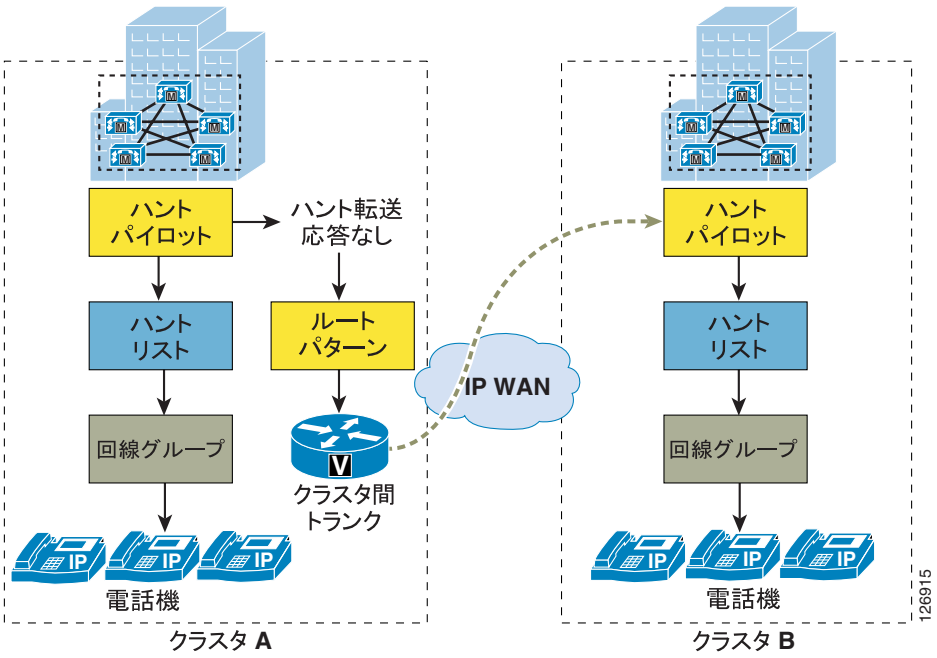
— SRST モードで動作しているルータがハント パイロットのコールを受信したときは、コール カバレッジ機能を使用できません。このコールは、使用可能な登録済み内線番号にコールを再ルーティングする設定が追加されていない場合、失敗します。**alias** コマンドまたは **default-destination** コマンドを Cisco IOS の **call-manager-fallback** モードで使用すると、ハント パイロットを宛先とするコールをオペレータ内線またはボイスメールに再ルーティングすることができます。

マルチサイト分散型コール処理モデルへのコール カバレッジの配置

Cisco Unified CallManager Release 4.1 以降では、ルート グループをハント リストに追加することができなくなりました。このため、ハント リストを使用して、コールを他のクラスタまたはリモート ゲートウェイに送信することはできません。ただし、Cisco Unified CallManager Release 4.1 で導入されたハント パイロットのハント オプション設定を使用して、ゲートウェイまたはトランクを指すルート パターンに対応付けることができます。

図 10-41 は、クラスタ間トランクを使用する分散型コール処理配置における、ハント リストの設定例を示しています。この例では、ハント パイロットのコールが最初にクラスタ A の内部に分配されることを前提としています。コールに対する応答がない場合は、ルート パターンに一致する Forward Hunt No Answer 設定を使用して、コールがコール分配のためにクラスタ B に再ルーティングされます。このルート パターンは、クラスタ B に向かうクラスタ間トランクを指しています。

図 10-41　分散型コール処理配置におけるクラスタ間でのコール カバレッジ



ヒント

分散型コール処理配置では、Cisco VoIP ゲートウェイとゲートキーパーを使用して、着信するハント パイロット コールの負荷共有を管理できます。あるクラスタ内でコールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することもできます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

ガイドライン

分散型コール処理モデルにコール カバレッジ機能を配置する場合は、次のガイドラインを考慮してください。

- コールが複数のクラスタにわたって分配される場合は、発信または着信のルート グループ デバイス上で実行される番号変換を考慮に入れて、ルート パターンを適切に設定する必要があります。番号変換が実行されない場合、設定するルート パターンとハント パイロットは、すべてのクラスタ上で同一にする必要があります。同一でない場合は、コールが適切に分配されません。
- 分散型コール処理配置では、Cisco VoIP ゲートウェイを使用して、着信ハント パイロット コールの負荷共有を管理できます。あるクラスタ内で着信コールに応答がなかった場合は、そのコールを別のクラスタにオーバーフローしてサービスを提供できます。

ヒント　コールは、ゲートウェイまたはトランクを通じて IVR 処理に送信することができます。Tool Command Language（TCL）IVR アプリケーションは、Cisco IOS ゲートウェイ上に実装できます。

ハント パイロットのスケーラビリティ

トップダウン、循環、および最長アイドル時間の各アルゴリズムを使用してコール カバレッジを配置する場合は、次のガイドラインを参考にすることをお勧めします。

- Cisco Unified CallManager クラスタは、最大で 15,000 のハント リスト デバイスをサポートします。
- ハント リスト デバイスは、1,500 個のハント リストそれぞれに 10 台の IP Phone を入れた組み合せにすることも、750 個のハント リストそれぞれに 20 台の IP Phone を入れた組み合せにすることもできます。ただし、ハント リストの数が多い場合は、その数に応じて、Cisco CallManager のサービス パラメータで指定するダイヤル プラン初期化タイマーの値を大きくする必要があります。ダイヤル プラン初期化タイマーは、ハント リストを 1,500 個設定する場合、600 秒に設定することをお勧めします。

（注）　コール カバレッジにブロードキャスト アルゴリズムを使用する場合、ハント リスト デバイスの数は、Busy Hour Call Completion（BHCC）の数によって制限されます。

- 1 つの回線グループ内に、コールをすべての DN に同時に送信することを目的として設定するディレクトリ番号の数は、最大で 35 までにすることをお勧めします。また、ブロードキャスト回線グループの数は、BHCC によって決まります。Cisco Unified CallManager システム内に複数のブロードキャスト回線グループがある場合、回線グループ内のディレクトリ番号の数は、35 よりも少なくする必要があります。すべてのブロードキャスト回線グループの Busy Hour Call Attempt（BHCA）の数が、1 秒あたり 35 コール セットアップを超えないようにします。

CHAPTER 11

緊急サービス

音声システムの適切な配置には、緊急サービスが非常に重要です。この章では、緊急コールのために不可欠な、次の設計上の主な考慮事項について説明しています。

- 911 機能の計画（P.11-2）
- ゲートウェイの考慮事項（P.11-11）
- Cisco Emergency Responder の考慮事項（P.11-13）

この章では、カナダと米国で配置されている 911 緊急ネットワークに固有の情報について、説明します。ここで説明されている概念の多くは、他の地域にも適応できます。緊急コール機能の適切な実装については、ローカル テレフォニー ネットワーク プロバイダーに問い合せてください。

米国の一部の州では、MLTS（Multi-Line Telephone System）のユーザに必要な 911 機能を対象とする法律がすでに制定されています。National Emergency Number Association（NENA）が作成した、『*Technical Information Document on Model Legislation Enhanced 911 for Multi-Line Telephone Systems*』は、次の Web サイトで入手可能です。

http://www.nena9-1-1.org/9-1-1TechStandards/TechInfoDocs/MLTS_ModLeg_Nov2000.PDF

米国連邦通信委員会（FCC）も、タイトル 47、パート 68、セクション 319 に新しいセクション案を作成しました。これは次の Web サイトで入手可能です。

http://www.apcointl.org/about/pbx/worddocs/mltspart68.doc

この章では、読者が北米在住の公衆網ユーザに使用可能な汎用 911 機能を十分理解していることを前提としています。この件の詳細については、次の URL で、北米の E911 サービスの現況の説明を参照してください。

http://www.nena.org/florida/Directory/911Tutorial%20Study%20Guide.pdf

911 機能の計画

ここでは、MLTS（Multi-Line Telephone Systems）におけるライフライン コールの機能要件の一部を説明しています。ライフライン コールとは、北米の公衆電話交換網（PSTN）によって処理される 911 コールのことです。

MLTS 配置を計画する場合は、まず、電話サービスに必要なすべての物理ロケーションを確立してください。これらのロケーションは、次のように分類できます。

- 単一の建物配置。すべてのユーザは同じ建物に住んでいます。
- 単一のキャンパス配置。ユーザは近くにある建物のグループに住んでいます。
- マルチサイト配置。ユーザは地理的に広い範囲に分散しており、WAN 接続を介してテレフォニー コール処理サイトにリンクされています。

これらのロケーション、つまり配置のタイプは、911 サービスの設計と実装に使用される基準に影響を与えます。次の項では、主な基準と、それぞれの標準的な状況および例外的な状況を共に説明します。これらの基準を分析し、適用する際には、ネットワーク内の電話ロケーションによって受ける影響を考慮してください。

Public Safety Answering Point（PSAP）

PSAP は、911 コールに応答して、適切な緊急対応（警察、消防署、または救急チームの派遣など）を手配する機関です。911 コールを発信する電話機の物理的なロケーションは、そのコールに応答する適切な PSAP を決定する基本要素です。一般に、各建物を、1 つのローカル PSAP が担当します。

所定のロケーションを担当する PSAP を確認するには、地域の防火管理者または警察署などの地域の公衆安全情報サービス機関に問い合せてください。また、通常、地域通信事業者のディレクトリにも、所定地域内の 911 コールを処理する機関がリストされています。

標準的な状況

- 1 つの番地に対して、1 つの PSAP だけが指定されます。
- 1 つの番地の 911 コールはすべて、同じ PSAP にルーティングされます。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP の管轄になります。
- 一部の 911 コールをオンネット ロケーション（キャンパスのセキュリティ、建物のセキュリティ）にルーティングする必要があります。

911 ネットワーク サービス プロバイダー

担当 PSAP を確認した後、各 PSAP が接続されている 911 ネットワーク サービス プロバイダーも特定する必要があります。通常、PSAP は公衆網から 911 電話コールを受信すると想定されますが、そうとは限りません。911 コールは、地域の重要な専用ネットワーク上で伝送され、各 PSAP は 1 つ以上のこうした地域ネットワークに接続されます。大部分の場合、既存 Local Exchange Carrier（LEC; 地域通信事業者）が PSAP の 911 ネットワーク サービス プロバイダーです。例外には、軍事施設、大学構内、国立または州立の公園、もしくは公衆安全の責任が地方自治体の管轄外であるロケーション、もしくは公共の地域通信事業者以外のエンティティによってプライベート ネットワークが運営されているロケーションがあります。

所定の PSAP の 911 ネットワーク サービス プロバイダーについて疑問がある場合は、その PSAP に直接連絡して、情報を確認してください。

標準的な状況

- 所定の番地の 911 ネットワーク サービス プロバイダーは、既存地域通信事業者（LEC）です。電話会社 X がサービスを提供するロケーションの場合、対応する PSAP も、電話会社 X からサービスを提供されます。
- すべての 911 コールは、オフネット ロケーションに直接ルーティングされるか、オンネット ロケーションに直接ルーティングされます。

例外的な状況

- MLTS インターフェイスから公衆網へ接続するために使用する地域通信事業者（LEC）と、PSAP に対して 911 ネットワーク サービス プロバイダーの役目をする LEC が異なる場合があります（たとえば、電話システムは電話会社 X からサービスを受け、PSAP は電話会社 Y に接続されている場合です）。この状況では、LEC 間の特別な調整、または電話システムと PSAP の 911 ネットワーク サービス プロバイダー間に特別な専用トランクが必要な場合があります。
- 一部の LEC は、ネットワーク上で 911 コールを受け入れることができません。この場合、LEC を変更するか、911 コールを適切な PSAP にルーティングできる LEC に接続されたトランク（911 コール ルーティング専用）を確立するかの 2 つのオプションしかありません。
- 一部（またはすべて）の 911 コールをオンネット ロケーション（キャンパスのセキュリティや建物のセキュリティ）にルーティングする必要があります。この状況は、設計および実装の段階で簡単に対応できますが、電話機ごとの 911 コールの宛先が、正しく計画され、文書化されている必要があります。

適切な 911 ネットワークへのインターフェイス ポイント

大規模なテレフォニー システムでは、911 接続に多数のインターフェイス ポイントが必要になる場合があります。一般に、複数の E911 選択ルータが LEC の管轄地区内で使用され、これらのルータは、通常、相互接続されません。

たとえば、大規模なキャンパスを備えた企業に、次の状況があるとします。

- 建物 A は San Francisco にある。
- 建物 B は San Jose にある。
- San Francisco 警察と San Jose 警察が、該当する PSAP である。
- San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーのサービスを利用している。
- しかし、San Francisco 警察と San Jose 警察は、同じ 911 ネットワーク サービス プロバイダーが運営する異なる E911 選択ルータのサービスを受けている。

このタイプの状況では、2 つの別々のインターフェイス ポイント（E911 選択ルータごとに 1 つずつ）が必要です。E911 選択ルータの管轄地区に関する情報は、一般に、担当 LEC が保持しており、その LEC の地域アカウント担当者が、企業カスタマーに関連情報を提供できます。多くの LEC は、911 問題の専門家のサービスも用意しています。この専門家は、911 アクセス サービスの適切なマッピングについてアカウント担当者と協議できます。

標準的な状況

- 単一サイト配置またはキャンパス配置では、通常、911 コール用に 1 つだけの PSAP があります。
- 1 つの PSAP のみへのアクセスが必要な場合は、1 つのインターフェイス ポイントだけが必要です。複数の PSAP へのアクセスが必要な場合でも、同じ集中インターフェイスを介して、同じ E911 選択ルータから到達可能です。企業の支店サイトが WAN を介してリンクされている場合（集中型コール処理）、Survivable Remote Site Telephony（SRST）操作がアクティブであるときに WAN 障害が発生した場合の 911 分離を防止するため、911 へのローカル（つまり、各支店内の）アクセスを各ロケーションに指定することをお勧めします。

例外的な状況

- キャンパスの物理的な規模により、一部の建物が別の PSAP 管轄になり、かつ
- 一部の 911 コールは、異なるインターフェイス ポイントを通じて、異なる E911 選択ルータにルーティングされる必要があります。

（注） PSAP と E911 選択ルータの地理的な管轄地区の設定に必要な情報は、オンライン、または各種の競合地域通信事業者（CLEC）の Web サイトから部分的に情報を入手できます。たとえば、https://clec.sbc.com/clec/hb/shell.cfm?section=782 では、SBC/Pacific Bell がカバーする管轄地区についての貴重なデータが提供されています。しかし、911 コール ルーティングを設計および実装する前に、該当するインターフェイス ポイントの適切な情報を LEC から入手しておくことを強くお勧めします。

インターフェイス タイプ

音声通信の提供に加えて、ネットワークへの 911 コールの発信に使用されるインターフェイスは、発信者についての識別データも提供する必要があります。

自動番号識別（ANI）は、ネットワークが適切な宛先へ 911 コールをルーティングするために使用する、発信者の E.164 番号を参照します。この番号は、PSAP がコールの ALI（Automatic Location Identification; 自動ロケーション識別）を検索するためにも使用されます。

911 コールは、ソースルートされます。つまり、911 コールは発信番号に応じてルーティングされます。別々のロケーションからすべて同じ番号（911）をダイヤルする場合でも、ANI によって表される起点ロケーションに基づいて、別々の PSAP に到達します。

次のインターフェイス タイプのどちらかを使用して、911 コール機能を実装できます。

- 動的 ANI 割り当て
- 静的 ANI 割り当て

動的 ANI 割り当ては、（複数の ANI をサポートするので）スケーラビリティに優れていますが、小規模のシステム配置には適していません。静的 ANI 割り込みは、最小のシステムから最大のシステムまで、より広範囲にわたる環境で使用できます。

動的 ANI（トランク接続）

動的 ANI では、システムの 1 つのインターフェイスを、911 ネットワークにアクセスする多数の電話機が共用します。また、ネットワークに送信される ANI がコールごとに異なっていることが必要な場合があります。

動的 ANI インターフェイスには、次の 2 つの主なタイプがあります。

- ISDN-PRI（Integrated Services Digital Network-Primary Rate Interface）または単に PRI
- CAMA（Centralized Automatic Message Accounting）

PRI

このタイプのインターフェイスは、通常、テレフォニー システムを公衆網 Class 5 スイッチに接続します。発番号（CPN）は、発信者の E.164 番号を識別するためにコールのセットアップ時に使用されます。

911 にコールする場合、LEC によって CPN を扱う方法が異なります。Class 5 スイッチ機能の制限、または LEC もしくは地方自治体の方針によっては、CPN が 911 コール ルーティング用の ANI として使用されない場合があります。この場合、CPN の代わりに LDN（Listed Directory Number）、または請求先番号（BTN）を ANI の目的で使用するように、ネットワークをプログラムすることができます。

CPN が ANI に使用されない場合、PRI インターフェイスから発信する 911 コールはすべて、911 ネットワークには同じように見えます。これらの 911 コールはすべて、同じ ANI をもち、同じ宛先（適切な宛先でない場合があります）にルーティングされるからです。

一部の LEC は、911 コールの CPN が PRI インターフェイスを通過するようにする機能を備えています。この機能を使用すると、コールのセットアップ時に Class 5 スイッチに提示された CPN は、コールをルーティングするために ANI として使用されます。この機能の名称は、LEC によって異なります（たとえば、SBC はカリフォルニアでこの機能を Inform 911 と呼びます）。

（注） CPN は、ルーティング可能な E.164 番号でなければなりません。つまり、CPN は、関連した E911 選択ルータのルーティング データベースに入力されている必要があります。

（注） ダイヤルイン方式（DID）の電話機の場合、DID 番号は、911 の目的で ANI として使用できますが、これは、911 サービス プロバイダーのネットワーク内で、緊急サービス番号に適切に関連付けられている場合だけです。DID 以外の電話機の場合は、別の番号を使用してください（詳細については、P.11-7 の「緊急ロケーション識別番号のマッピング」を参照してください）。

多くの Class 5 スイッチは、複数のエリア コードをサポートしないトランクを通じて、E911 選択ルータに接続されています。このような場合、PRI が 911 コールの伝送に使用される場合、適切にルーティングされる 911 コールだけが、Class 5 スイッチと同じ Numbering Plan Area（NPA）のある CPN（または ANI）を持ちます。

例

MLTS は、エリア コード 514（NPA = 514）の Class 5 スイッチに接続されるとします。MLTS が PRI トランク上で 911 コールを送信し、CPN が **450**.555.1212 である場合、Class 5 スイッチは、（正しい **450**.555.1212 ではなく）ANI **514**.555.1212 として E911 選択ルータにそのコールを送信するので、不適切なルーティングが実行され、ALI を取り出すための検索が発生します。

PRI を 911 インターフェイスとして適切に使用するには、システム計画者は、CPN が ANI に使用されることを確認し、リンク上で受け入れ可能な番号の範囲（NPA NXX TNTN の形式）を適切に識別する必要があります。たとえば、PRI リンクが、範囲 514 XXX XXXX 内の ANI 番号を受け入れるように指定されている場合、NPA = 514 の発番号を持つコールだけが適切にルーティングされます。

CAMA

CAMA（Centralized Automatic Message Accounting）トランクも、MLTS がコールを 911 ネットワークに送信することを可能にします。ただし、PRI 方式とは次の相違点があります。

- CAMA トランクは、E911 選択ルータに直接接続されます。E911 選択ルータと MLTS ゲートウェイ ポイント間の距離をカバーするために、マイレージ追加料金が適用される場合があります。

- CAMA トランクは、911 コールのみをサポートします。CAMA トランクの設置と操作に関連した資産コストと運営コストは、911 トラフィックのサポートのみに使用されます。
- MLTS 業界の CAMA トランクは、固定エリア コードに制限され、このエリア コードは、一般に、リンク プロトコルで黙示されます（つまり、明示的に送信されません）。接続には、すべてのコールが同じ固定エリア コードを共用するので、7 桁または 8 桁のみが ANI として送信されます。

（注） シスコは、VIC-2CAMA、VIC-2FXO、および VIC-4FXO トランク カードを介した CAMA ベースの 911 機能をサポートしています。

静的 ANI（回線接続）

静的 ANI は、公衆網との回線（トランクではなく）接続をサポートし、発信側の電話機の CPN に関係なく、回線の ANI が、その回線で発信されるすべての 911 コールに関連付けられます。一般電話サービス（POTS）が、この目的に使用されます。

POTS 回線は、最も単純かつ、最も広くサポートされている公衆網インターフェイスの 1 つです。POTS 回線は、通常、911 コールを受け入れるように設定されています。さらに、既存の E911 インフラストラクチャは、POTS 回線からの 911 コールを非常によくサポートします。

POTS には、次のような特徴があります。

- POTS 回線に関連した運用コストを低減できます。
- POTS 回線に、電源障害に備えたバックアップ回線の役割をもたせることができます。
- POTS 回線番号を、ALI データベースに入力されるコールバック番号として使用できます。
- POTS 回線は、公衆網へのローカル PRI、または CAMA アクセスに見合うユーザ密度をもたないロケーションに対して、最低コストで最適な 911 サポートを実現します。
- 公衆網の敷設に伴い、POTS 回線は広く普及しています。

このタイプのインターフェイスを介した発信 911 コールはすべて、E911 ネットワークによって同じものとして扱われます。ANI は POTS 回線番号に過ぎないので、E911 ネットワークに提示される ANI を Cisco Unified CallManager が制御できるようにするツール（たとえば、発信者番号変換マスク）は、無意味です。

緊急応答ロケーションのマッピング

National Emergency Number Association（NENA）は、最近、企業テレフォニー システムで 911 を規定する規則を制定する際に、州および国の機関が使用する法律モデルを提案しました。NENA 提案の概念の 1 つは、次のように定義される緊急応答ロケーション（ERL）です。

> *911 緊急応答チームの派遣先ロケーション：このロケーションは、緊急応答チームがそのロケーション内で発信者の位置をすばやく確認するための妥当な機会を提供できる、明確なものでなければならない。*

この要件は、各電話機のロケーションを個々に識別するのではなく、電話機を「ゾーン」（ERL）にグループ化することを見込んでいます。ERL の最大サイズは、この法律の地域ごとの実施に応じて異なる可能性がありますが、ここでは説明の基準として 7000 平方フィートを使用します（ここで説明する概念は、任意の州または地域で許可される最大 ERL サイズとは無関係です）。

緊急ロケーション識別番号（ELIN）が各 ERL に関連付けられます。ELIN は、E911 ネットワーク内でコールのルーティングに使用される完全修飾 E.164 番号です。関連した ERL から発信するすべての 911 コールで、ELIN が E911 ネットワークに送信されます。このプロセスは、911 の目的で、複数の電話機を同じ完全修飾 E.164 番号に関連付けることを可能にし、DID 電話機と非 DID 電話機にも同様に適用できます。

(注)　このマニュアルは、法律の実際の要件を提示しようとするものではありません。ここで提示する情報や例は、説明のためだけのものです。システム計画者の責任において、適用されるローカル要件を確認してください。

たとえば、ある建物の床面積が 70,000 平方フィートであり、100 台の電話機があるとします。911 機能を計画する際に、この建物を 7000 平方フィートごとの 10 個のゾーン（ERL）に分割し、各電話機を、それが置かれている ERL に関連付けることができます。911 コールが発信されると、関連した ELIN を PSAP に送信することによって、ERL（複数の電話機に対して同一）が識別されます。この例のように、電話機が均等に分散されている場合、10 台の電話機を持つ各グループには、同じ ERL があり、したがって同じ ELIN をもちます。

各種法律により、最小台数の電話機（たとえば 49）と最低床面積（たとえば、40,000 平方フィート）が定義されます。この数を下回ると、MLTS 911 の要件は適用されません。しかし、法律が企業の 911 機能を要求しない場合であっても、911 機能をプロビジョニングすることが常に最善の方法です。

緊急ロケーション識別番号のマッピング

一般に、緊急ロケーション識別番号（ELIN）と呼ばれる 1 つの完全修飾 E.164 番号を、各 ERL に関連付ける必要があります（ただし、Cisco Emergency Responder を使用する場合は、ERL ごとに複数の ELIN を設定できます）。ELIN は、E911 インフラストラクチャ全体でコールをルーティングするために使用され、ALI データベースへのインデックスとして PSAP が使用します。

ELIN は次の要件を満たす必要があります。

- ELIN は、E911 インフラストラクチャ全体でルーティング可能でなければなりません（P.11-4 の「インターフェイス タイプ」の項の例を参照してください）。ELIN がルーティング不能である場合、関連した ERL からの 911 コールは、E911 選択ルータでプログラムされたデフォルト ルーティングに応じて処理されます。
- 企業の ERL-to-ELIN マッピングが定義された後、LEC を使用して、対応する ALI レコードを設定する必要があります。その結果、PSAP にサービスを提供する ANI と ALI データベース レコードを正確に更新することができます。

ELIN マッピング プロセスは、所定の ERL に対する E911 インフラストラクチャとのインターフェイスのタイプに応じて、次のどちらかを選択できます。

- 動的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は MLTS によって制御されます。MLTS のテレフォニー ルーティング テーブルは、発信側電話機の ERL に基づいて、正しい ELIN をコールに関連付けます。Cisco Unified CallManager では、変換マスクを使用して、911 へのコールの発番号を変更できます。たとえば、所定の ERL 内にあるすべての電話機が、トランスレーション パターン（911）を含み、かつ電話機の CPN をそのロケーションの ELIN に置き換える発信者番号変換マスクも含むパーティションをリストする同じコーリング サーチ スペースを共有できます。

- 静的 ANI インターフェイス

  このタイプのインターフェイスを使用すると、ネットワークに渡される発番号識別は公衆網によって制御されます。これは、インターフェイスが POTS 回線である場合に該当します。ELIN は POTS 回線の電話番号であり、電話機の発信者識別番号に追加操作はできません。

PSAP コールバック

PSAP は、最初の会話の完了後、発信者に到達できることが必要な場合があります。PSAP がコールバックできるかどうかは、PSAP が最初の着信コールと共に受信する情報によって決まります。

この情報は、次の 2 つの部分から成るプロセスによって、PSAP に送信されます。

1. まず、自動番号識別（ANI）が PSAP に送信されます。ANI は、コールをルーティングするために使用される E.164 番号です。この説明では、PSAP で受信された ANI は、MLTS が送信した ELIN を指しています。
2. PSAP は ANI を使用して、データベースを照会し、自動ロケーション識別（ALI）を抽出します。ALI は、次のような情報を PSAP 係員に知らせます。
   - 発信者の名前
   - 住所
   - 該当する公衆安全機関
   - コールバック情報を組み込むことができる、その他のオプション情報。たとえば、救援活動の調整に役立てるために、企業のセキュリティ サービスの電話番号がリストされています。

標準的な状況

- ANI 情報が PSAP コールバックに使用されます。ここでは、ELIN がダイヤル可能番号であると想定します。
- ELIN は、MLTS に関連した公衆網番号です。公衆網から ELIN にコールすると、そのコールは、MLTS によって制御されるインターフェイス上で終端します。
- システム内の任意の ELIN に発信されたコールが、関連した ERL のすぐ近くにある電話機（または複数の電話機）を鳴らすように、コール ルーティングをプログラムするのは、MLTS システム管理者の責任です。
- ERL-to-ELIN マッピングが設定された後、修正が必要なのは、企業の物理的な状況に変更があった場合だけです。電話機が単に追加、移動、またはシステムから削除された場合、ERL-to-ELIN マッピングと、それに関連した ANI/ALI データベース レコードは変更する必要はありません。

例外的な状況

- 発信 ERL のすぐ近くへのコールバックを、オンサイト緊急デスクへのコールバックのルーティングと組み合せる（もしくは、置き換える）ことができます。これは、PSAP が最初の発信者を呼び出し、緊急事態に対してただちに支援を要請するときに役立ちます。
- たとえば、エリア コードの分割、公衆安全業務の新しい配分を必要とする地方自治体業務の変更、新しい建物の追加、または 911 の目的でコールの望ましいルーティングに影響を与えるその他の変更により、企業の状況が変わる場合があります。こうした状況では、企業の ERL-to-ELIN マッピングおよび ANI/ALI データベース レコードの変更が必要です。

非固定電話機の考慮事項

この章のここまでの説明はすべて、電話機のロケーションが静的（固定）であることを前提としていました。しかし、電話機が ERL 境界を越えて移動する場合、新しい場所に移動した電話機からの 911 コールは、正しくルーティングされません。別の ERL に物理的に配置されるので、電話機は現在の ERL の ELIN を使用する必要があります。Cisco Unified CallManager データベースで設定が変更されない場合、次のイベントが発生します。

- 旧 ERL の ELIN が、E911 インフラストラクチャ上のコールのルーティングに使用されます。
- IP ネットワークから E911 インフラストラクチャへの出口点が正しくない可能性があります。
- PSAP に提供されるコールバック機能により、誤った宛先に到達する可能性があります。
- ALI 情報が PSAP に提供されると、緊急応答担当者を誤ったロケーションに派遣する可能性があります。
- 電話機に対するロケーション ベースのコール アドミッション制御は、電話機の WAN 帯域幅使用量を正しく把握できず、WAN 帯域幅リソースのオーバーサブスクリプションやアンダーサブスクリプションが発生する可能性があります。

この状況を修復する方法は、Cisco Unified CallManager における電話機の設定（コーリング サーチ スペースやロケーション情報など）を手動で更新して、新しい物理ロケーションを反映することだけです。

Cisco Emergency Responder

移動、追加、および変更の管理が容易であることが、IP テレフォニー テクノロジーの主な利点の 1 つです。ユーザが介入することなく自動的に 911 情報を更新する移動、追加、および変更をサポートするために、シスコは、Cisco Emergency Responder（Cisco ER）と呼ばれる製品を開発しました。

Cisco ER は、次の主な機能を備えています。

- 検出された電話機の物理ロケーションに基づいて、電話機を ERL に動的に関連付けます。
- コールバックのために、ELIN　を発信側電話機に動的に関連付けます。上記の項で説明されている ER 以外のシナリオと異なり、Cisco ER は、911 コールを発信した電話機にコールバックできるようにします。
- 緊急コールが進行中であることを知らせるために、指定された通話者へのオンサイト通知が可能です（ポケットベル、Web ページ、または電話による）。ポケットベルと Web ページによる通知には、発信者の名前と電話番号、ERL、およびそのコールに関連した日付と時刻の詳細が含まれます。電話による通知では、緊急コールの発信番号に関する情報が提供されます。

Cisco ER の詳細は、P.11-13 の「Cisco Emergency Responder の考慮事項」の項、および次の Web サイトで入手可能な Cisco ER 製品資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/respond/index.htm

Cisco ER の主な機能は、電話機が 911 コールを発信したネットワーク ポート（ファースト イーサネット スイッチ ポートなどのレイヤ 2 ポート）の検出による、電話機のロケーションの検出に依存します。この検出メカニズムは、主に次の 2 つの前提事項に依存します。

- 企業のワイヤード インフラストラクチャが十分に確立され、散発的な変更が行われないこと。
- Cisco ER が、このインフラストラクチャをブラウズできること。つまり、Cisco ER は、敷設されたネットワーク インフラストラクチャとの簡易ネットワーク管理プロトコル（SNMP）セッションを確立することができ、接続された電話機を検出するためにネットワーク ポートをスキャンできること。

Cisco ER はコールの発信ポートを検出した後、そのコールを、そのポートのロケーション用にあらかじめ設定された ERL に関連付けます。このプロセスは、ロケーションにあらかじめ設定された ELIN との関連付け、および発信 ERL に基づく、E911 インフラストラクチャとの適切な出口点の選択も行います。

Cisco ER では、上記の項で説明されている ERL-to-ELIN マッピング プロセスが適用されますが、相違点が 1 つあります。それは、Cisco ER を使用しない場合、各 ERL は 1 つの ELIN だけに関連付けられますが、Cisco ER を使用すると、ERL ごとに複数の ELIN を使用できることです。この機能拡張の目的は、次の例に示されているように、同じ期間内に 1 つの ERL から複数の 911 コールが発信される特定のケースに対応するためです。

例 1

- 電話機 A と電話機 B はどちらも、ERL X 内に置かれ、ERL X は ELIN X に関連付けられています。
- 電話機 A は 13:00 に 911 にコールします。ELIN X は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、解除します。その後、13:15 に電話機 B が 911 にコールします。再び ELIN X が、コールを PSAP X にルーティングするために使用されます。
- PSAP X は、電話機 B からコールを解除した後、電話機 A の最初のコールに関連した詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X にダイヤルしますが、（目的の電話機 A ではなく）電話機 B につながります。

この状況を回避するために、Cisco ER では、ERL ごとに ELIN のプールを定義できます。このプールにより、後続のコールごとに別個の ELIN をラウンドロビン方式で使用できます。この例で ERL X に対して 2 つの ELIN を定義すると、例 2 で説明する状況になります。

例 2

- 電話機 A と電話機 B はどちらも、ERL X 内に置かれ、ERL X は ELIN X1 と ELIN X2 の両方に関連付けられます。
- 電話機 A は 13:00 に 911 にコールします。ELIN X1 は、そのコールを PSAP X にルーティングするために使用され、PSAP X はそのコールに応答し、解除します。その後、13:15 に電話機 B が 911 にコールし、このコールを PSAP X にルーティングするのに ELIN X2 が使用されます。
- PSAP X は、電話機 B からコールを解除した後、電話機 A の最初のコールに関連した詳細情報を取得するために、電話機 A にコールバックすることを決定します。PSAP は ELIN X1 にダイヤルし、電話機 A につながります。

もちろん、3 番目の 911 コールが発信されたが ERL に 2 つの ELIN しかない場合、コールバック機能では、最後の 2 人の発信者にしか正しく到達できません。

緊急コール ストリング

アクセス コード（たとえば、9）を使用するかどうかにかかわらず、システムが緊急コールを認識しやすいように、ダイヤル プランを設定することが望まれます。北米の緊急ストリングは、通常、911 です。ストリング 911 と 9911 の両方を認識するように、システムを設定することを強くお勧めします。

緊急ルート パターンに Urgent Priority のマークを明示的に付けて、Cisco Unified CallManager が、コールのルーティング前に、桁間タイムアウト（Timer T.302）を待機しないようにすることも強くお勧めします。

これ以外の緊急コール ストリングを、システム上で並行してサポートすることができます。選択した緊急コール ストリング使用を想定した訓練をテレフォニー システム ユーザに行うことをお勧めします。

また、ユーザが誤って緊急ストリングをダイヤルした場合に適切な対応ができるように訓練することも望まれます。北米では、アクセス コード 9 を使用して長距離番号にアクセスしようとするユーザが、誤って 911 をダイヤルする可能性があります。このような場合、ユーザは、緊急事態ではないので、緊急隊員を派遣する必要がないことを確認するために、回線を保持する必要があります。Cisco ER のオンサイト通知機能では、誤って発信されたコールを含め、911 に発信されたすべてのコールの詳細なアカウントを提供することによって、そのような疑わしい 911 コールの起点にある電話機を識別できます。

ゲートウェイの考慮事項

システムの緊急コールを処理するゲートウェイを選択する際には、次の要素を考慮してください。

- ゲートウェイの配置（P.11-11）
- ゲートウェイのブロック（P.11-11）
- 応答監視（P.11-12）
- 応答監視（P.11-12）

ゲートウェイの配置

地域通信事業者（LEC）ネットワーク内で、911 コールは、コールの起点に基づいて、ローカル側で有効なインフラストラクチャ上でルーティングされます。サービスを提供する Class 5 スイッチは、ロケーションに関連した PSAP に直接接続されるか、E911 選択ルータに接続されます。この選択ルータ自体は、その地域に有効な PSAP 群に接続されます。

シスコの IP ベースの企業テレフォニー アーキテクチャでは、リモート側に置かれているゲートウェイに、オンネットでコールをルーティングすることが可能です。たとえば、San Francisco に置かれている電話機は、IP ネットワークを介して、San Jose にあるゲートウェイにコールを伝送してから、LEC のネットワークに送信することができます。

911 コールの場合、緊急コールが適切なローカル PSAP にルーティングされるように、LEC ネットワークへの出口点を選択することが重要です。上記の例では、San Francisco の電話機からの 911 コールが、San Jose のゲートウェイにルーティングされてしまうと、San Francisco の PSAP に到達できません。これは、そのコールを受信する San Jose の LEC スイッチには、San Francisco PSAP にサービスを提供する E911 選択ルータへのリンクがないからです。さらに、San Jose 地域の 911 インフラストラクチャは、San Francisco の発番号に基づいてコールをルーティングすることができません。

大まかに言えば、発信側電話機と物理的に同じ場所にあるゲートウェイに、911 コールをルーティングしてください。共通ゲートウェイを使用して、複数のロケーションからの 911 コールを集約できるかどうかは、LEC に問い合せてください。所定の地域の 911 ネットワークが、911 コールに中央ゲートウェイを使用しやすい場合でも、911 コール ルーティングが WAN 障害中の影響を受けないように、発信側電話機と同じ場所にあるゲートウェイを使用することが望ましいことに注意してください。

ゲートウェイのブロック

911 コールが「全トランク使用中」状況にならないようにすることが望まれます。911 コールを接続する必要がある場合、トランキング リソースの不足により他のタイプのコールがブロックされる場合でも、911 コールは処理可能にしておく必要があります。このような状況に備えて、明示トランク グループを 911 コール専用にすることができます。

緊急コールを独占的に緊急トランク グループにルーティングするのが、好ましい方法です。もう 1 つの方法は、通常の公衆網コールと同じトランク グループに緊急コールを送信し（インターフェイスが許可する場合）、専用緊急トランク グループへの代替パスを用意するものです。後者の方法では、最大限の柔軟性が得られます。

たとえば、緊急コールを PRI トランク グループに向け、オーバーフロー状態になったときに備えて POTS 回線への代替パス（緊急コール専用に予約済み）を指定することができます。代替トランク グループに 2 つの POTS 回線を入れる場合、メインのトランク グループで許可されたすべてのコールの他に、少なくとも 2 つの 911 コールを同時にルーティングできることを保証します。

優先ゲートウェイが使用不能になる場合、緊急コールを代替番号にオーバーフローさせて、代替ゲートウェイが使用されるようにすることができます。たとえば、北米で 911 にダイヤルされたコールは、E.164（911 以外）ローカル緊急番号にオーバーフローすることができます。この方法は、北米の 911 ネットワーク インフラストラクチャを利用しません（つまり、選択ルーティング、ANI、または ALI サービスを使用しません）。この方法は、該当する公衆安全機関によって受け入れられる場合に限り、ネットワーク リソースの不足による緊急コールのブロックを回避する最後の手段としてのみ使用してください。

応答監視

通常の状態では、緊急番号に発信されたコールは、PSAP との接続後、応答監視を戻します。応答監視は、他のコールと同じように、オンネット発信者と、LEC ネットワークへの出口インターフェイスとの間の全二重音声接続をトリガできます。

一部の北米 LEC では、「無料」コールを行う場合、応答監視は戻されません。これは、一部のフリーダイヤル番号（たとえば、800 番）にも該当します。例外的な状況では、緊急コールは「無料」コールと見なされるので、PSAP との接続後、応答監視は戻されません。この状況は、911 テストコールを発信するだけで検出できます。PSAP との接続後、音声が存在する場合、コール タイマーが発信コールの所要時間を記録します。コール タイマーがない場合は、応答監視が戻されなかった可能性があります。応答監視が戻されない場合、LEC に連絡して、この状況を報告することをお勧めします。おそらく、望ましい機能ではありません。

この状況が地域通信事業者によって修正できない場合、LEC ネットワークにコールが発信されるときに応答監視を必要としないように出口ゲートウェイを設定することをお勧めします。また、応答監視が戻されない場合でも、進行標識音、代行受信メッセージ、および PSAP との通信が可能であるように、両方向で音声をカットスルーすることもお勧めします。

デフォルトでは、Cisco IOS ベースの H.323 ゲートウェイは、両方向で音声を接続するために、応答監視を受信する必要があります。これらのゲートウェイ上で応答監視の必要をなくすには、次のコマンドを使用してください。

- **progress_ind alert enable 8**

  このコマンドは、アラートの受信時に経過識別子 8（インバンド情報が使用可能）を受信することに相当します。このコマンドを使用すると、ゲートウェイの POTS 側が、コールの起点方向の音声を接続できます。

- **voice rtp send-recv**

  このコマンドは、宛先スイッチから Connect メッセージを受信する前に、逆方向と順方向の両方の音声カットスルーを可能にします。このコマンドは、すべての Voice over IP（VoIP）コール（使用可能である場合）に影響を与えます。

応答監視が提供されない場合は、Call Detail Record（CDR; コール詳細レコード）が 911 コールの接続時間または期間を正確に反映しません。その結果、コール レポーティング システムが、911 コール関連の統計情報を正しく表すことができない場合があります。

いかなる場合でも、すべてのコール パスからの 911 コール機能をテストし、PSAP との接続後、応答監視が戻されることを確認することをお勧めします。

Cisco Emergency Responder の考慮事項

デバイス モビリティにより、緊急コールに特別な設計上の考慮事項が生じます。Cisco Emergency Responder（Cisco ER）は、デバイスの動的な物理ロケーションに基づいて、デバイス モビリティをトラッキングし、システムによる緊急コールのルーティングを適合させるために使用できます。

Cisco Unified CallManager と Emergency Responder とのバージョンの互換性

Cisco Unified CallManager 5.0 との互換性を維持するには、Emergency Responder 1.3(1) が必要です。Emergency Responder と Cisco Unified CallManager のソフトウェア バージョン間の互換性の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide 1.3(1)*』を参照してください。

http://www.cisco.com

コール アドミッション制御ロケーションを超えたデバイス モビリティ

集中型コール処理配置では、Cisco ER は、複数のコール アドミッション制御ロケーションにわたるデバイスの移動を完全にサポートすることはできません。これは、Cisco Unified CallManager が、デバイスの移動を認識しないからです。たとえば、電話機を支店 A から支店 B に物理的に移動したにもかかわらず、電話機のコール アドミッション制御ロケーションが同じままである（たとえば、Location_A）場合、Location_A に使用可能な帯域幅がすべて、他のコールで使用中であれば、その電話機から 911 に発信するコールは、コール アドミッション制御拒否によりブロックされる可能性があります。現在、ロケーション B にある電話機が、ロケーション B の PSAP との接続に使用されるゲートウェイと物理的に同じ場所にある場合でも、このコール ブロックは発生します。

同じ理由で、Cisco ER は、ゲートキーパーによって制御されるコール アドミッション制御ゾーン間のデバイス移動をサポートできません。ただし、Cisco ER は、コール アドミッション制御ロケーション内でのデバイスの移動を完全にサポートできます。

集中型コール処理配置では、Cisco ER は、支店内のデバイス移動を自動的にサポートします。ただし、デバイスが支店間を移動する場合、Cisco ER が 911 コールを完全にサポートできるようにするには、デバイスのロケーションとリージョンのパラメータを手動で調整する必要があります。

デフォルトの緊急応答ロケーション

Cisco ER が、電話機の物理的なロケーションを直接判別できない場合、コールにデフォルトの緊急応答ロケーション（ERL）を割り当てます。デフォルトの ERL は、こうしたすべてのコールを、特定の PSAP に導きます。この状態が発生した場合、コールの送信先について共通の推奨事項はありませんが、通常、中央に置かれ、最大の公衆安全管轄権を提示する PSAP を選択するのが望ましい方法です。また、デフォルト ERL の緊急ロケーション識別番号（ELIN）の ALI レコードに、企業の緊急番号の連絡先情報を取り込み、発信者のロケーションの不確実さについての情報を提供することも、お勧めします。さらに、緊急コールのデフォルト ルーティングが発生したという注記を、ALI レコードに付けることもお勧めします。

ソフト クライアント

Cisco IP Communicator などのソフト クライアントが企業内で使用される場合、Cisco ER は、デバイス モビリティをサポートできます。しかし、企業の境界外でソフト クライアントが使用される場合（たとえば、ホーム オフィスやホテルからの VPN アクセス）、Cisco ER は、発信者のロケーションを判別できません。さらに、Cisco のシステムで、発信者のロケーションに該当する PSAP にコールを送信できるように、適切な位置にゲートウェイが配置されている可能性はほとんどありません。

ソフト クライアントに 911 コールの使用を許可するか、許可しないかは、企業ポリシーの問題です。インターネット上でローミングする可能性があるソフト クライアントに対して、企業のポリシーとして 911 コールを許可しないことをお勧めします。それにもかかわらず、このようなユーザが 911 をコールした場合、ベスト エフォート型のシステム応答では、オンサイト保安部隊、またはシステムのメイン サイトに近い大規模 PSAP のどちらかに、コールをルーティングします。

次のパラグラフは、ソフト クライアント ユーザに対して緊急コール機能が保証されていないことを警告するために、ユーザに発行される通知の例を示しています。

> *緊急コールは、設定されているサイト（たとえば、オフィス）に設置されている電話機から発信してください。地域保安当局は、設定されたサイトから移動された電話機からの緊急コールに応答しない可能性があります。設定済みのサイトから離れているときに、この電話機を緊急コールに使用する必要がある場合は、公共安全応答機関に、ロケーションについての特定情報を伝えてください。旅行または在宅勤務時の緊急コールには、サイトに対してローカル側で設定されている電話機（たとえば、ホテルの電話機や自宅の電話機）を使用してください。*

テスト コール

企業テレフォニー システムの場合、911 コール機能のテストは、初期インストール後だけでなく、予防手段として定期的に実施することをお勧めします。

テストの実行には、次の項目を参考にしてください。

- PSAP に連絡して、テスト前に許可を要請し、テストを実施する人物の連絡先情報を伝えます。
- 各コール発信時に、実際の緊急事態ではなく、単なるテストであることを伝えます。
- 通話者の画面上に表示される ANI と ALI を確認します。
- コールがルーティングされた先の PSAP を確認します。
- IP Phone 上のコール所要時間タイマーを調べることによって、応答監視が受信されたことを確認します。アクティブ コール タイマーは、応答監視が正しく機能していることを示します。

共用ディレクトリ番号への PSAP コールバック

Cisco ER は、緊急ロケーション識別番号（ELIN）に対する着信コールのルーティングを処理します。911 コールの発信元の回線が、共用ディレクトリ番号である場合、PSAP コールバックにより、すべての共用ディレクトリ番号アピアランスが鳴ります。その後、共用アピアランスのいずれかがコールに応答します。これは、911 コールが発信された電話機ではない可能性があります。

マルチクラスタの考慮事項

複数の Cisco Unified CallManager クラスタに基づく企業テレフォニー システムは、Cisco Emergency Responder（Cisco ER）の機能から利点を得ることができます。

ここで使用する用語の詳細、および次の説明を理解するために必要な背景情報については、『*Cisco Emergency Responder Administration Guide*』を参照してください。「Planning for Cisco Emergency Responder」の章は特に重要です。このマニュアルは、次の Web サイトで入手できます。

http://www.cisco.com

単一の Cisco ER グループ

単一の Emergency Responder グループを配置して、複数の Cisco Unified CallManager クラスタからの緊急コールを処理できます。この設計の目的は、どの電話機の緊急コールも、その Cisco ER グループにルーティングされることを保証することです。その Cisco ER グループが、ELIN を割り当て、電話機のロケーションに基づいてコールを適切なゲートウェイにルーティングします。

単一の Cisco ER グループを使用する 1 つの利点は、すべての ERL と ELIN が単一のシステムに設定されることです。単一の Cisco ER グループがシステムのすべてのアクセス スイッチのポーリングを担当しているため、どのクラスタに登録されている電話機でも、そのグループによって位置が確認されます。図 11-1 では、2 つの Cisco Unified CallManager クラスタとインターフェイスする単一の Cisco ER グループを示しています。

図 11-1　2 つの Cisco Unified CallManager クラスタに接続されている単一の Cisco ER グループ

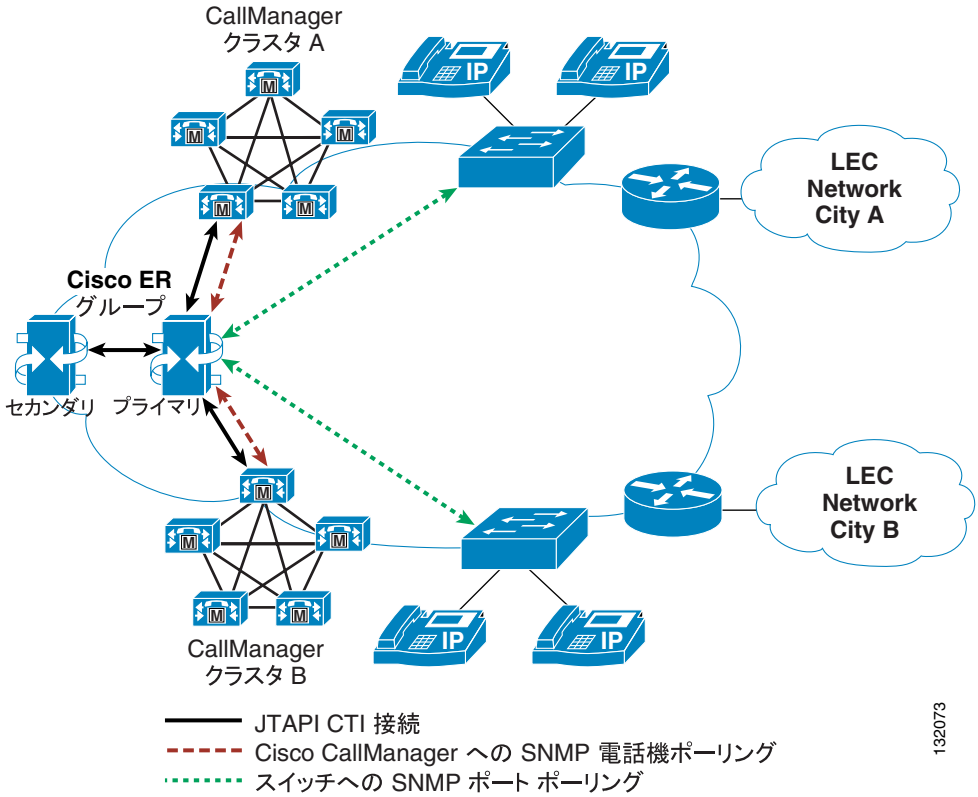


図 11-1 の単一の Cisco ER グループは、次のコンポーネントとインターフェイスします。

- SNMP を介して各 Cisco Unified CallManager クラスタとインターフェイスし、それぞれに設定されている電話機に関する情報を収集する。
- SNMP を介して企業のすべてのスイッチとインターフェイスし、どのスイッチに接続されているどのクラスタの電話機でも、その位置を確認できるようにする。電話機のロケーションが IP サブネットに基づいて識別される場合、この接続は不要です。IP サブネットベースの ERL を設定する方法の詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Configuring Cisco Emergency Responder」の章を参照してください。

  http://www.cisco.com

- JTAPI を介して各 Cisco Unified CallManager クラスタとインターフェイスし、911 をダイヤルするどの電話機にも必要なコール処理を可能にする。そのコール処理とは、発信側電話機の ERL の識別、ELIN の割り当て、（発信側電話機のロケーションに基づく）適切なゲートウェイへのコール リダイレクション、PSAP コールバック機能の処理などです。

Cisco Emergency Responder によって使用される JTAPI インターフェイスのバージョンは、Cisco Emergency Responder が接続される Cisco Unified CallManager ソフトウェアのバージョンによって決まります。システムの初期化時に、Cisco ER は Cisco Unified CallManager クラスタに問い合せ、適切な JTAPI Telephony Service Provider（TSP）をロードします。Cisco ER サーバ上には 1 つのバージョンの JTAPI TSP しか存在できないため、単一の Cisco ER グループがインターフェイスするすべての Cisco Unified CallManager クラスタが、同じバージョンの Cisco Unified CallManager ソフトウェアを実行する必要があります。

配置によっては、このソフトウェア バージョン要件によって問題が生じる場合があります。たとえば、Cisco Unified CallManager のアップグレード中は、クラスタが異なると、実行されているソフトウェアのバージョンが異なり、一部のクラスタが、Cisco ER サーバ上で実行されているバージョンと互換性のないバージョンの JTAPI を実行していることがあります。このような場合、Cisco ER グループの JTAPI バージョンとは異なるバージョンを実行しているクラスタからの緊急コールは、緊急番号の CTI ルート ポイントの Call Forward Busy 設定によって提供されるコール処理を受けることができます。

複数の Cisco Unified CallManager クラスタに対して単一の Cisco ER グループが適切であるかどうかを検討する場合は、次のガイドラインを適用してください。

- 緊急コールの数ができるだけ少ない許容可能なメンテナンス時間帯に（たとえば、営業時間後や、システムの使用量が最小限のとき）、Cisco Unified CallManager をアップグレードする。
- クラスタの数とサイズから判断して、ソフトウェアのアップグレード中に異なるバージョンの JTAPI が使用される時間を最小限に抑えることができると思われる場合にだけ、単一の Cisco ER グループを使用する。

たとえば、8 台のサーバで構成される 1 つの大規模なクラスタと、2 台のサーバで構成される 1 つの小規模なクラスタを同時に配置し、単一の Cisco ER グループと共に使用するとします。この場合、大規模なクラスタを最初にアップグレードすることをお勧めします。これにより、アップグレードのメンテナンス時間帯に Cisco ER サービスを使用できないユーザ（小規模なクラスタからサービスを受けるユーザ）の数を最小限に抑えることができます。さらに、小規模なクラスタのユーザは、Cisco ER に到達できない間、実際には、緊急コールの一時スタティック ルーティングによって適切にサービスを受けることができます。これは、そのユーザが、その時間中に発信されるすべての非 ER コールに割り当てられている単一の ERL/ELIN によって識別されることが可能なためです。

（注） Cisco Unified CallManager クラスタのいずれかが Cisco Unified CallManager Release 4.2 または 5.0 を実行する場合は、Emergency Responder バージョン 1.3(1) が必要です。

複数の Cisco ER グループ

マルチクラスタ システムをサポートするために、複数の Cisco ER グループを配置することもできます。この場合は、各 ER グループが次のコンポーネントとインターフェイスします。

- Cisco Unified CallManager クラスタ。次の方式を使用します。
  - SNMP：クラスタに設定されている電話機に関する情報を収集します。
  - JTAPI：適切なゲートウェイへの、またはローミング電話機の場合は適切な Cisco Unified CallManager クラスタへの、コール リダイレクションに関連するコール処理を可能にします。

- その Cisco ER グループの Cisco Unified CallManager に関連付けられているほとんどの電話機の接続先となるアクセス スイッチ（SNMP を使用）。

この方法を使用すると、Cisco Unified CallManager クラスタが、異なるバージョンのソフトウェアを実行できます。これは、各クラスタが、別の Cisco ER グループとインターフェイスするためです。

電話機がネットワーク上のさまざまな場所をローミングし、Cisco ER がその電話機をトラッキングできるようにするには、Cisco ER グループを 1 つの Cisco ER クラスタに設定する必要があります。Cisco ER のクラスタとグループの詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Planning for Cisco Emergency Responder」の章を参照してください。

http://www.cisco.com

図 11-2 では、Cisco ER クラスタリングの背後にある基本的な概念を表すトポロジの例を示しています。

図 11-2　複数の Cisco ER グループ

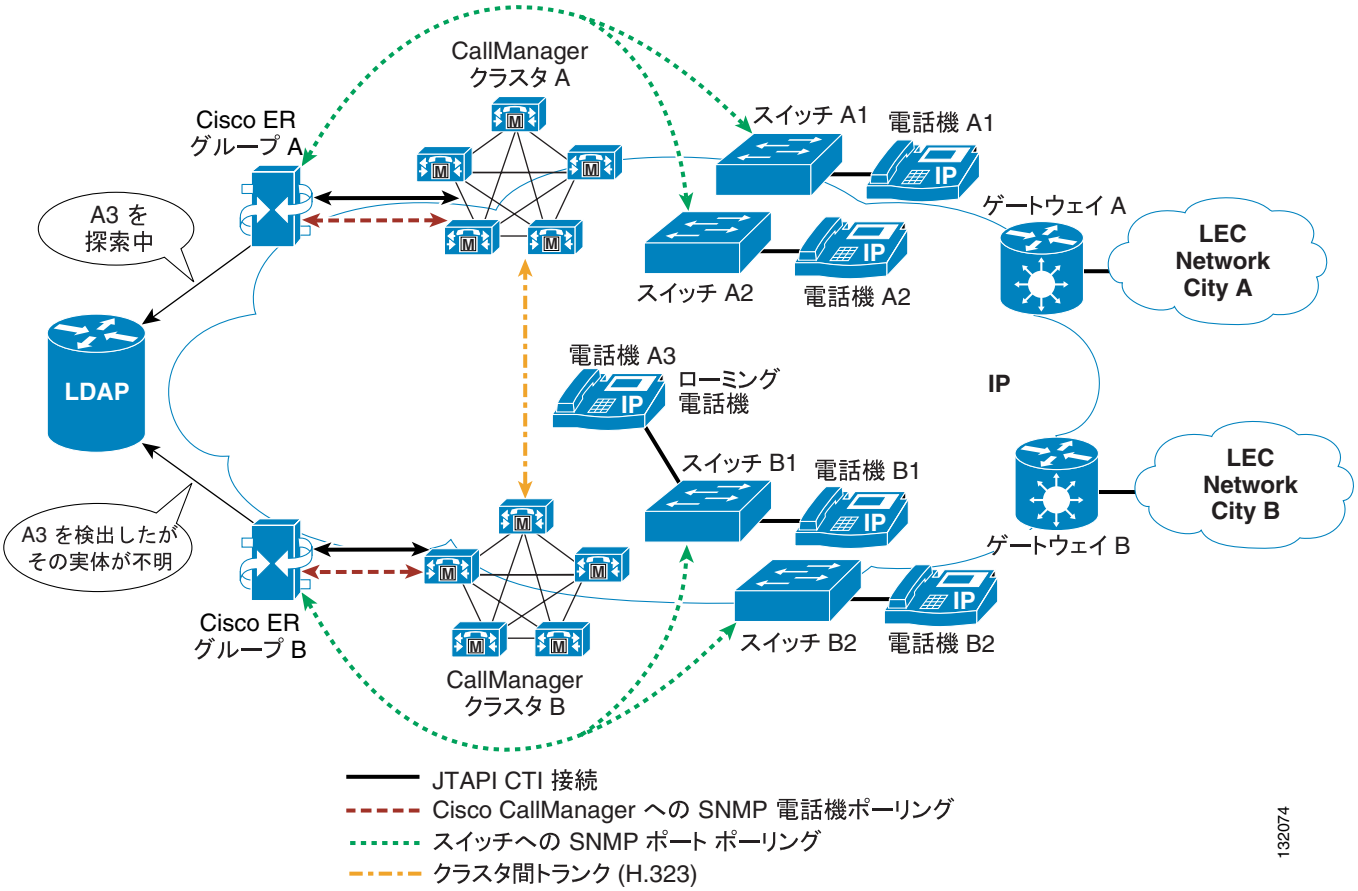


図 11-2 では、次のトポロジを示しています。

- Cisco ER グループ A は、Cisco Unified CallManager クラスタ A とインターフェイスして、スイッチ A1 および A2 にアクセスする。このグループは、Cisco Unified CallManager クラスタ A に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。
- 同様に、Cisco ER グループ B は、Cisco Unified CallManager クラスタ B とインターフェイスして、スイッチ B1 および B2 にアクセスする。このグループは、Cisco Unified CallManager クラスタ B に登録されているすべての電話機のホーム Cisco ER グループであると見なされます。

(注) Emergency Responder 1.3(1) を使用する場合は、ER クラスタのすべての ER グループが同じバージョンのソフトウェアを実行する必要があります。したがって、Cisco Unified CallManager クラスタのいずれかが Cisco Unified CallManager Release 4.2 または 5.0 を使用する場合は、すべての ER グループが Emergency Responder 1.3(1) を使用する必要があります。

Cisco ER グループのトラッキング ドメイン内の電話機移動

電話機が、同じホーム Cisco ER グループによって制御されるアクセス スイッチ間を移動する場合、その電話機の緊急コール処理は、単一の Cisco Unified CallManager クラスタを使用する配置で行われる処理と同じです。たとえば、アクセス スイッチ A1 と A2 の間を移動する電話機は、Cisco Unified CallManager クラスタ A に登録されたままで、移動前も移動後もその電話機のロケーションは Cisco ER グループ A によって特定されます。Cisco Unified CallManager クラスタ A による電話機検出と、スイッチ A2 による電話機のロケーション特定の両方で、電話機は引き続き Cisco ER グループ A の完全な制御下にあります。したがって、電話機は位置未確認の電話機と見なされません。

Cisco ER クラスタのさまざまなトラッキング ドメイン間の電話機移動

Cisco ER クラスタは、基本的に、Lightweight Directory Access Protocol（LDAP）データベースを介してロケーション情報を共有する Cisco ER グループの集まりです。各グループは、アクセス スイッチ上または IP サブネット内で検出するすべての電話機のロケーションを共有します。ただし、Cisco ER グループ独自の Cisco Unified CallManager クラスタ内で検出される電話機は*不明*であると見なされ、その情報は共有されません。

Cisco ER グループは、Cisco ER グループのトラッキング ドメイン内（スイッチまたは IP サブネット内）で位置を確認できないが、そのグループに関連付けられている Cisco Unified CallManager クラスタに登録されていることがわかっている電話機に関する情報も共有します。このような電話機は、*位置未確認*と見なされます。

異なる Cisco ER グループによって監視されるアクセス スイッチ間を電話機がローミングする場合、それらのグループは、電話機のロケーションに関する情報を交換できるように、1 つの Cisco ER クラスタに設定される必要があります。たとえば、Cisco Unified CallManager クラスタ A に登録されている電話機 A3 が、Cisco ER グループ B によって制御されるアクセス スイッチに接続されているとします。Cisco ER グループ A は、電話機 A3 が Cisco Unified CallManager クラスタ A に登録されていることを認識しますが、サイト A のどのスイッチでも電話機 A3 の位置を確認できません。したがって、電話機 A3 は Cisco ER グループ A によって*位置未確認*と見なされます。

これに反して、Cisco ER グループ B は、監視対象のスイッチの 1 つで、電話機 A3 の存在を検出します。電話機 A3 は、Cisco Unified CallManager クラスタ B に登録されていないため、*不明*な電話機として Cisco ER LDAP データベースを介してアドバタイズされます。

2 つの Cisco ER グループは、LDAP データベースを介して通信しているため、Cisco ER グループ B の*不明*な電話機 A3 が Cisco ER グループ A の*位置未確認*の電話機 A3 と同じであることがわかります。

Cisco ER グループ A の Unlocated Phone ページには、この電話機のホスト名が、リモート Cisco ER グループ（この場合は Cisco ER グループ B）と共に表示されます。

Cisco ER クラスタ内の緊急コール ルーティング

Cisco ER クラスタリングは、1 つの Cisco Unified CallManager クラスタと 1 つの Cisco ER で構成されるペア間で緊急コールをリダイレクトできるようにするルート パターンにも依存します。詳細については、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide*』の「Creating Route Patterns for Inter-Cisco Emergency Responder-Group Communications」の項を参照してください。

http://www.cisco.com

電話機 A3 が緊急コールを発信した場合、コール シグナリング フローは次のようになります。

1. 電話機 A3 が、処理のために緊急コール ストリングを Cisco Unified CallManager クラスタ A に送信する。
2. Cisco Unified CallManager クラスタ A が、リダイレクションのためにコールを Cisco ER グループ A に送信する。
3. Cisco ER グループ A が、電話機 A3 の位置を Cisco ER グループ B のトラッキング ドメイン内であると確認し、Cisco Unified CallManager クラスタ B を指すルート パターンにコールをリダイレクトする。
4. Cisco Unified CallManager クラスタ A がコールを Cisco Unified CallManager クラスタ B に送信する。
5. Cisco Unified CallManager クラスタ B が、リダイレクションのためにコールを Cisco ER グループ B に送信する。
6. Cisco ER グループ B が、電話機 A3 のロケーションに関連付けられている ERL と ELIN を識別し、コールを Cisco Unified CallManager クラスタ B にリダイレクトする。発信番号は、電話機 A3 の ERL に関連付けられている ELIN に変換されます。着信番号は、コールを適切なゲートウェイにルーティングするように変更されます。
7. Cisco Unified CallManager クラスタ B が、Cisco ER グループ B から入手した新しい着信番号情報に従ってコールをルーティングする。
8. Cisco Unified CallManager クラスタ B が、ゲートウェイを通じてコールを緊急公衆網ネットワークに送信する。

Cisco ER クラスタリングのスケーラビリティの考慮事項

Cisco ER クラスタでは、ホーム Cisco ER グループのトラッキング ドメイン外をローミングする電話機の数が、スケーラビリティ ファクタとなります。このような電話機の数は、次の Web サイトで入手可能な『*Cisco Emergency Responder Administration Guide 1.2(3)*』の「Network Hardware and Software Requirements」の項に記載されている制限内に収める必要があります。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

Cisco MCS 7845 サーバ プラットフォームおよび Cisco ER ソフトウェアのバージョン 1.2(3) では、Cisco ER クラスタは最大 3000 台のローミング電話機をサポートできます。この制限を超える必要のある配置（たとえば、複数の Cisco Unified CallManager クラスタを含む大規模なキャンパス配置）では、IP サブネットによって電話機の移動をトラッキングできます。各 Cisco ER グループに IP サブネットを定義し、Cisco ER グループごとに各 ERL を 1 つの ELIN に割り当てることによって、事実上、ローミング電話機をなくすことができます。これは、キャンパス内のすべての電話機が、それぞれの Cisco ER グループのトラッキング ドメインに含まれるためです。

ALI フォーマット

マルチクラスタ構成では、単一の Cisco ER グループに定義されている ERL と ELIN の物理ロケーションが、複数の電話会社の管轄地区にまたがることがあります。これにより、複数の LEC 用のレコードを含む共通ファイルから、さまざまな電話会社用のレコードを抽出する必要が生じることがあります。

Cisco ER は、この情報を、National Emergency Number Association（NENA）2.0、2.1、および 3.0 フォーマットに準拠する ALI レコードとしてエクスポートします。ただし、数多くのサービス プロバイダーが NENA 規格を使用しません。そのような場合は、Cisco ER によって生成された ALI レコードが、サービス プロバイダーによって指定されたフォーマットに準拠するように、ALI Formatting Tool（AFT）を使用してそのレコードを変更できます。これにより、サービス プロバイダーは、フォーマットし直されたファイルを使用して、ALI データベースを更新できます。

ALI Formatting Tool（AFT）では、次の機能を実行できます。

- レコードを選択し、ALI フィールドの値を更新する。AFT では、ALI フィールドを編集し、さまざまなサービス プロバイダーの要件を満たすようにカスタマイズできます。これにより、サービス プロバイダーは、フォーマットし直された ALI ファイルを読み取り、そのファイルを使用して ELIN レコードを更新できます。
- 複数の ALI レコードに対するバルク更新を実行する。バルク更新機能を使用すると、選択したすべてのレコード、1 つのエリア コード、または 1 つのエリア コードと 1 つのシティ コードに対して共通の変更を適用できます。
- エリア コード、シティ コード、または 4 桁のディレクトリ番号に基づいて ALI レコードを選択してエクスポートする。たとえば、あるエリア コードのすべての ALI レコードを選択してエクスポートすることにより、各サービス プロバイダーのすべての ELIN レコードに素早くアクセスできるため、複数のサービス プロバイダーを簡単にサポートできます。

AFT の柔軟性を利用して、単一の Cisco ER グループが、複数の ALI データベース フォーマットで ALI レコードをエクスポートできます。Cisco ER グループがサービスを提供する Cisco Unified CallManager クラスタが 2 つの LEC の管轄地区内にあるサイトを持つ場合、基本的な方法は次のとおりです。

1. Cisco Emergency Responder からの ALI レコード ファイル出力を標準の NENA フォーマットで入手します。このファイルには、複数の LEC 用のレコードが含まれています。
2. 必要な ALI フォーマットごとに元のファイルの 1 つのコピーを作成します（LEC ごとに 1 つのコピー）。
3. 最初の LEC（たとえば、LEC-A）の AFT を使用して、NENA フォーマットのファイルのコピーをロードし、他の LEC に関連付けられているすべての ELIN のレコードを削除します。削除する情報は、通常、NPA（またはエリア コード）によって識別できます。
4. 結果として生成されたファイルを、LEC-A に必要な ALI フォーマットで保存し、適宜ファイル名を付けます。
5. LEC ごとにステップ 3 ～ 4 を繰り返します。

ALI Formatting Tool は、次の Web サイトで入手できます。

http://www.cisco.com/en/US/products/sw/voicesw/ps842/prod_maintenance_guides_list.html

この URL にリストされていない LEC の場合、スプレッドシート プログラムや標準のテキスト エディタなど、標準のテキスト ファイル編集ツールを使用して Cisco Unified CallManager からの出力をフォーマットできます。

CHAPTER 12

サードパーティ製のボイスメール設計

この章では、Cisco Unified CallManager と共にサードパーティ製のボイスメール システムを配置するためのさまざまなオプションについて説明します。

(注) この章では、ポートやストレージに関して、ボイスメール　システムをサイジングする方法については説明しません。このような情報については、ボイスメール ベンダーに問い合せてください。特定のトラフィック パターンに基づき、ベンダー独自のシステムの個々の要件について詳細な説明を受けることができます。

数多くのボイスメール ベンダーが存在します。お客様が Cisco Unified CallManager を配置するときに、既存のボイスメール システムを引き続き使用するよう希望するのは、珍しいことではありません。このような要求を念頭において、シスコは、Simplified Message Desk Interface（SMDI）と呼ばれる業界標準のボイスメール プロトコルをサポートしています。SMDI はシリアル プロトコルであり、ボイスメール システムが適切にコールに応答するために必要なすべてのコール情報を提供します。

この他にも、Digital Set Emulation、Microsoft TAPI、QSIG など、Cisco Unified CallManager をボイスメール システムに統合するためのオプションがあります。各方法にはそれぞれ長所と短所があり、採用する方法は、ボイスメール システムがどのように現在の PBX に統合されているかに大きく左右されます。

ここでは、サードパーティ製のボイスメール システムと Cisco Unified CallManager の統合について、次の項目を説明します。

- SMDI（P.12-2）
- Digital Set Emulation（P.12-4）
- 二重 PBX 統合（P.12-5）
- 集中型ボイスメール（P.12-7）
- 確実な接続解除監視（P.12-12）
- サードパーティ製ボイスメール統合の要約（P.12-12）

SMDI

Cisco Unified CallManager では、次のいずれかの方法で SMDI を使用できます。

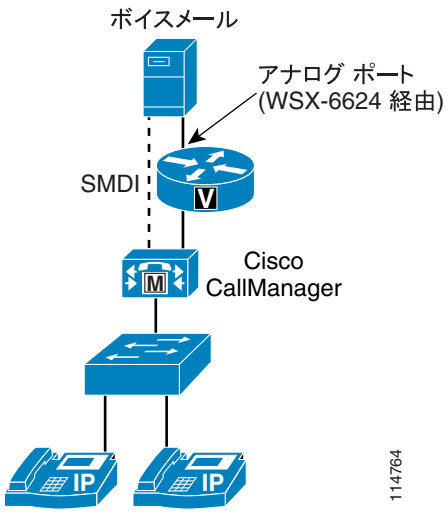
- Cisco Messaging Interface（P.12-2）
- Cisco VG248（P.12-3）

Cisco Messaging Interface

Cisco Messaging Interface（CMI）は、パブリッシャ サーバ上だけで実行する必要のある Cisco CallManager サービスです。このサービスは、ボイスメール用のコールを代行受信して、適切な SMDI メッセージを生成します。その後、この SMDI メッセージはサーバの Component Object Model（COM; コンポーネント オブジェクト モデル）ポートの 1 つに送信されます。CMI サービスは、アナログ FXS ポートまたは T1 CAS E&M をサポートするどの MGCP ゲートウェイにも対応しています。ただし、WS-X6624 モジュールと VG224 モジュールは、確実な接続解除監視（P.12-12 の「確実な接続解除監視」を参照）をサポートする 3 つしかないゲートウェイの 2 つであるため、現在 CMI サービスと共に使用することが推奨される最適のゲートウェイです。

図 12-1 では、Cisco Unified CallManager 内の CMI サービスを介して SMDI を使用する方法を示しています。

図 12-1　Cisco Unified CallManager を介した SMDI



Cisco Unified CallManager は、CMI を介して、事実上、アナログ FXS ポートを備えた SMDI を提供できるどのボイスメール システムとの統合もサポートしています。このボイスメール システムには、次のようなものがあります。

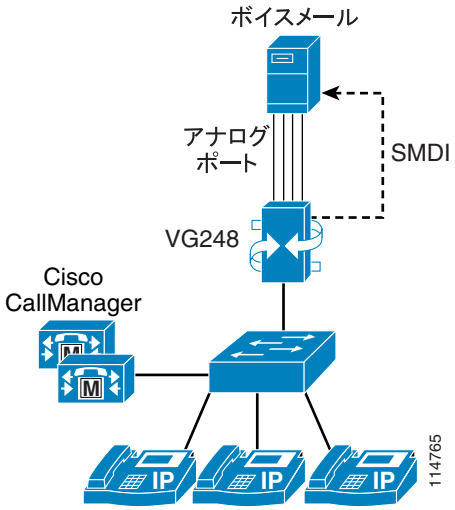
- Octel 100、200/300、および 250/350
- Intuity Audix
- Siemens PhoneMail
- Centigram/BayPoint（OnePoint Messenger および NuPoint Messenger）
- Lyrix ECS
- IBM Message Center

Cisco VG248

Cisco VG248 は SCCP ゲートウェイであり、48 個のアナログ FXS ポートをサポートし、ローカルで SMDI を生成します（つまり、CMI サービスとは関係なく動作します）。WS-X6624 モジュールおよび VG224 モジュールと同様に、VG248 も確実な接続解除監視をサポートしています。

図 12-2 では、VG248 によって SMDI を使用する方法を示しています。

図 12-2　VG248 を介した SMDI



VG248 を介したボイスメール統合では、次の機能および利点が提供されます。

- Cisco Unified CallManager ごとに複数の SMDI リンク
- SMDI フェールオーバー機能
- ボイスメール システムのロケーションからの独立性

VG248 は、ボイスメール統合に使用されることのある他の 2 つのシリアル プロトコルもサポートできます。そのプロトコルとは、NEC Message Center Interface（MCI）および Ericsson MD110 専用プロトコルです。

FXS ポートを使用する場合の考慮事項

ボイスメール システムにアナログ FXS ポートが装備されている場合は、次の Cisco ゲートウェイを使用してボイスメール システムと統合します。

- WS-X6624

  Catalyst 6500 シャーシ内にこのモジュールに使用できるスロットがある場合は、このモジュールを使用します。

- VG224

  Catalyst 6500 シャーシの物理スロットが使用できない場合、およびシリアル ポートの自動フェールオーバーが不要と思われる場合は、このゲートウェイを使用します。

- VG248

  シリアル ポートおよび音声ポートに完全なフェールオーバーが必要な場合、SMDI 以外のシリアル プロトコル（たとえば、NEC MCI や Ericsson MD110）が必要な場合、または Catalyst 6500 シャーシのスロットが使用できない場合は、このゲートウェイを使用します。

Digital Set Emulation

Digital Set Emulation（DSE）は、PBX をボイスメール システムに統合するもう 1 つの方法です。このモードでは、ボイスメール ポートが PBX にとって専用デジタル受話器のように見えます。この統合方法は、アナログ FXS ポートを備えた SMDI を使用する場合よりも次の点で優れています。

- 音声パスとコール情報のシグナリングの両方で、回線が完全にデジタルである。
- 音声とシグナリングの両方が同じ物理回線を介して転送されるため、アウトバンド シグナリングがない。
- 一般に、コールの全体的な品質が高い。

Digital PBX Adapter（DPA）

シスコは、特に、Digital Set Emulation を介して Cisco Unified CallManager をサードパーティ製のボイスメール システムと統合するために、Digital PBX Adapter（DPA）を開発しました。DPA は、基本的に、一方の側で IP 接続を持ちながら、もう一方の側で複数のデジタル PBX 内線として機能します。DPA を使用すると、既存のボイスメール システムとそのインターフェイスを保持しながら、Cisco Unified CallManager に接続できます。

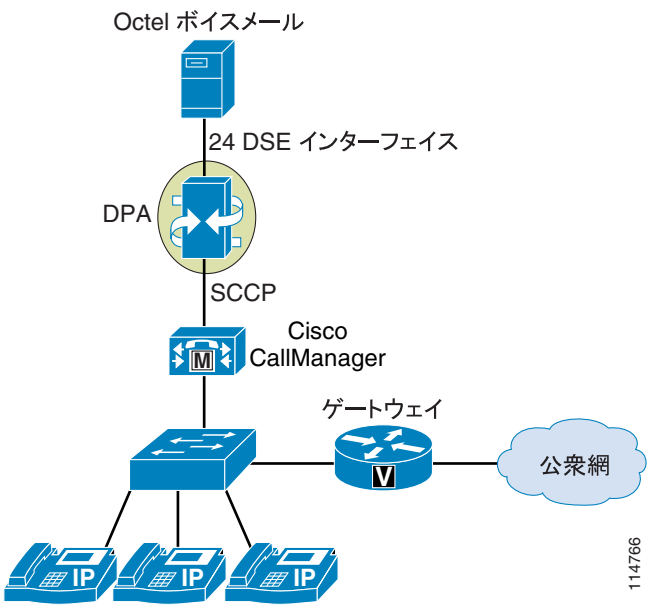
これら 2 種類の DPA があります。

- Avaya Definity G3 7400 シリーズのデジタル電話セットをエミュレートするための DPA 7630
- Nortel Meridian 1 2616 デジタル電話セットをエミュレートするための DPA 7610

（注） DPA は、Lucent/Avaya または Nortel の Digital Set Emulation を使用する場合に限り、Octel Aria 250/350 または Serenade 200/300 のボイスメール システムと連携します。

図 12-3 では、Octel ボイスメール システムを Cisco Unified CallManager と統合している DPA を示しています。

図 12-3　Octel ボイスメールを Cisco Unified CallManager と統合している DPA



二重 PBX 統合

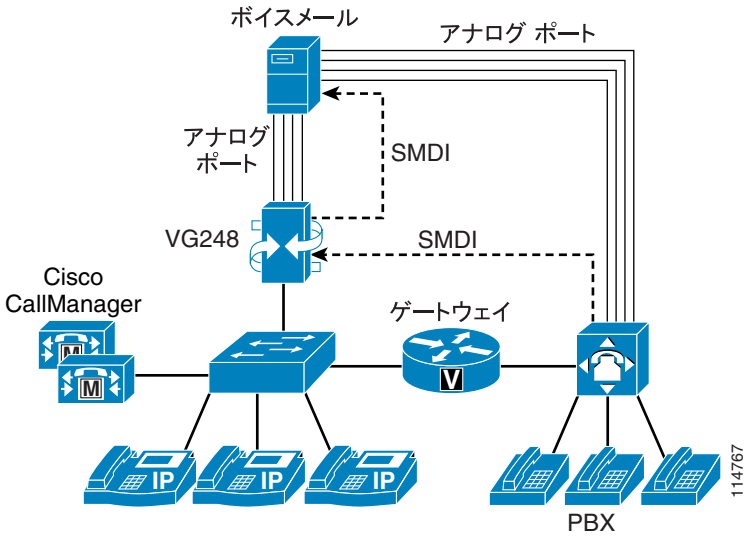
二重 PBX 統合は、既存のボイスメール サービスを保持しながら、現在の PBX から IP テレフォニーに移行する企業にとって便利なオプションです。

(注)

このシナリオは複雑であるため、ほとんどのボイスメール　ベンダーはこのシナリオをサポートしていませんが、必要に応じて「サイト固有に」サポートするベンダーもあります。このソリューションを実装するには、事前にボイスメール ベンダーに問い合せてください。

Cisco VG248 には、二重統合を提供できるようにする固有の多重化機能が備わっています。VG248 は、既存のシリアル リンクからの情報を独自のリンクと結合してから、単一のシリアル ストリームをボイスメール システムに提供できます（図 12-4 を参照）。

図 12-4　VG248 と SMDI を介した二重統合

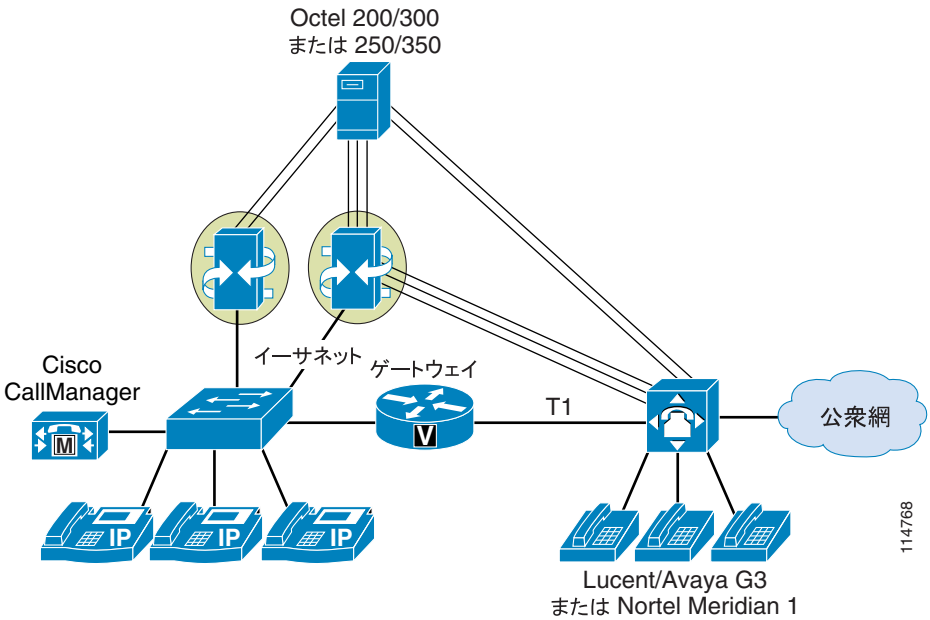


VG248 は、SMDI 機能とアナログ FXS ポートを備えた任意のボイスメール システムと連携します。二重統合が必要である場合は、実装する前に次の前提条件が必要となります。

- 統一されたダイヤル プラン
- 転送および再接続のシーケンス
- PBX と Cisco Unified CallManager の間の接続

図 12-5 に示しているように、Cisco DPA にも Digital Set Emulation を介して二重統合を実現する機能が備わっています。

図 12-5　DPA を介した二重統合



DPA は、Octel の Digital Set Emulation と連携します。二重統合が必要である場合は、実装する前に次の前提条件が必要となります。

- 統一されたダイヤル プラン
- 転送および再接続のシーケンス
- PBX と Cisco Unified CallManager の間の接続

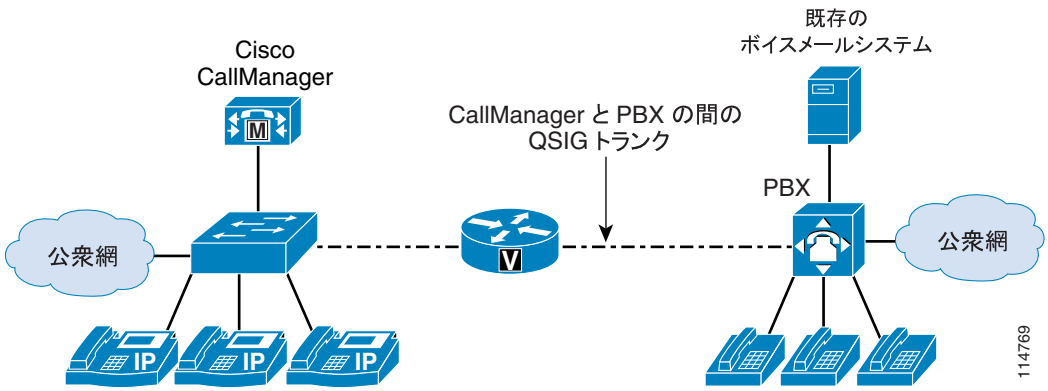
集中型ボイスメール

集中型ボイスメール配置では、複数の PBX が単一のボイスメール システムを共有します。この共有は、ボイスメール システムを 1 つの PBX だけに統合してから、PBX 間のプライベート ネットワーキング プロトコルを利用して、ボイスメール サービスをリモート加入者まで拡張することによって実現されます。ネットワーク接続された PBX は、ボイスメール システムにとって、1 つの大規模な PBX のように見え、そのように機能します。さまざまな PBX 製造業者が、大規模なネットワーク全体の加入者に対する機能透過性を実現しながらそのようなサービスの提供を可能にする専用プロトコル（たとえば、Avaya DCS、Nortel MCDN、Siemens CorNet、Alcatel ABC、NEC CCIS、Fujitsu FIPN）を開発しました。

集中型ボイスメール システムを使用するための主な動機付けは、既存のボイスメール システムから IP テレフォニー加入者にボイスメール サービスを提供することで、加入者が新しい Telephony User Interface（TUI; 電話ユーザ インターフェイス）を学習する必要がないようにするという目的から来ています。

一部のボイスメール システムは、Simple Messaging Desktop Interface（SMDI）などのプロトコルを介して複数の PBX をサポートできます（二重 PBX 統合）。Cisco Digital PBX Adapter（DPA）など、二重統合を可能にする他のソリューションも導入されています。状況によっては、ボイスメール ベンダーがこの構成をサポートしないと決めたため、このようなソリューションを実現できないことがあります。また、ボイスメール システムが、異なる PBX 統合を同時にサポートできないため、二重統合が単に技術的に不可能な場合もあります。そのような場合は、集中型ボイスメール配置が、二重統合に代わるソリューションを提供します（図 12-6 を参照）。

図 12-6　Cisco Unified CallManager と QSIG による集中型ボイスメール



既存のボイスメール システムを使用する場合は、そのシステムの製造業者およびモデルを考慮します。対象のボイスメール システムの製造業者が PBX システムの製造業者と同じ場合、通常は完全なボイスメール機能が Cisco Unified CallManager サブスクライバで利用できます。Nortel システムの例については図 12-7 を参照し、Avaya システムについては図 12-8 を参照してください。

図 12-7　Meridian Mail または CallPilot による Nortel M1 の集中型ボイスメール

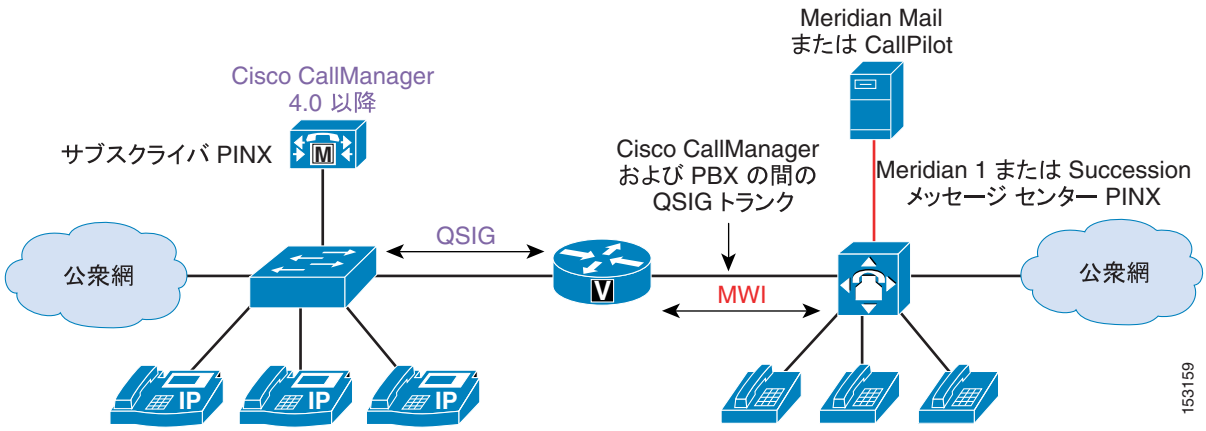


図 12-7 のシステムには、次の特性があります。

- ボイスメール サービスはすべてのサブスクライバで利用可能である。
- ボイスメールはメッセージ センター PINX でホスティングされる。
- QSIG MWI は Meridian Mail または CallPilot のみと連携する。

図 12-8　Intuity Audix による Avaya G3 の集中型ボイスメール

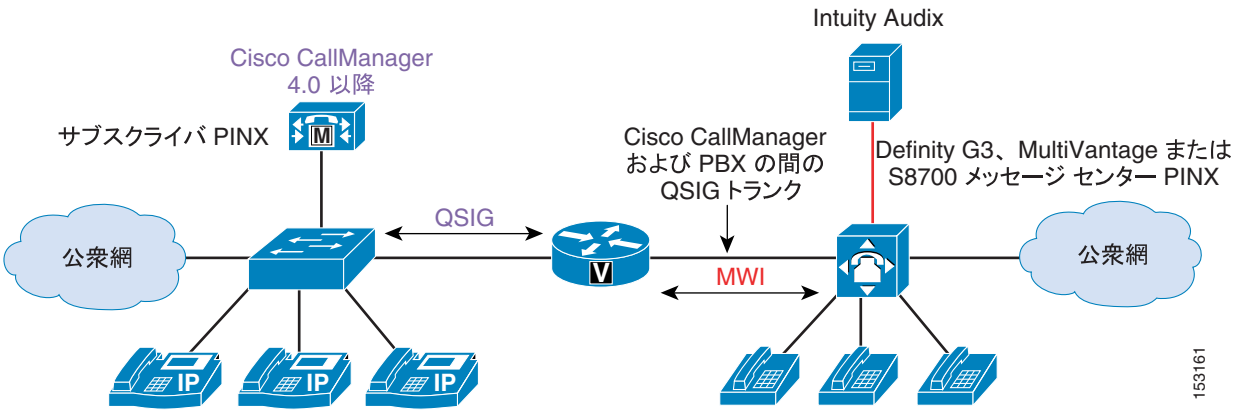


図 12-8 のシステムには、次の特性があります。

- ボイスメール サービスはすべてのサブスクライバで利用可能である。
- ボイスメールはメッセージ センター PINX でホスティングされる。
- QSIG MWI は Avaya Intuity Audix のみと連携する。

ボイスメール システムの製造業者が PBX システムの製造業者とは異なる場合、一部の機能が QSIG トランク経由で Cisco Unified CallManager に渡されないことがあります。この例では、Cisco Unified CallManager に MWI を直接提供するために特に Cisco Digital PBX Adapter（DPA）を使用できます。Nortel システムの例については図 12-9 を参照してください。Avaya システムについては図 12-10 を参照してください。

図 12-9　Octel Aria または Serenade による Nortel M1 の集中型ボイスメール

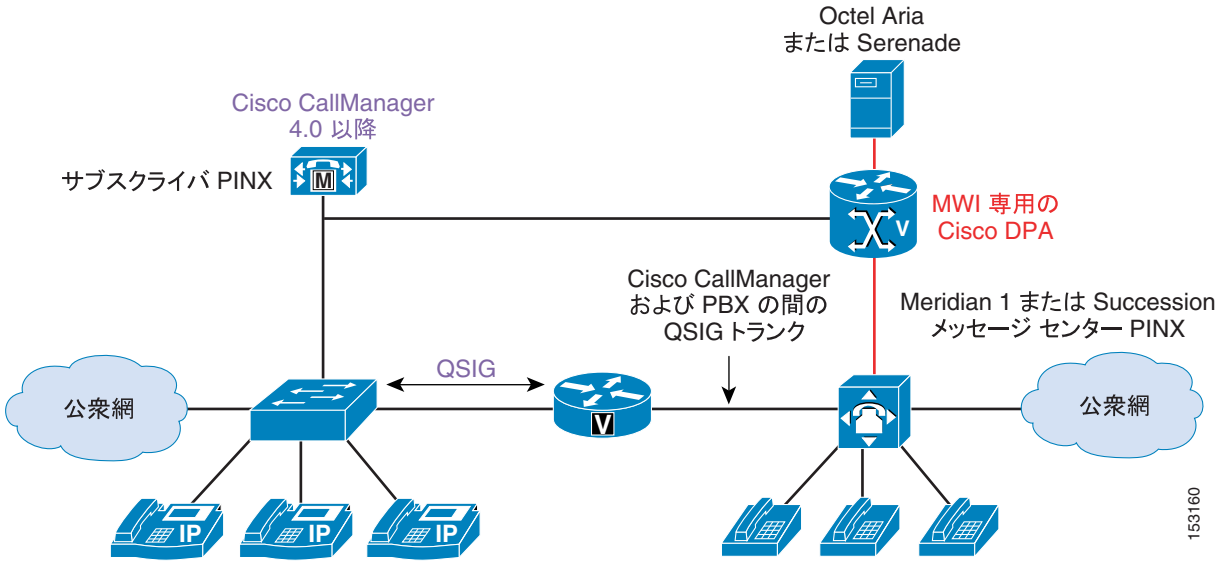


図 12-9 のシステムには、次の特性があります。

- ボイスメール サービスはすべてのサブスクライバで利用可能である。
- ステーションで呼び出したメッセージ センター機能は QSIG MWI にマッピングされない。
- Cisco DPA は Cisco Unified CallManager に対する MWI のみに使用される。

図 12-10　Octel Aria または Serenade による Avaya G3 の集中型ボイスメール

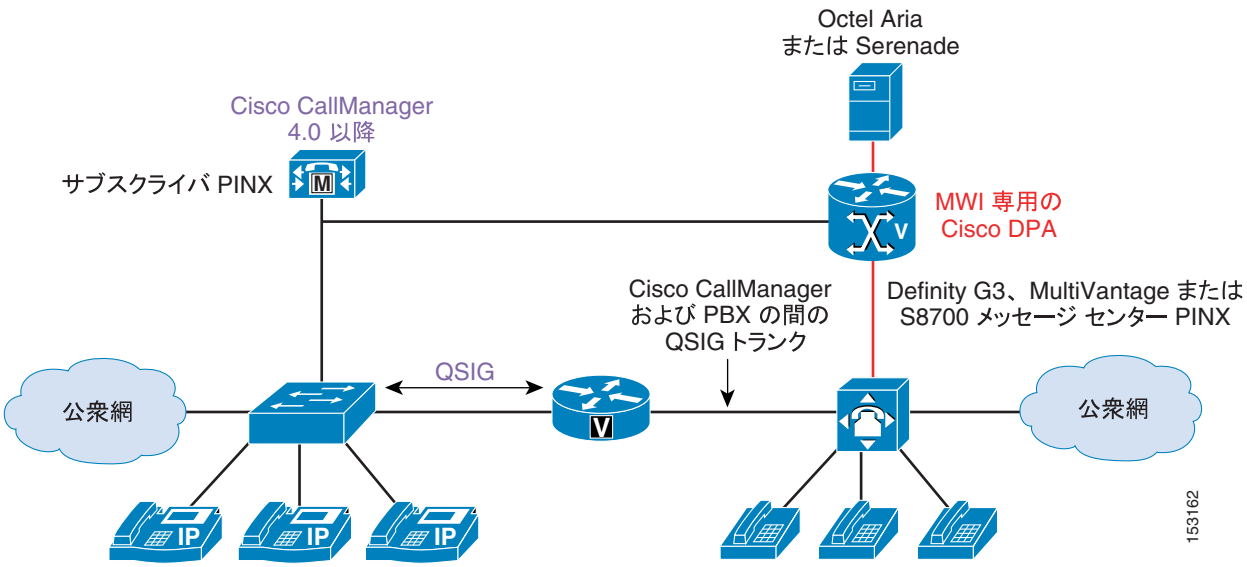


図 12-10 のシステムには、次の特性があります。

- ボイスメール サービスはすべてのサブスクライバで利用可能である。
- Leave Word Calling（LWC）は QSIG MWI にマッピングされない。
- Cisco DPA は Cisco Unified CallManager に対する MWI のみに使用される。

「集中型ボイスメール」という用語は、ボイスメール システム自体を意味しているのではないことに注意してください。集中型ボイスメールは、ボイスメール機能の提供に必要な、PBX の PBX 間ネットワーキング プロトコル（Avaya DCS、Nortel MCDN、Siemens CorNet などの専用プロトコル、または QSIG や DPNSS などの規格ベース プロトコル）の機能です。

集中型ボイスメールには、次の重要な用語および概念が適用されます。

- メッセージ センター Private Integrated Services Network Exchange（PINX）：これは、ボイスメール システムを「ホスティング」する PBX です（ボイスメール システムに直接接続されている PBX）。
- サブスクライバ PINX：これは、ボイスメール システムから「リモート」である PBX です（ボイスメール システムに直接接続されていない PBX）。

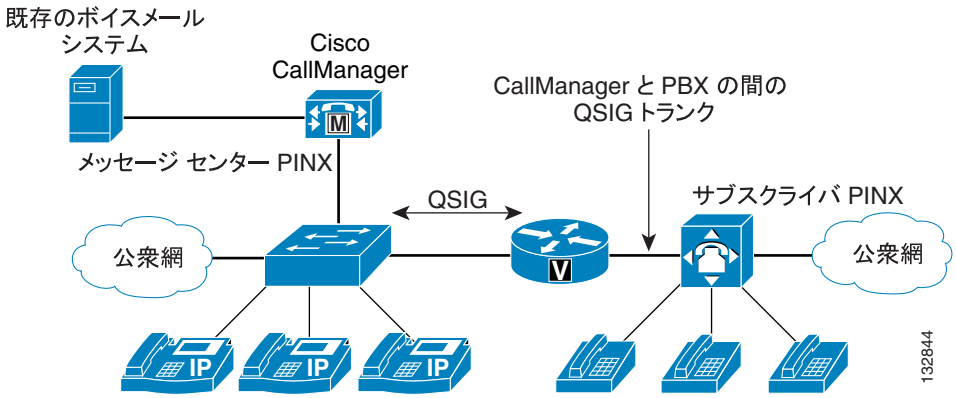
集中型ボイスメール構成では、QSIG などの適切な PBX 間ネットワーキング プロトコルが必要です。このプロトコルは、次のような最小限の機能サポートも提供する必要があります。

- メッセージ待機表示（MWI）
- 転送：正しい発信者 ID と着信者 ID がボイスメール システムに送信されることを保証するために必要です。
- 宛先変更：正しい発信者 ID と着信者 ID がボイスメール システムに送信されることを保証するために必要です。

ボイスメール システムがどのように使用されるかに応じて、他の機能が必要になる場合もあります。たとえば、ボイスメール システムが自動応答機能も提供する場合は、ヘアピンコールを防ぐために、パス置換機能が必要となります。

すべての PBX がメッセージ センター PINX として機能できるわけではありません。PBX がメッセージ センター PINX として機能できない場合は、ボイスメール システムを Cisco Unified CallManager の方に移動して、Cisco Unified CallManager をメッセージ センター PINX として機能させ、PBX をサブスクライバ PINX として機能させることを検討します（図 12-11 を参照）。

図 12-11　Cisco Unified CallManager がメッセージ センター PINX として機能する集中型ボイスメール



サポート

シスコは、他のベンダーの製品が特定の方法で動作することを保証できません。また、他のベンダーの製品に対する設定変更またはアップグレードに関して、何が必要であるかを指示できません。各製品のサプライヤやベンダーに直接質問をしたり確認を求めたりするのは、お客様の責任です。

シスコは、お客様がサプライヤやベンダーに尋ねるべき質問を決める際に、お役に立つことができます。たとえば、「QSIG を介して接続されるリモート PBX ユーザが、メールボックスを持ち、かつすべてのボイスメール機能（MWI など）にフル アクセスできるようにするには、PBX に対して何を行う必要がありますか」などの質問です。

PBX の相互運用性を支援するために、シスコはさまざまな PBX を Cisco Unified CallManager とテストし、これらのテストをアプリケーション ノートという形で文書化しています。これらの文書は、成功を保証するものではありませんが、サポートされている機能および Cisco Unified CallManager と PBX の両方の設定詳細に関して、ある程度のガイダンスを提供します。主な PBX に関して Cisco Unified CallManager のアプリケーション ノートがすでに記述されており、その中で Cisco Unified CallManager がメッセージ センター PINX として機能する集中型ボイスメールのシナリオが扱われています。アプリケーション ノートは、次の Web サイトで入手できます。

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

（注） シスコは、メッセージ センター PINX として機能する他のベンダーの PBX をテストすることはできません。シスコには、このようなシステムを構成するファシリティも専門知識もありません。したがって、お客様がこれらの情報をサプライヤやベンダーに直接要求する必要があります。

要約

- 集中型ボイスメールは、ボイスメール システム自体ではなく、PBX 間ネットワーキング プロトコルの機能である。
- すべての PBX がメッセージ センター PINX として機能できるわけではない。お客様が PBX のサプライヤやベンダーにこの機能を確認する必要があります。シスコは、PBX のこの機能を提供することもサポートすることもできません。
- Cisco Unified CallManager はメッセージ センター PINX として機能できるため、PBX がこの機能を実行できない場合、お客様に代替を提供できる。
- パス置換が必要であるかを確認する必要がある。Cisco Unified CallManager Release 4.1 以降は、この機能をサポートしています。

確実な接続解除監視

確実な接続解除監視は、遠端のデバイスがオンフックになったことを示すために PBX ポートからボイスメール システムに送信される信号です。この信号は、通常、約 600 ms のループ電流切断という形を取ることによって、ボイスメール システムにセッションを終了させます。

この信号がないと、ボイスメール システムは遠端のデバイスがオンフックになったことを認識せず、この状況で PBX が提供するどのような監視トーンでも録音し続けます（たとえば、ダイヤルトーンを再生する PBX も、ビジー トーンを再生する PBX もあります）。ボイスメール システムは、メッセージの最大時間に達するまで、このようなトーンを録音し続けます（たとえば、メールボックスでメッセージごとの制限が 3 分であり、発信者が 30 秒後に電話を切った場合、確実な接続解除監視がないと、ボイスメール システムはその後 2 分 30 秒間このようなトーンを録音し続けます）。この不必要な録音によって、加入者がいらいらすることがあります。また、ディスク使用率が上がり、ポート使用時間が増えるため、システムのパフォーマンスが低下することもあります。ボイスメール システムの中には、既知のトーンを監視して、その後削除することにより、このシナリオに対処できるものもありますが、その場合でもシステム パフォーマンスへの影響は避けられません。

加入者がメールボックスにコールしてメッセージがないか調べる場合にも、同様の問題が発生します。接続解除監視がない場合にユーザが単に電話を切ると、ボイスメール システムは、アクティビティ タイマーが期限切れになるまで、セッションを終了させずに有効な応答を待ち続けます。このシナリオの場合、主な影響は追加のポート使用時間が発生することからもたらされます。

これらの理由から、ボイスメール システムに接続されているアナログ ポートが、確実な接続解除監視を提供する必要があります。

サードパーティ製ボイスメール統合の要約

ボイスメール システムを Cisco Unified CallManager に接続する方法は他にもありますが（SMDI と併用する Microsoft TAPI および PRI ISDN トランクなど）、これらの方法は一般的ではありません。サードパーティ製ボイスメール統合の大部分は、Cisco VG248 または Digital PBX Adapter（DPA）を使用するため、これらがお勧めのソリューションです。

Cisco Unified CallManager をボイスメール システムに統合する方法は、ボイスメール システムが現在どのように PBX に統合されているかによって異なります。現在アナログ ポートが使用されている場合、Cisco VG248 または VG224 は優れた統合方法を提供します。ただし、Avaya または Nortel の Digital Set Emulation が使用されている場合は、Cisco DPA を導入すると、現在のボイスメール システムをアナログ FXS ポート用に設計し直さずに統合を行うことができるため、低コストでソリューションを実現できます。

（注） シスコは、サードパーティ製のボイスメール システムのテストおよび認定を行いません。一般に、業界では、このような製品をさまざまな PBX システムに対してテストしたり認定したりするのは、ボイスメール ベンダーの責任であると考えられています。もちろん、シスコは、接続されるサードパーティ製のボイスメール システムに関係なく、PBX システムに対してシスコのインターフェイスをテストし、そのインターフェイスをサポートします。

CHAPTER 13

Cisco Unity

この章では、Cisco Unity および Cisco Unity Connection と Cisco Unified CallManager の統合について、設計上の側面を中心に説明します。この章で扱う設計に関するトピックは、ボイスメール設定とユニファイド メッセージング設定の両方に適用されます。

さらに、この章では、Microsoft Exchange 2000 または 2003 メッセージ ストアあるいは Lotus Notes Domino メッセージ ストアおよび Microsoft Windows 2000 または 2003 と共に Cisco Unity を配置する場合の設計上の問題についても説明します。この章では、Microsoft NT 4.0 や Exchange 5.5 による配置、および Microsoft NT 4.0 や Exchange 5.5 からのアップグレードは扱いません。Cisco Unity Connection は外部メッセージ ストアに依存しません。

シスコ以外のメッセージング システムとの統合など、Cisco Unity と Unity Connection に関するその他の設計情報については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』を参照してください。

http://www.cisco.com

この章では、Cisco Unity と Unity Connection の設計に関する次のトピックについて取り上げます。

- メッセージング配置モデル（P.13-3）
- メッセージング システム インフラストラクチャ コンポーネント（P.13-6）
- ポート グループ（分離統合）（P.13-7）
- 帯域幅の管理（P.13-8）
- Cisco Unity および Unity Connection のネイティブ トランスコーディング動作（P.13-10）
- ボイスメール統合のための Cisco Unified CallManager SIP トランクの設定（P.13-11）
- Cisco Unified CallManager クラスタとの音声ポート統合（P.13-12）
- 専用 Cisco Unified CallManager バックアップ サーバを使用する音声ポート統合（P.13-14）
- 集中型メッセージングと集中型コール処理（P.13-15）
- 分散型メッセージングと集中型コール処理（P.13-17）
- 結合されたメッセージング配置モデル（P.13-19）
- 集中型メッセージングと WAN を介したクラスタ化（P.13-21）
- 分散型メッセージングと WAN を介したクラスタ化（P.13-23）
- Cisco Unity メッセージング フェールオーバー（P.13-25）
- Cisco Unity フェールオーバーと WAN を介したクラスタ化（P.13-26）
- 集中型メッセージングと複数の Cisco Unified CallManager サーバ（P.13-27）

Cisco Unified CallManager Release 4.0 では、回線グループ、ハント リスト、およびハント パイロットが導入されています。これらは、既存の音声ポートの動作に影響を及ぼすことができます。Release 4.0 以前のバージョンの Cisco Unified CallManager を Cisco Unified CallManager Release 5.0 以降にアップグレードする前に、次の Web サイトで入手可能な 5.*x* リリース用の『*Cisco Unified CallManager Administration Guide*』を参照してください。

http://www.cisco.com

この章で説明する配置モデルおよび設計上の考慮事項はすべて、Cisco Unified CallManager Release 5.0 以降によって完全にサポートされています。

Cisco Unified CallManager 5.0 には、SIP トランクの新機能も追加されています。SIP トランクで Cisco Unity および Unity Connection との統合が直接サポートされ、SIP プロキシ サーバの必要性がなくなりました。

メッセージング配置モデル

Cisco Unity は、次の 3 つの主なメッセージング配置モデルをサポートしています。

- 単一サイト メッセージング（P.13-3）
- 集中型メッセージング（P.13-3）を使用したマルチサイト WAN 配置
- 分散型メッセージング（P.13-4）を使用したマルチサイト WAN 配置

Cisco Unity Connection は単一サイト メッセージング、および単一メッセージング サーバによる集中型メッセージングをサポートしています。

Cisco Unified CallManager と Cisco Unity または Unity Connection の両方を含む配置では、Cisco Unified CallManager に 1 つのコール処理モデルを使用し、Cisco Unity に 1 つのメッセージング モデルを使用します。メッセージング配置モデルは、配置されるコール処理モデルのタイプに依存しません。

3 つのメッセージング配置モデルに加えて、Cisco Unity はメッセージング フェールオーバーもサポートしています（P.13-4 の「メッセージング フェールオーバー」を参照）。Cisco Unity Connection は現在、フェールオーバーをサポートしていません。Cisco Unity Connection はサーバ間のネットワーキングのない単一サーバだけを使用するため、単一サイト モデルと集中型メッセージング モデルだけをサポートしています。

すべてのメッセージング配置モデルが、ボイスメールとユニファイド メッセージングの両方のインストールをサポートしています。Cisco Unity Connection はボイスメールだけをサポートしています。

単一サイト メッセージング

このモデルでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。サイトは、単一サイトである場合も、高速 Metropolitan Area Network（MAN; メトロポリタン エリア ネットワーク）を介して相互接続されたキャンパス サイトである場合もあります。メッセージング システムのクライアントもすべて、単一（またはキャンパス）サイトに置かれます。このモデルの際立った特徴は、リモート クライアントが存在しないことです。

集中型メッセージング

このモデルでは、単一サイト モデルと同様に、メッセージング システムとメッセージング インフラストラクチャ コンポーネントがすべて、同じサイトに置かれます。サイトは、1 つの物理的なサイトである場合も、高速 MAN を介して相互接続されたキャンパス サイトである場合もあります。ただし、単一サイト モデルとは異なり、集中型メッセージング クライアントをローカルとリモートの両方に置くことができます。

メッセージング クライアントはメッセージング システムに対してローカルでもリモートでもかまわないため、特別な設計上の考慮事項が、次の Graphical User Interface（GUI; グラフィカル ユーザ インターフェイス）クライアントに対して適用されます。そのクライアントとは、Microsoft Exchange を使用する ViewMail for Outlook（VMO）クライアント、Lotus Domino を使用する Domino Unified Communications Services（DUC）クライアント、および Telephone Record and Playback（TRaP; 電話での録音および再生）機能とメッセージ ストリーミング機能を使用するクライアントです。リモート クライアントは、TRaP を使用できません。また、リモート クライアントは、再生前にメッセージをダウンロードするように設定する必要があります。ローカル クライアントとリモート クライアントで機能や操作が異なるとユーザが混乱する恐れがあるため、クライアントがローカルであるかリモートであるかに関係なく、音声ポートで TRaP を無効にし、メッセージをダウンロードするように、および TRaP を使用しないように GUI クライアントを設定する必要があります。Cisco Unity Personal Assistant（CPCA）を介してアクセスされる Cisco Unity Inbox は、ローカル クライアントに

対してだけ許可される必要があります。Cisco Unity Telephone User Interface（TUI; 電話ユーザ インターフェイス）は、ローカル クライアントとリモート クライアントの両方に対して同様に動作します。

分散型メッセージング

分散型メッセージングでは、メッセージング システムとメッセージング インフラストラクチャ コンポーネントが分散方式で同じ場所に置かれます。複数のロケーションを持つことができ、各ロケーションに独自のメッセージング システムとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのクライアント アクセスが各メッセージング システムに対してローカルであり、メッセージング システムは、すべてのロケーションにまたがるメッセージング バックボーンを共有します。分散型メッセージング システムからのメッセージ送信は、ハブアンドスポーク タイプのメッセージ ルーティング インフラストラクチャによって、メッセージング バックボーンを介して行われます。WAN によって、メッセージング インフラストラクチャ コンポーネントを、サービス提供先のメッセージング システムから切り離すことはできません。分散型メッセージングは、基本的に、共通のメッセージング バックボーンを持つ複数の単一サイト メッセージング モデルです。

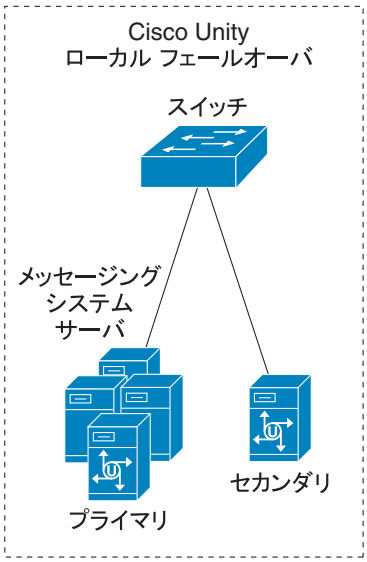
分散型メッセージング モデルは、ローカルおよびリモートの GUI クライアント、TRaP、およびメッセージのダウンロードに関して、集中型メッセージングと同じ設計基準を持っています。

Cisco Unity Connection は単一サーバだけをサポートしているため、メッセージング サーバの分散はできません。そのため、Cisco Unity Connection は分散型メッセージング モデルをサポートしません。

メッセージング フェールオーバー

3 つのメッセージング配置モデルはすべて、メッセージング フェールオーバーをサポートしています。図 13-1 に示しているように、ローカル メッセージング フェールオーバーを実装できます。ローカル フェールオーバーでは、プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が、アベイラビリティの高い同じ LAN 上の同じサイトに置かれます。この設計は Cisco Unity 専用で、Cisco Unity Connection は現在のところフェールオーバーをサポートしていません。

図 13-1　Cisco Unity メッセージングのローカル フェールオーバー



Cisco Unity および Cisco Unified CallManager は、メッセージング配置モデルとコール処理配置モデルの次の組み合せをサポートしています。Cisco Unity Connection は、分散型メッセージング モデル以外のすべての組み合せをサポートしています。

- 単一サイト メッセージングと単一サイト コール処理
- 集中型メッセージングと集中型コール処理
- 分散型メッセージングと集中型コール処理
- 集中型メッセージングと分散型コール処理
- 分散型メッセージングと分散型コール処理

サイト分類の詳細、およびメッセージング配置モデルとコール処理配置モデルのサポートされている組み合せの詳細な分析については、http://www.cisco.com で入手可能な Cisco Unity および Cisco Unity Connection の設計ガイドを参照してください。

メッセージング システム インフラストラクチャ コンポーネント

Cisco Unity は、Dynamic Domain Name Server（DDNS）、ディレクトリ サーバ、メッセージ ストアなど、さまざまなネットワーク リソースと対話します（図 13-2 を参照）。Cisco Unity はメッセージ ストアとして、Microsoft Exchange と IBM Lotus Notes の両方をサポートしています。これらのメッセージ ストア タイプはそれぞれ異なるインフラストラクチャ コンポーネントを持っています（http://www.cisco.com で入手可能な『*Cisco Unity Design Guide*』で該当する配置タイプを参照してください）。

Cisco Unity は、単一の一体型デバイスではなく、相互依存コンポーネントのシステムと見なす方が適しています。正常に動作するには、Cisco Unity メッセージング システムの各メッセージング システム インフラストラクチャ コンポーネントが必要であり、これらすべてのコンポーネントがアベイラビリティの高い同じ LAN 上に存在することが重要です（ほとんどの場合、これらのコンポーネントは物理的に同じ場所に置かれます）。これらのコンポーネント間に WAN リンクがある場合は、どのような WAN リンクでも、Cisco Unity の動作に影響を及ぼす遅延を引き起こす可能性があります。このような遅延は、TUI 操作中の長い遅延や無音期間となって表れます。詳細については、http://www.cisco.com から入手可能な『*Cisco Unity Design Guide*』の「*Network and Infrastructure Considerations*」の章を参照してください。

図 13-2　Cisco Unity メッセージング システム インフラストラクチャ コンポーネント（Exchange 固有）

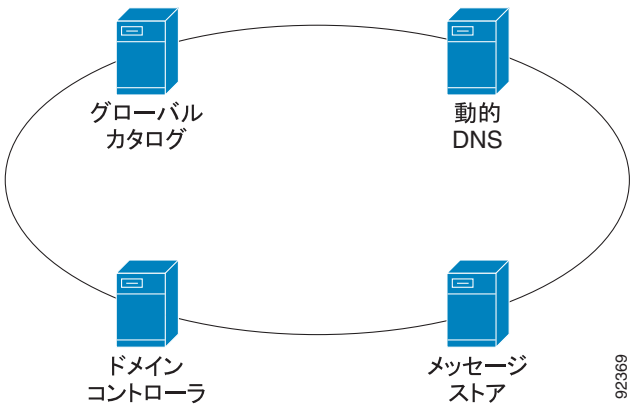


図 13-2 は、メッセージ システム インフラストラクチャ コンポーネントを論理的に表現したものです。これらのコンポーネントのいくつかは、同じサーバ上に置くことができます。Domino Lotus Notes の場合、メッセージ ストアとディレクトリ（Names.nsf）が同じサーバ上に置かれます。Microsoft Windows、グローバル カタログ サーバ、およびドメイン コントローラも同じサーバ上に置くことができます。メッセージ ストア クラスタリングの場合と同様に、Cisco Unity が Microsoft Exchange 2000 または 2003 および Lotus Domino に対してサポートする各コンポーネントの複数のインスタンスを使用することもできます。すべてのメッセージング システム インフラストラクチャ コンポーネントは、サービス提供先の Cisco Unity サーバと同じ、アベイラビリティの高い LAN 上に置く必要があります。

Cisco Unity Connection を配置するときは、Automatic Speech Recognition（ASR; 自動音声認識）サービスを別のサーバに置くことも可能です。この配置環境では、Cisco Unity Connection サーバと ASR サーバが同じロケーションに存在する必要があります。Cisco Unity Connection のインフラストラクチャ要件または依存関係は、Cisco Unity とは異なります。

ポート グループ（分離統合）

Unity Connection では、Cisco Unity 4.2 で*分離統合*とも呼ばれている、*ポート グループ*という概念が導入されています。Unity の初期のリリースでは、Cisco Unity Telephony Integration Manager（UTIM）で同じタイプの統合の*複数クラスタ*を設定できました。ポート グループと分離統合が、単一統合における複数のクラスタとどのように異なるかを理解することが重要です。単一統合で複数のクラスタという手法では、Unity データベースがユーザをクラスタではなく、統合と関連付けます。単一統合しかないため、すべてのサブスクライバはどのクラスタ上に存在するかに関係なく、その単一統合と関連付けられていました。Message Waiting Indication（MWI; メッセージ待機インジケータ）に対して、Unity は MWI アップデートを、サブスクライバが存在しないクラスタも含めて、単一統合におけるすべてのポートからブロードキャストする必要がありました。Unity（4.2）の分離統合、および Unity Connection のポート グループが新たに追加されたことで、サブスクライバは所属する特定の統合に関連付けられます。MWI 信号をすべてのポートからブロードキャストする必要がなくなり、特定のサブスクライバに関連付けられた特定のポートだけに送信されるようになりました。

従来型の電話システムと Cisco Unified CallManager 電話システムを統合したり、Cisco Unified CallManager SIP システムと Cisco Unified CallManager SCCP システムを統合したりするなど、複数のタイプのシステムを Unity または Unity Connection サーバに統合すると、二重統合が発生します。SCCP で 2 つ以上の Cisco Unified CallManager クラスタに統合する場合など、同じタイプの統合によって 4.1 以前のバージョンの Cisco Unity を複数の Cisco Unified CallManager クラスタに統合すると、複数統合が発生します。

Unity 4.2 では、分離統合は UTIM で設定されるのに対して、Unity Connection ポート グループはシステム管理者が設定します。

帯域幅の管理

Cisco Unified CallManager は、帯域幅を管理するためのさまざまな機能を備えています。リージョン、ロケーション、およびゲートキーパーさえも使用して、Cisco Unified CallManager は、WAN リンクを介して伝送される音声コールの数によって既存の帯域幅がオーバーサブスクリプションの状態になることがなく、音声品質が低下しないことを保証できます。Cisco Unity および Unity Connection は、帯域幅の管理とコールのルーティングを Cisco Unified CallManager に依存しています。コール（音声ポート）が WAN リンクを通過することのある環境に Cisco Unity または Unity Connection を配置する場合、このようなコールはゲートキーパーベースのコール アドミッション制御にとって透過的になります。このような状況は、Cisco Unity または Unity Connection サーバが分散クライアントにサービスを提供している場合（分散型メッセージング（Unity のみ）または分散型コール処理）、または Cisco Unified CallManager がリモートに置かれている場合（分散型メッセージング（Unity のみ）または集中型コール処理）、いつでも発生します。Cisco Unified CallManager は、コール アドミッション制御用のリージョンとロケーションを提供します。

図 13-3 では、集中型メッセージングと集中型コール処理を使用する小規模なサイトで、リージョンとロケーションを連携させて使用可能な帯域幅を管理する方法を示しています。リージョンとロケーションの詳細については、P.9-1 の「コール アドミッション制御」の章を参照してください。

図 13-3　ロケーションとリージョン

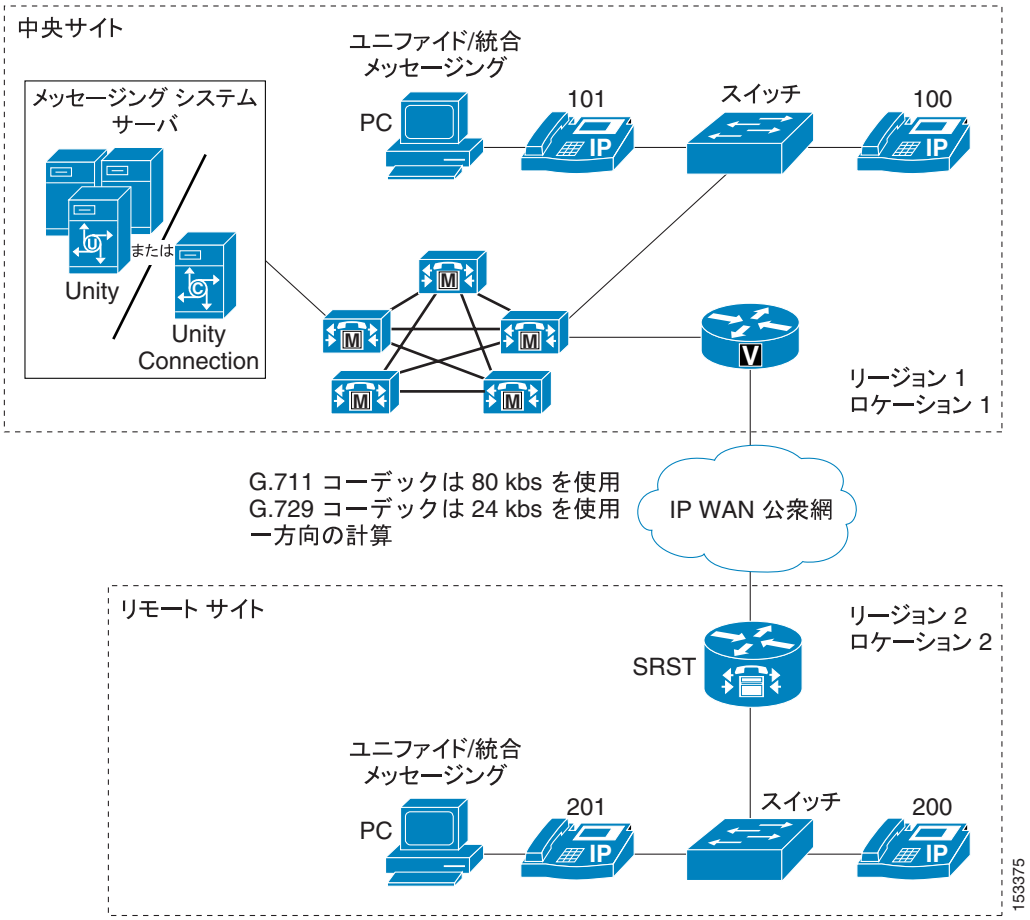


図 13-3 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。ロケーション 1 と 2 は、両方 24 kbps に設定されています。ロケーションの帯域幅は、ロケーション間コールの場合にだけ配分されます。

リージョン内（G.711）コールは、ロケーションの使用可能な帯域幅に対して配分されません。たとえば、内線番号 100 が内線番号 101 をコールする場合、このコールはロケーション 1 の使用可能帯域幅 24 kbps に対して配分されません。ただし、G.729 を使用するリージョン間コールは、ロケーション 1 とロケーション 2 の両方の帯域幅割り当て 24 kbps に対して配分されます。たとえば、内線番号 100 が内線番号 200 をコールすると、このコールは接続されますが、追加の（同時）リージョン間コールでは、リオーダー（ビジー）トーンが聞こえます。

AAR によってルーティングされるボイスメール コールで RDNIS が送信されないことによる影響

Cisco Unified CallManager の機能である Automated Alternate Routing（AAR; 自動代替ルーティング）では、WAN がオーバーサブスクリプションの状態になった場合に、公衆網を介してコールをルーティングできます。ただし、公衆網を介してコールが再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。Cisco Unity または Unity Connection がメッセージング クライアントに対してリモートである場合は、正しくない RDNIS 情報によって、AAR が外線を介して再ルーティングするボイスメール コールに影響が及ぼされることがあります。RDNIS 情報が正しくない場合、コール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、自動アテンダント プロンプトを受信します。発信者は、到達を試みているユーザ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。オーバーサブスクリプションの状態になった WAN に対して AAR を使用する代わりの方法は、単に、オーバーサブスクリプションの状況で発信者にリオーダー トーンが聞こえるようにすることです。

Cisco Unity および Unity Connection のネイティブ トランスコーディング動作

デフォルトでは、Cisco Unity または Unity Connection サーバは自動的にトランスコーディングを実行します。現在、Cisco Unified CallManager および Cisco Unity は、Skinny Client Control Protocol（SCCP）TAPI Service Provider（TSP）音声ポートに対して G.729 と G.711 だけをサポートしています。他のコーデックは、Intel または Dialogic の音声ボードを使用する従来型の統合でサポートされています。Cisco Unity のネイティブ トランスコーディングは、外部ハードウェア トランスコーダを使用せず、サーバのメイン CPU を使用します。SCCP 統合の場合に限り、Cisco Unified CallManager がハードウェア トランスコーダを音声ポート コールに割り当てるようにするには、レジストリ設定によって、Cisco Unity サーバ上でネイティブ トランスコーディングを無効（オフ）にする必要があります。このレジストリ設定は「Audio - Enable G.729a codec support」と呼ばれます。これを設定するためのツールは、http://www.CiscoUnityTools.com で入手可能な *Advanced Settings Tool* です（この項の最後で説明するように、Cisco Unity Connection のネイティブ トランスコーディングを無効にするには、メッセージング コーデックの設定を別に行います）。

デフォルトでは、コーデック レジストリ キーが存在しないため、ネイティブ トランスコーディングは有効（オン）です。Advanced Settings Tool により、使用可能な 2 つのコーデックのうちのどちらか 1 つを選択できる新しいレジストリ キーが追加されます。その後、Cisco Unity は、1 つのコーデックだけをサポートすることを Cisco Unified CallManager に「アドバタイズ」します。音声ポートを終端または起点とするコールが、Cisco Unity サーバに設定されているタイプと異なるコーデックを使用している場合、Cisco Unified CallManager はそのコールに外部トランスコーディング リソースを割り当てます。Cisco Unified CallManager 上でトランスコーディング リソースを設定する方法の詳細については、P.6-1 の「メディア リソース」の章を参照してください。

Advanced Settings Tool を使用して 1 つのコーデックだけを有効にする場合は、Cisco Unity サーバのシステム プロンプトが、使用されるコーデックと同じである必要があります。デフォルトでは、システム プロンプトは G.711 です。コーデックが G.711 に設定されている場合、システム プロンプトは正常に機能します。ただし、G.729 が選択されている場合は、システム プロンプトを変更する必要があります。システム プロンプトを変更する方法の詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Administration Guide*』を参照してください。システム プロンプトが、レジストリで選択されているコーデックと同じでない場合は、エンド ユーザに、理解不能なシステム プロンプトが聞こえます。

SIP で統合するときに Unity のネイティブ トランスコーディングを無効にする方法の詳細については、http://www.cisco.com で入手可能な Unity 製品のマニュアルを参照してください。

Cisco Unity Connection がサポートするコーデックをアドバタイズする方法を変更するには、Cisco Unity とは異なる設定を行います。Cisco Unity Tools Depot は使用せず、設定変更は Cisco Unity Connection Administration ページで行います。Telephony Integrations の Port Groups リンクを選択します。Port Groups ページで、アドバタイズの設定を G.711 のみ、G.729 のみ、またはその両方に変更しますが、G.711 または G.729 のどちらかに設定するようにしてください。このように設定にすると、Cisco Unity Connection は両方のプロトコル（ネイティブ トランスコーディング）をサポートするものの、指定された一方のみの使用が適していることをアドバタイズします。ネイティブ トランスコーディングが無効の状態では、トランスコーダ リソースが必要な場合に、Unity または Unity Connection サーバの CPU を使用する代わりに、Cisco Unified CallManager がリソースを提供します。

ボイスメール統合のための Cisco Unified CallManager SIP トランクの設定

Cisco Unified CallManager 5.0 では、回線側デバイスの SIP をサポートする新機能が導入され、トランク側の SIP も拡張されました。このような機能により、Cisco Unified CallManager は SIP で直接 Cisco Unity および Unity Connection と統合できるようになり、SIP プロキシ サーバが必要なくなりました。

ただし、Cisco Unified CallManager は SIP トランクを介したボイスメールの直接統合が可能ですが、Skinny Client Control Protocol（SCCP）ポートと同じ Voicemail Port Wizard を持っていません。ある程度の手動設定が必要です。基本的な統合シナリオでは、SIP トランクの設定に次の手順が必要です。

ステップ 1　Cisco Unified CallManager Administration で SIP Profile を作成します。それには、**Device** > **Device Setting** > **SIP Profile** の順に選択します。

このとき、ボイスメール統合に固有のものは特にありませんが、管理機能を簡単にし、一貫したものにするため、実際のボイスメール統合に固有の SIP プロファイルを作成し、それに応じた名前を付けるようにしてください。

ステップ 2　CallManager Administration で SIP Trunk Security Profile を作成します。それには、**System** > **Security Profile** > **SIP Trunk Security Profile** の順に選択します。

SIP Trunk Security Profile の **Incoming Port #** はボイスメールに固有のもので、Cisco Unity または Unity Connection サーバが Cisco Unified CallManager クラスタへの接続に使用する SIP ポート番号の数値です。また、**Accept Unsolicited Notifications** をオン（有効）にし、Cisco Unity および Unity Connection が Cisco Unified CallManager of Message Waiting Indicator（MWI）イベントを通知できるようにします。

（注）　MWI 機能は Unsolicited Notifies で処理されます。SCCP 統合に必要な MWI DN を設定する必要はありません。

ステップ 3　CallManager Administration で SIP Trunk を作成します。それには、**Device** > **Trunk [Add New]** の順に選択します。トランクの作成ページで、設定済みの SIP Profile と SIP Trunk Security Profile を対応するフィールドに指定します。また、Unity または Unity Connection サーバの宛先アドレスを設定し、**Unattended Port** をオンに（有効に）します。**Redirecting Number IE Deliver - Outbound** もオンに（有効に）します。

（注）　Unattended Port の例外として、複数の Cisco Unity サーバを 1 つの Cisco Unified CallManager クラスタに接続し（たとえば、72 を超えるボイスメール ポートが配置されたため、2 つ以上の Cisco Unity サーバが必要な場合）、ライブ応答またはクロスサーバ ログオンが設定されている場合があります。このシナリオでは、Unattended Port をオフ（無効）のままにすると、あるサーバのボイスメール ポートからのコール転送が、他のサーバで終端されるようにできます。現在のところ、この例外は Unity だけに適用されます。

ステップ 4　ルート パターンを作成し、ボイスメール SIP トランクを宛先として指定します。

ステップ 5　ステップ 4 で設定したルートパターンと同じ番号のボイスメール パイロット番号を作成します。

ステップ 6　対応するボイスメール パイロット番号を使用して、ボイスメール プロファイルを作成します。

Cisco Unified CallManager クラスタとの音声ポート統合

単一サイト メッセージング環境に Cisco Unity を配置する場合、Cisco Unified CallManager クラスタとの統合は SCCP 音声ポートまたは SIP ポートを介して行われます。Cisco Unified CallManager サブスクライバに障害が発生した場合でも（Cisco Unified CallManager フェールオーバー）、ユーザおよび外部コールが引き続き音声メッセージングにアクセスできるように、設計上の考慮事項には、Cisco CallManager サブスクライバ間の音声ポートの適切な配置が含まれる必要があります（図 13-4 を参照）。

図 13-4　Cisco Unified CallManager クラスタと統合された Cisco Unity サーバ（専用バックアップ サーバなし）

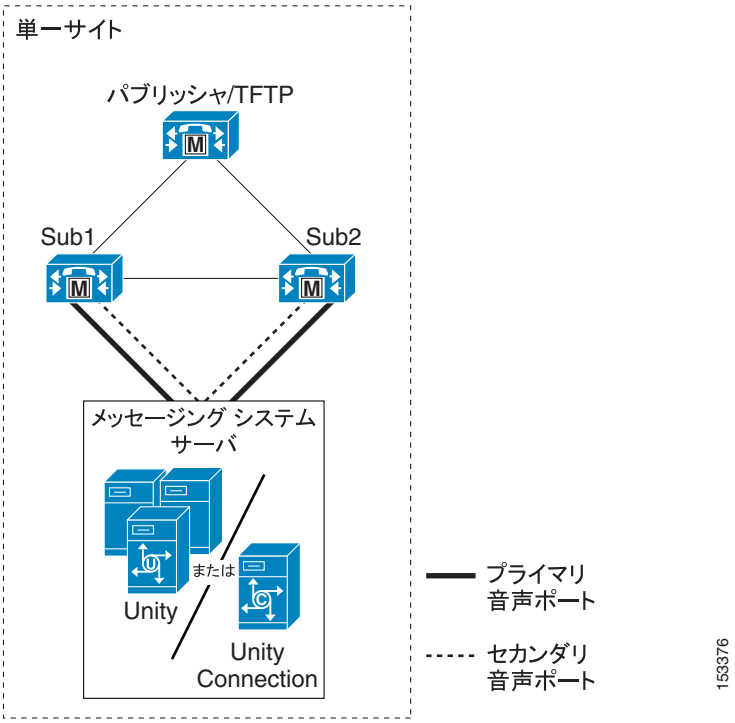


図 13-4 の Cisco Unified CallManager クラスタは、1 対 1 のサーバ冗長性および 50/50 のロード バランシングを採用しています。正常な動作時には、各サブスクライバ サーバがアクティブで、サーバの全コール処理負荷の最大 50% を処理します。1 台のサブスクライバ サーバに障害が発生すると、残りのサブスクライバ サーバが、障害の発生したサーバの負荷を担います。

この設定では、ボイスメール ポートのグループが 2 つ使用され、各グループに、ライセンスのある音声ポートの合計数の半分が含まれています。1 つのグループは、プライマリ サーバが Sub1 で、セカンダリ（バックアップ）サーバが Sub2 になるように設定されています。もう 1 つのグループは、Sub2 がプライマリ サーバで、Sub1 がバックアップになるように設定されています。

MWI 専用ポートや他の特殊なポートが、2 つのグループ間で等しく分散されていることを確認してください。音声ポートの設定中は、命名規則に特に注意してください。Cisco Unity Telephony Integration Manager（UTIM）ユーティリティでポートの 2 つのグループを設定する場合は、必ずデバイス名プレフィックスがグループごとに固有となるようにし、Cisco Unified CallManager Administration でボイスメール ポートを設定するときと同じデバイス名を使用します。この例では、デバイス名プレフィックスがポートのグループごとに固有になっています。グループ Sub1 ではデバイス名プレフィックスとして CiscoUM1 が使用され、Sub2 では CiscoUM2 が使用されています。

着信ボイスメール ポートと発信ボイスメール ポート（MWI、メッセージ通知、および TRaP 用）の比率に関する設計上の詳細情報については、http://www.cisco.com で入手可能な『*Cisco Unity Design Guide*』を参照してください。

（注） デバイス名プレフィックスは、ポートのグループごとに固有で、Cisco Unified CallManager Administration に設定されているボイスメール ポートの命名規則と一致する必要があります。

Cisco Unified CallManager Administration では、この例のポートの半分が固有なデバイス名プレフィックス CiscoUM1 を使用して登録されるように設定され、残りの半分が一意のデバイス プレフィックスを使用して登録されるように設定されています（表 13-1　を参照）。ポートが Cisco Unified CallManager に登録される場合、半分がサブスクライバ Sub1 に登録され、残りの半分が Sub2 に登録されます（表 13-1 を参照）。

表 13-1　Cisco Unified CallManager Administration でのボイスメール ポート設定

デバイス名	説明	デバイス プール	SCCP Security Profile	ステータス	IP アドレス
CiscoUM1-VI1	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI2	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI3	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM1-VI4	Unity1	Default	Standard Profile	sub1 に登録	1.1.2.9
CiscoUM2-VI1	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI2	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI3	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9
CiscoUM2-VI4	Unity1	Default	Standard Profile	sub2 に登録	1.1.2.9

（注） Cisco Unified CallManager Administration でボイスメール ポートに使用される命名規則は、Cisco UTIM で使用されるデバイス名プレフィックスと一致する必要があります。一致しないと、ポートの登録に失敗します。

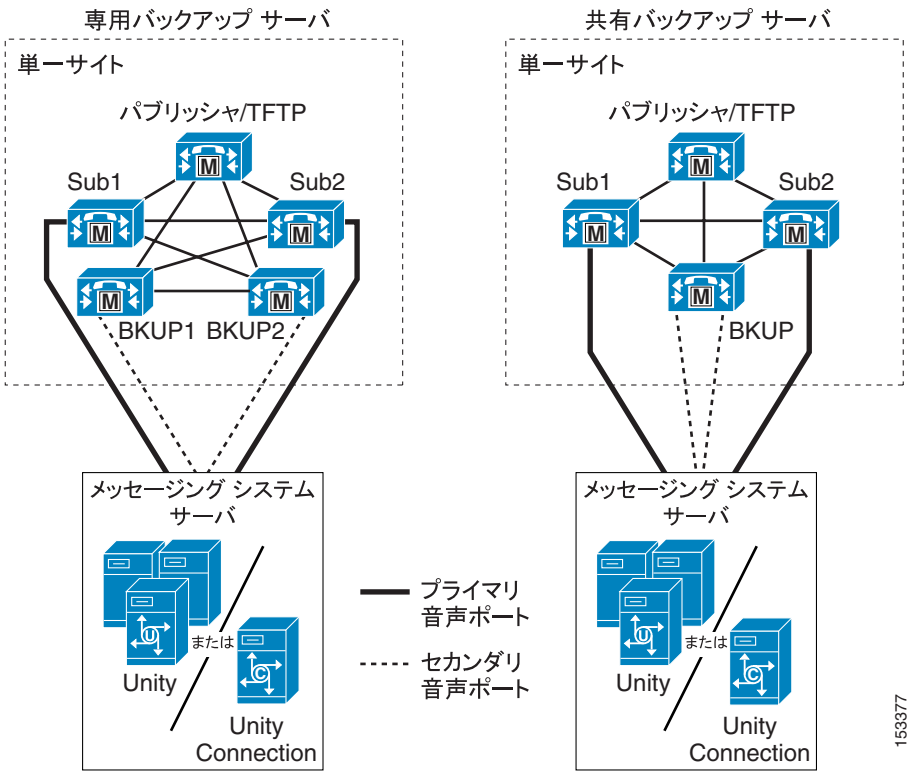
Cisco Unified CallManager 4.0 では、SCCP ボイスメール ポートでのハントと転送の方法に関して多数の変更が行われました。ボイスメール ポートの動作と設定に影響のあるこれらの変更の詳細については、次の Web サイトで入手可能な Cisco Unified CallManager 4.0 のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_0/index.htm

専用 Cisco Unified CallManager バックアップ サーバを使用する音声ポート統合

この Cisco Unified CallManager クラスタ構成では、各サブスクライバ サーバが 50% を超えるコール処理負荷で動作できます。各プライマリ サブスクライバ サーバは、専用バックアップ サーバまたは共有バックアップ サーバを持ちます（図 13-5 を参照）。正常な動作時、バックアップ サーバはコールを処理しません。サブスクライバ サーバの障害時またはメンテナンス時に、バックアップ サーバはそのサブスクライバ サーバのすべての負荷を担います。

図 13-5　単一の Cisco Unified CallManager クラスタと統合された Cisco Unity サーバ（バックアップ サブスクライバ サーバを使用）



この場合のボイスメール ポートの設定は、50/50 のロードバランシング クラスタに似ています。ただし、もう 1 台のサブスクライバ サーバをセカンダリ サーバとして使用するように音声ポートを設定せず、個別の共有バックアップ サーバまたは専用バックアップ サーバを使用します。共有バックアップ サーバと共にクラスタ化された Cisco Unified CallManager では、両方のサブスクライバ サーバのセカンダリ ポートが、単一のバックアップ サーバを使用するように設定されます。

音声ポート名（デバイス名プレフィックス）は、Cisco UTIM グループごとに固有で、Cisco Unified CallManager サーバ上で使用されるデバイス名と同じである必要があります。

Cisco Unity でボイスメール ポートを設定するには UTIM ツールを使用します。Cisco Unity Connection では、Unity Connection Administration コンソールの Telephony Integration セクションを使用します。詳細については、http://www.cisco.com で入手可能な Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

集中型メッセージングと集中型コール処理

集中型メッセージングでは、Cisco Unity サーバを Cisco Unified CallManager クラスタと同じ場所に置くことができます。集中型コール処理では、サブスクライバがクラスタおよびメッセージング サーバに対して、リモートとローカルのどちらにも存在できます（図 13-6 を参照）。リモート ユーザが中央のサイトのリソース（Tail-End Hop-Off（TEHO; テールエンド ホップオフ）の場合と同様に、音声ポート、IP Phone、公衆網ゲートウェイなど）にアクセスする場合、そのコールはゲートキーパー コール アドミッション制御にとって透過的になります。したがって、Cisco Unified CallManager でリージョンとロケーションを設定して、コール アドミッション制御を提供する必要があります（P.13-8 の「帯域幅の管理」を参照）。IP Phone または MGCP ゲートウェイにリージョン間コールを発信する場合、IP Phone は設定済みのリージョン間コーデックを自動的に選択します。WAN を通過する（リージョン間）コールのために Cisco Unity 音声ポートが Cisco Unified CallManager トランスコーディング リソースを使用するように、ネイティブ トランスコーディングを無効にする必要があります。

図 13-6　集中型メッセージングと集中型コール処理

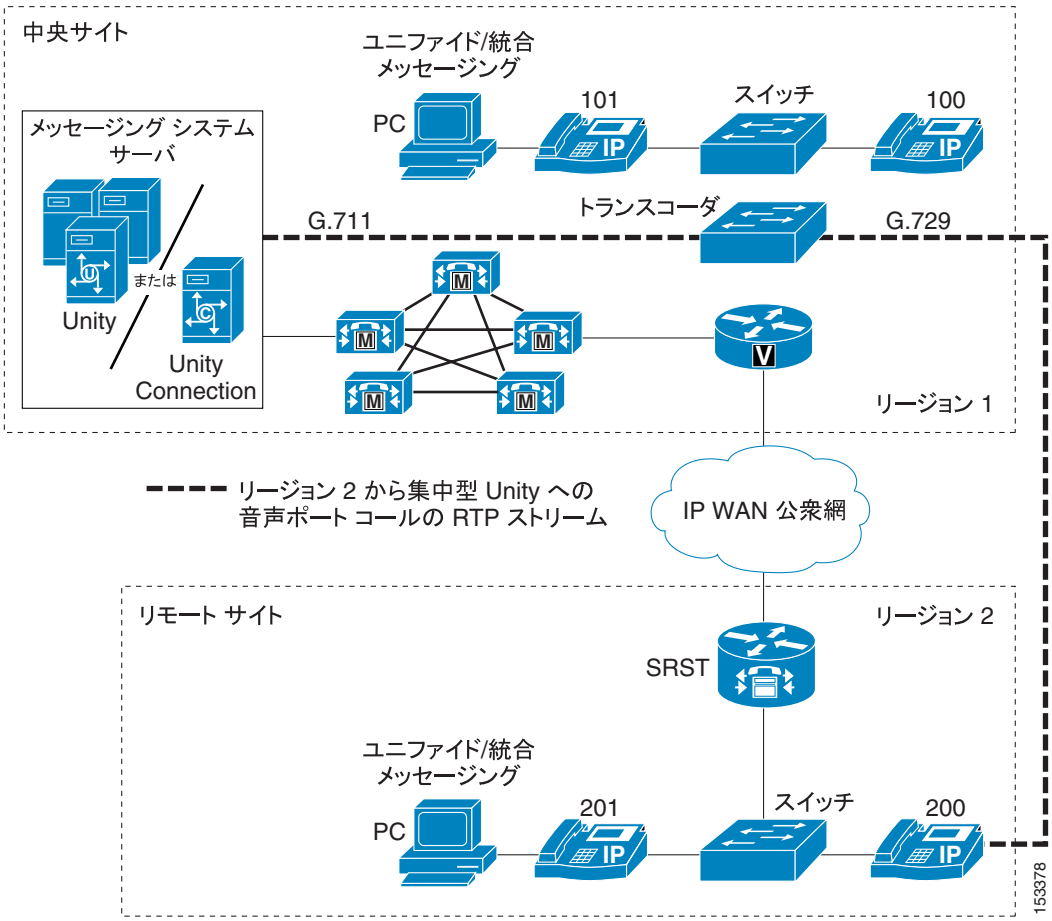


図 13-6 では、リージョン 1 と 2 が、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

図 13-6 で示しているように、内線番号 200 からリージョン 1 のボイスメール ポートにコールが発信されると、エンドポイントではリージョン間の G.729 コーデックが使用されますが、RTP ストリームがトランスコードされ、音声ポート上では G.711 が使用されます。この例では、Cisco Unity サーバ上のネイティブ トランスコーディングが無効になっています。Cisco Unified CallManager トランスコーディング リソースは、ボイスメール システムと同じサイトに置く必要があります。

ヘアピン

考慮する必要のあるもう 1 つの問題は、複数の Cisco Unity 音声ポートを介する音声コールのヘアピン（トロンボーニング）です。ヘアピンは、SCCP TSP 音声ポートだけを使用する環境では問題ではありませんが、二重統合環境では問題になります。二重統合環境では、従来型のシステムの音声ポートと SCCP TSP 音声ポートの間でヘアピンが発生する可能性があります。

二重統合の詳細については、次の Web サイトで入手可能な『*Cisco Unity Administration Guide*』を参照してください。

http://www.cisco.com

分散型メッセージングと集中型コール処理

分散型メッセージングは、テレフォニー環境内に複数のメッセージング システムが分散されており、各メッセージング システムがローカル メッセージング クライアントだけにサービスを提供することを意味します。このモデルは集中型メッセージングとは異なります。集中型メッセージングでは、メッセージング システムに対してローカルなクライアントとリモートのクライアントの両方が存在します。図 13-7 では、集中型コール処理を使用する分散型メッセージング モデルを示しています。他のマルチサイト コール処理モデルと同様に、WAN 帯域幅を管理するためにリージョンとロケーションを使用する必要があります。このモデルでは、Cisco Unity ネイティブ トランスコーディングを無効にすることも必要です。

図 13-7　分散型メッセージングと集中型コール処理

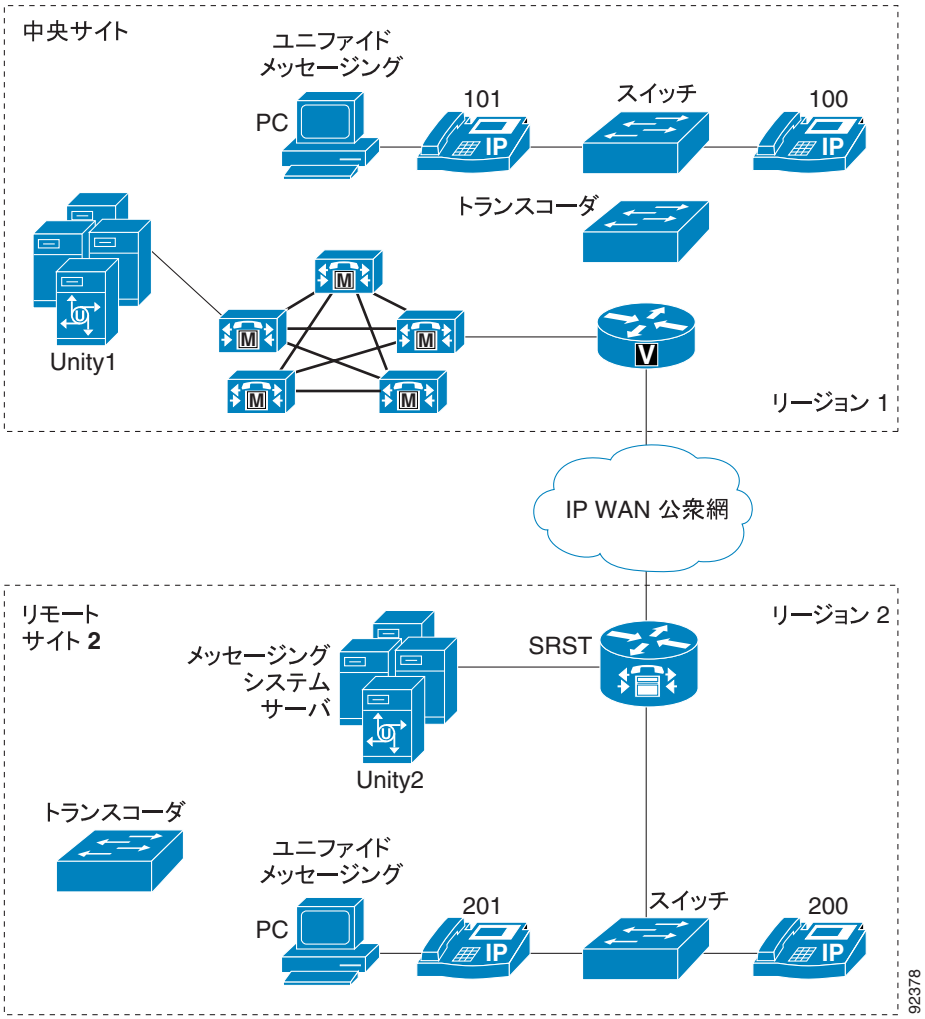


図 13-7 の構成では、トランスコーダ リソースが各 Cisco Unity メッセージ システム サイトに対してローカルである必要があります。リージョン 1 と 2 は、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。Cisco Unity サーバ上でネイティブ トランスコーディングは無効になっています。

Cisco Unified CallManager サーバに設定されているコーリング サーチ スペースとデバイス プールによって、両方の Cisco Unity サーバの音声メッセージング ポートに、適切なリージョンとロケーションが割り当てられる必要があります。さらに、テレフォニー ユーザをボイスメール ポートの特定のグループに関連付けるために、Cisco Unified CallManager ボイスメール プロファイルを設定する必要があります。コーリング サーチ スペース、デバイス プール、およびボイスメール プロファイルを設定する方法の詳細については、次の Web サイトで入手可能な、該当するバージョンの『*Cisco Unified CallManager Administration Guide*』を参照してください。

http://www.cisco.com

メッセージング システムは相互に「ネットワーク接続」され、内部ユーザと外部ユーザの両方に単一のメッセージング システムを提供します。分散 Unity サーバ向けの Cisco Unity ネットワーク機能については、次の Web サイトで入手可能な『*Networking in Cisco Unity Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/products_feature_guides_list.html

結合されたメッセージング配置モデル

複数のメッセージング モデルを同じ配置で組み合せることができます。ただし、その配置は、上記の項で示したすべてのガイドラインに従う必要があります。図 13-8 では、集中型メッセージングと分散型メッセージングの両方が同時に採用されるユーザ環境を示しています。

図 13-8　結合された配置モデル

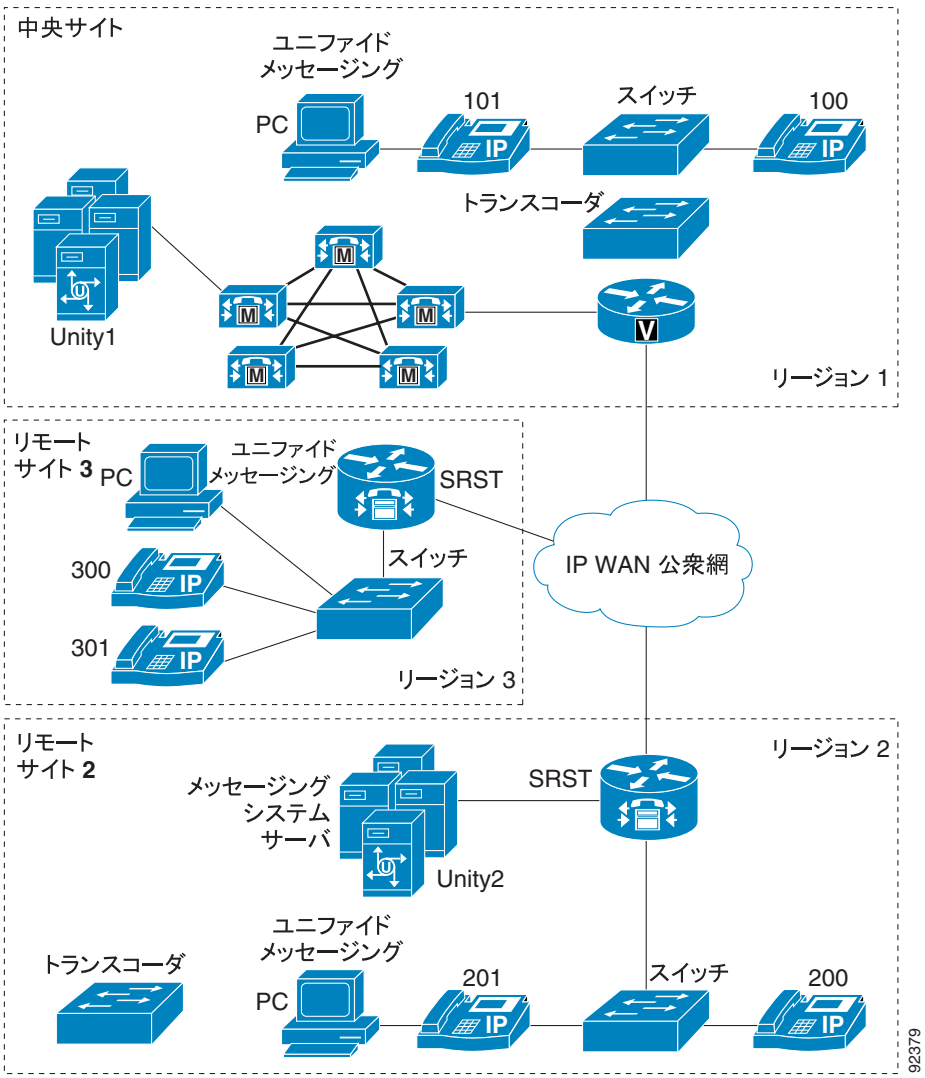


図 13-8 では、2 つのメッセージング モデルの結合を示しています。リージョン 1 と 3 は集中型メッセージングと集中型コール処理を使用し、リージョン 2 は分散型メッセージングと集中型コール処理を使用しています。すべてのリージョンが、リージョン内コールに G.711 を使用し、リージョン間コールに G.729 を使用するように設定されています。

図 13-8 では、中央サイトとサイト 3 の間で、集中型メッセージングと集中型コール制御が使用されています。中央サイトのメッセージング システムは、中央サイトとサイト 3 の両方のクライアントにメッセージング サービスを提供します。サイト 2 は、集中型コール処理を使用する分散型メッセージング モデルを使用しています。サイト 2 に置かれているメッセージング システム（Unity2）は、サイト 2 の中にいるユーザだけにメッセージング サービスを提供します。この配置では、両方

のモデルが、この章に記載されているそれぞれの設計上のガイドラインに従っています。トランスコーディング リソースは各メッセージング システム サイトに対してローカルに置かれ、サイト 2 のユーザが中央サイトのユーザにメッセージを残す場合のように、（メッセージング システムに対して）リモートのサイトからメッセージング サービスにアクセスするクライアントをサポートします。

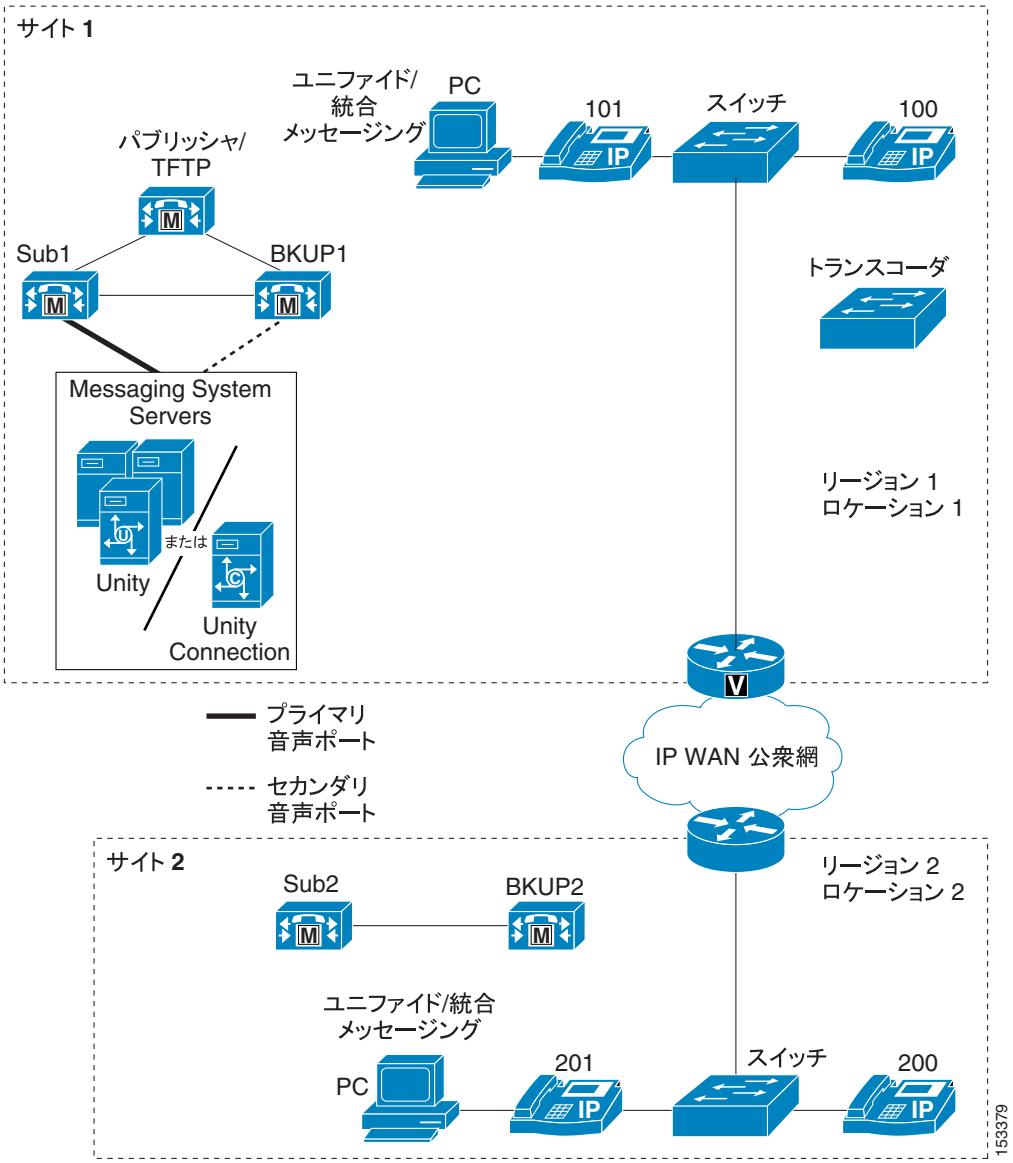
集中型メッセージングと WAN を介したクラスタ化

ここでは、集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介した Cisco Unified CallManager クラスタ化を一緒に配置する場合の Cisco Unity の設計上の問題について説明します。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、すべてのリモート メッセージング サイトがボイスメール機能を失います（図 13-9 を参照）。

WAN を介したクラスタ化は、ローカル フェールオーバーをサポートしています。ローカル フェールオーバーでは、各サイトが、物理的にそのサイトに置かれているバックアップ サブスクライバ サーバを持ちます。ここでは、Cisco Unity 集中型メッセージングと、WAN を介したクラスタ化のローカル フェールオーバーを一緒に配置する方法を中心に説明します。

詳細については、P.2-19 の「IP WAN を介したクラスタ化」の項を参照してください。

図 13-9　Cisco Unity 集中型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



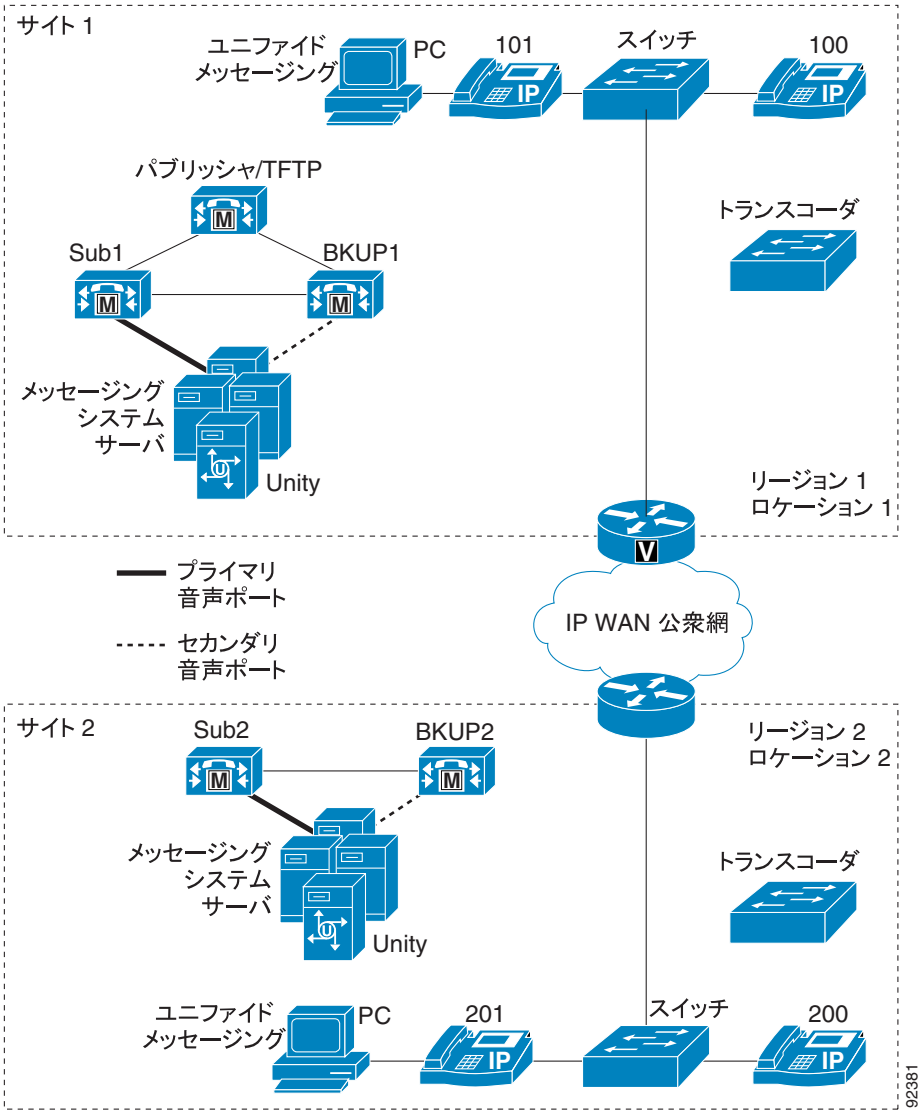
クラスタ サイト間で必要な最小帯域幅は T1 回線（1,544 MHz）です。この帯域幅で、最大 10,000 の Busy Hour Call Attempts（BHCA: 混雑時発呼）に対してシグナリング トラフィックおよびデータベース トラフィックをサポートできます。ただし、これには、必要なメディア帯域幅が含まれていません。

Cisco CallManager Release 3.3(3) 以前を使用する WAN を介したクラスタ化では、クラスタごとに最大 4 つのサイトをサポートしますが、Cisco Unified CallManager Release 4.1 以上では最大 8 つのサイトをサポートします。Cisco Unity は、どちらの場合でもその最大数までサイトをサポートします。ボイスメール ポートは、Cisco Unity メッセージング システムが置かれているサイトだけに設定されます（図 13-9 を参照してください）。ボイスメール ポートは、WAN を介してリモート サイトに登録されません。他のサイトのメッセージング クライアントは、プライマリ サイトのすべてのボイスメール リソースにアクセスします。WAN に障害が発生すると、リモート サイトは集中型メッセージング システムにアクセスできなくなるため、WAN を介してリモート サイトに音声ポートを設定してもメリットがありません。帯域幅を考慮して、ボイスメール ポートで TRaP を無効にし、すべてのメッセージング クライアントがそのローカル PC（ユニファイド メッセージング専用）にボイスメール メッセージをダウンロードするようにする必要があります。

分散型メッセージングと WAN を介したクラスタ化

Cisco Unity メッセージング サーバも配置されたローカル フェールオーバー サイトでは、集中型メッセージング モデルと同様に、音声ポートがローカル Cisco Unified CallManager サブスクライバ サーバに登録されます。音声ポートの設定については、P.13-12 の「Cisco Unified CallManager クラスタとの音声ポート統合」および P.13-14 の「専用 Cisco Unified CallManager バックアップ サーバを使用する音声ポート統合」を参照してください。

図 13-10　Cisco Unity 分散型メッセージングと、ローカル フェールオーバー機能を持つ WAN を介したクラスタ化



WAN を介したクラスタ化を含む単純分散型メッセージング実装では、クラスタ内の各サイトに、独自の Cisco Unity メッセージング サーバとメッセージング インフラストラクチャ コンポーネントが置かれます。すべてのサイトにローカル Cisco Unity メッセージング システムが置かれるわけではなく、一部のサイトで、ローカル メッセージング クライアントがリモート メッセージング サーバを使用する場合、その配置は分散型メッセージングと集中型メッセージングの結合モデルとなります（P.13-19 の「結合されたメッセージング配置モデル」を参照）。このモデルで WAN に障害が発生した場合は、WAN が復元されるまで、集中型メッセージングを使用するすべてのリモート サイトがボイスメール機能を失います。

ローカル メッセージング サーバを持たない各サイトは、そのすべてのメッセージング クライアントに対して単一のメッセージング サーバを使用する必要がありますが、そのようなサイトのすべてが同じメッセージング サーバを使用する必要はありません。たとえば、サイト 1 とサイト 2 のそれぞれがローカル メッセージング サーバを持っているとします。その場合、サイト 3 のすべてのクライアントがサイト 2 のメッセージング サーバを使用し（そのメッセージング サーバに登録し）、サイト 4 のすべてのクライアントがサイト 1 のメッセージング サーバを使用するようにすることができます。ローカル Cisco Unity メッセージング サーバを持つサイトには、トランスコーダ リソースが必要です。

他の分散型コール処理配置と同様に、これらのサイト間のコールはゲートキーパー コール アドミッション制御にとって透過的です。したがって、Cisco Unified CallManager でリージョンとロケーションを設定してコール アドミッション制御を提供する必要があります（P.13-8 の「帯域幅の管理」を参照）。

分散 Cisco Unity サーバは、デジタルでネットワーク接続することもできます。このトピックの詳細については、http://www.cisco.com で入手可能な『*Cisco Unity Networking Guide*』を参照してください。配置される特定のメッセージング ストアに固有の Networking Guide が用意されています。

Cisco Unity メッセージング フェールオーバー

Cisco Unity フェールオーバーにより、Cisco Unity サーバに障害が発生した場合のボイスメール存続可能性が確保されます（図 13-1 を参照）。Cisco Unity ローカル フェールオーバーでは、プライマリとセカンダリの両方の Unity メッセージング サーバが同じ物理ロケーションに存在し、メッセージング インフラストラクチャ コンポーネントがプライマリ サーバと同じ場所に置かれます。メッセージング インフラストラクチャ コンポーネント（メッセージング ストア サーバ、Domain Controller/Global Catalog（DC/GC; ドメイン コントローラ / グローバル カタログ）サーバ、DNS サーバなど）は、オプションで、冗長コンポーネントを持つこともできます。これらは、Cisco Unity セカンダリ サーバと物理的に同じ場所に置くことができます。

Cisco Unity フェールオーバーは、すべてのメッセージング配置モデルでサポートされています。Cisco Unity Connection は現在、フェールオーバーをサポートしていません。

Cisco Unity フェールオーバーの設定については、次の Web サイトで入手可能な『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

http://www.cisco.com

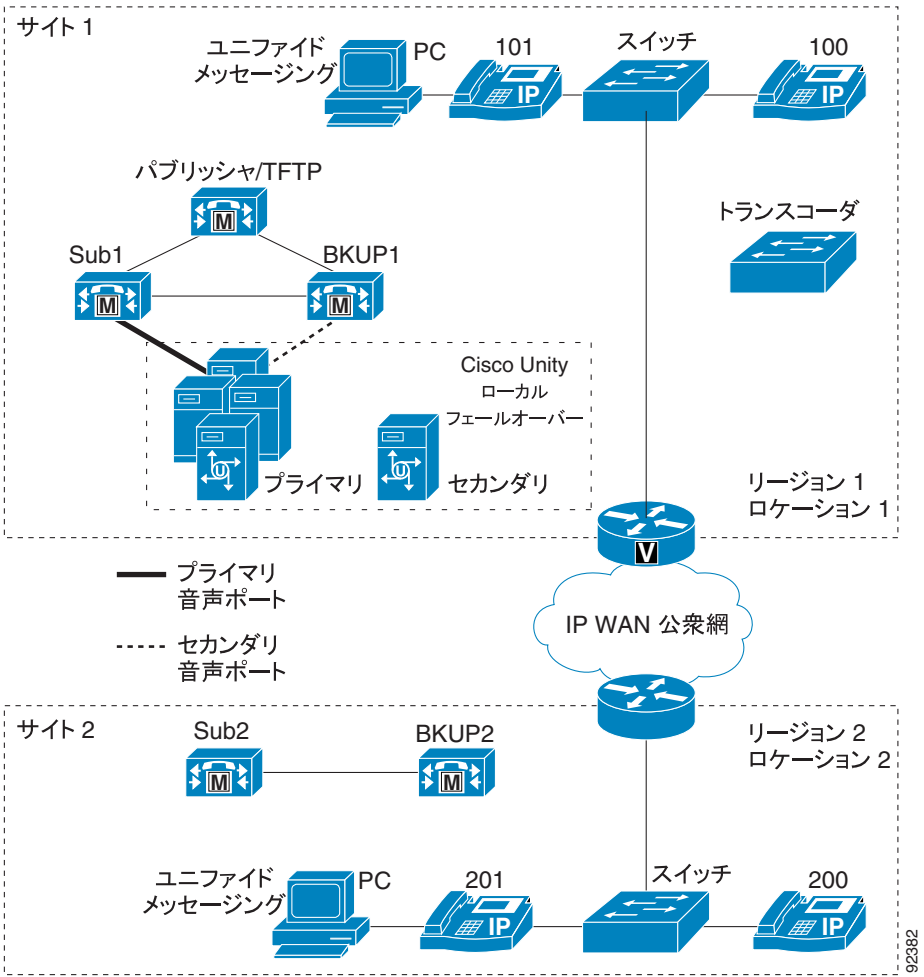
Cisco Unity フェールオーバーと WAN を介したクラスタ化

Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化を配置する場合は、P.13-21 の「集中型メッセージングと WAN を介したクラスタ化」および P.13-23 の「分散型メッセージングと WAN を介したクラスタ化」で説明している設計プラクティスを適用します。正常な動作時、プライマリ Cisco Unity サーバからの音声ポートは WAN を通過しません。

図 13-11 では、Cisco Unity ローカル フェールオーバーを示しています。プライマリ Cisco Unity サーバとセカンダリ Cisco Unity サーバの両方が物理的に同じサイトに置かれていることに注意してください。Cisco Unity フェールオーバーは、Cisco Unified CallManager の WAN を介したクラスタ化で使用可能な最大数までリモート サイトをサポートします。

(注)　Unity Connection は現在、フェールオーバーをサポートしていません。

図 13-11　Cisco Unity ローカル フェールオーバーと WAN を介したクラスタ化



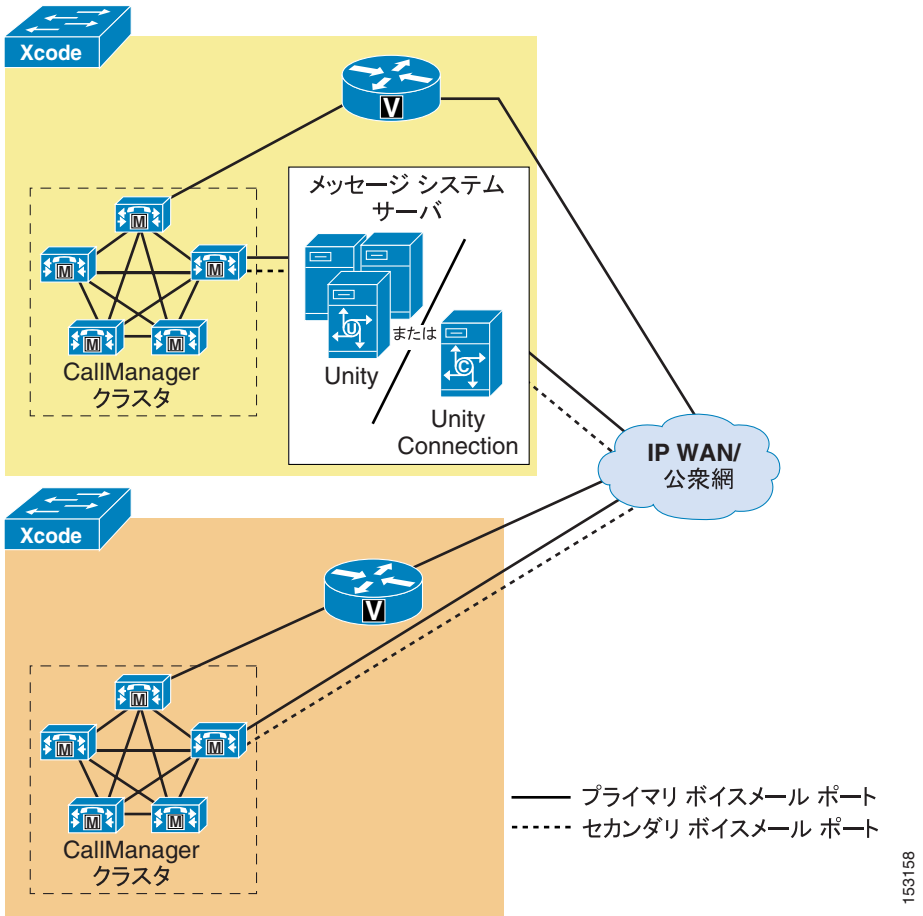
Cisco Unity フェールオーバーの設定については、次の Web サイトで入手可能な『*Cisco Unity Failover Configuration and Administration Guide*』を参照してください。

http://www.cisco.com

集中型メッセージングと複数の Cisco Unified CallManager サーバ

Cisco Unity および Unity Connection はポート グループをサポートしているため、いずれかの Unity 製品サーバ上のサブスクライバをポート グループと関連付け、最終的に統合することができます。サブスクライバが特定のポート グループに関連付けられると、そのポート グループに属する MWI ポートだけで、ユーザの MWI 機能が実行されます。この機能は、SCCP と SIP の両方のボイスメール ポートで同じ動作になります。Cisco Unity は最大 7 つのポート グループをサポートしますが、Cisco Unity Connection は最大 9 つのポート グループをサポートしています。詳細については、http://www.cisco.com で入手可能な該当する Cisco Unity または Cisco Unity Connection のアドミニストレーション ガイドを参照してください。

図 13-12　Cisco Unity または Unity Connection と複数の Cisco Unified CallManager クラスタの統合



クラスタ 1 とクラスタ 2 の両方のサイトのメッセージング クライアントが、物理的にクラスタ 1 に置かれている Cisco Unity または Unity Connection メッセージング インフラストラクチャを使用します（図 13-12 を参照）。

CHAPTER 14

Cisco Unified MeetingPlace の統合

この章では、Cisco Unified MeetingPlace を既存の Cisco Unified Communications ネットワークに組み込むための技術上および設計上の問題について説明します。MeetingPlace の基本的なネットワークインフラストラクチャと IP テレフォニーの設計に関する考慮事項は、Cisco Unified CallManager の IP テレフォニーの設計に関する考慮事項と同じです。この章では、読者がすでに Cisco Unified Communications についての基本的な知識と経験を持っていることを前提にしています。

この章では、主に Cisco Unified MeetingPlace と IP テレフォニーの両方を、1 つの統合されたネットワーク内で組み合せる際の統合と設計上の問題について説明します。このセットアップでは、MeetingPlace から公衆電話交換網（PSTN）への時分割多重（TDM）接続は考慮されません。公衆網アクセスは、Cisco Unified CallManager を通じて音声ゲートウェイによって提供されるのが一般的なためです。

この章では、統合に影響しないその他の MeetingPlace コンポーネント（たとえば、Outlook、Lotus Notes、電子メール（Simple Mail Transfer Protocol、SMTP）、ディレクトリ サービス、インスタントメッセージングなどのための MeetingPlace コンポーネント）については説明していません。また、MeetingPlace に関する特定の製品レベルの情報（機能の説明や設定オプションなど）も、このマニュアルの対象外です。MeetingPlace の詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/index.htm

MeetingPlace サーバの推奨事項

表 14-1 に、各種の配置シナリオで使用する際に推奨される Cisco Media Convergence Server（MCS）のモデルを示します。

表 14-1　推奨される MCS の配置

サーバの MeetingPlace コンポーネント	最大 480 の音声ユーザ ライセンス	480 を超える音声ユーザ ライセンス
すべてのバンドル（H.323/SIP IP Gateway、Web ユーザ インターフェイス、電子メール ゲートウェイを含む） Outlook または Notes ディレクトリ サービス 音声ゲートウェイ	MCS 7835	MCS 7845
Web 会議	Web ユーザ ライセンス 200 ごとに 1 台の MCS 7845 を追加	
インスタント メッセージング（IM）ゲートウェイ	1 台の MCS 7835 を追加	

MCS の配置には、次のガイドラインも適用されます。

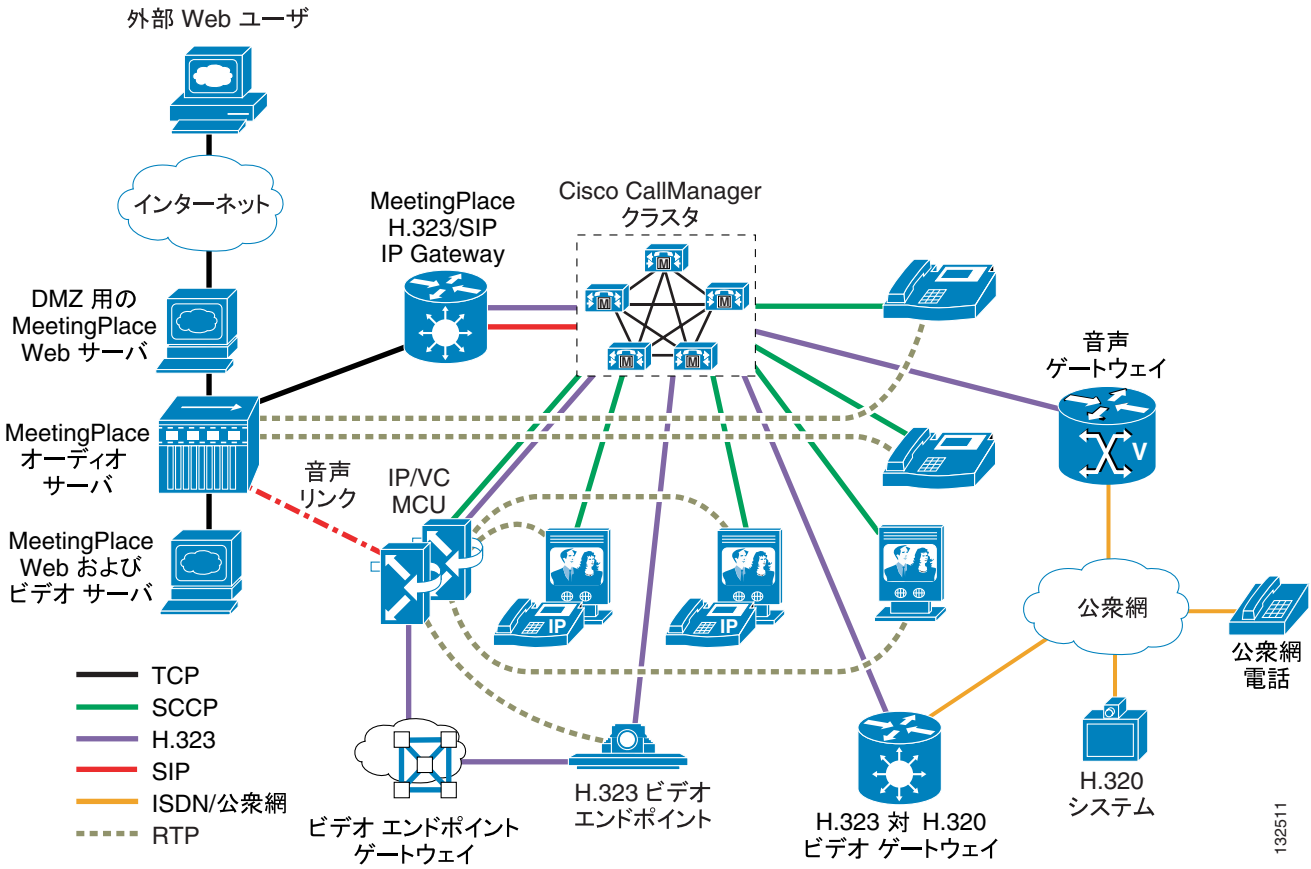
- 最大 50 の Web 会議ユーザ ライセンスの配置では、バンドルされたソフトウェアとその他のオプションを使用して、同じ MCS 上で Web 会議を実行できます。
- 50 を超える Web 会議ユーザ ライセンスの配置では、Outlook または Notes、および Web 会議の Schedule、Find、Attend の各機能を Web 会議専用の MCS 7845 に移動します。
- 100 を超える Web 会議ユーザ ライセンスの配置では、Microsoft Desktop Engine（MSDE）2000 を使用しないでください。スケジューリングと Web 会議のための同時接続が 8 つまでに制限されているためです。SQL 2000 が必須であり、お客様が用意する必要があります。大規模なインストレーション（500 を超えるユーザ ライセンス）では、専用のサーバで SQL 2000 を実行してください。
- 200 を超える音声ユーザ ライセンスの配置（一般的には 10,000 を超えるレコード数）では、Directory Integration 用に専用の MCS 7835 が必要です。

配置モデル

この項では、MeetingPlace を Cisco Unified CallManager と組み合せて配置するために使用する主要な配置モデルについて説明します。この項の説明では、Cisco Unified CallManager クラスタを持つ大規模サイトに MeetingPlace システムが設定されているものとします。

図 14-1 は、包括的な Cisco Unified Communications トポロジと統合された Cisco Unified MeetingPlace 5.3 を示しています。Cisco Unified CallManager クラスタ（Cisco Unified CallManager 4.0 以上を実行している）には、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）が提供するビデオ会議機能を備えたビデオ配置（SCCP と H.323 の両方のビデオ エンドポイント）が含まれています。H.323 から H.320 へのビデオ ゲートウェイは、公衆網へのビデオ コールを処理します。MeetingPlace H.323/SIP IP Gateway を通じて、Cisco Unified CallManager は MeetingPlace がそのオーディオ、ビデオ、および Web 会議ソリューションで提供するリッチメディア機能を十分に活用し、外部ユーザもインターネットからアクセスできます。

図 14-1　MeetingPlace と IP テレフォニーを統合するトポロジの例



次の各項では、MeetingPlace と Cisco Unified CallManager を統合するための主要な配置モデルについて説明します。

単一サイト

単一サイトで IP テレフォニーと MeetingPlace を実現する場合のモデルは、その単一サイトに配置されるコール処理エージェントと、そのサイト全体に音声、ビデオ、およびコラボレーションのトラフィックを伝送するための LAN または MAN（メトロポリタンエリア ネットワーク）から構成されます。会議の参加者が LAN または MAN の外部にいる場合は、PSTN（公衆電話交換網）が使用されます。IP WAN が単一サイト モデルに組み込まれている場合、IP WAN はデータと Web コラボレーションのトラフィック専用です。テレフォニー サービスは WAN を介して行われることはありません。

IP テレフォニーの単一サイト配置モデルの詳細な説明については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

会議およびコラボレーション システムの復元性を最大限に高めるために、MeetingPlace はデータ センター内に配置してください。単一サイト モデルでは、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）音声ゲートウェイの使用をお勧めします。ただし、外部のビデオ参加者をサポートするには、H.323/H.320 Cisco Unified Videoconferencing ゲートウェイが必要です。外部アクセスを提供するための推奨される方法は、Cisco Unified CallManager ゲートウェイを介した MeetingPlace のパイロット番号にフリーダイヤル番号または Direct Inward Dial（DID; ダイヤルイン方式）番号を使用することですが、MeetingPlace に直接接続した専用の公衆網 T1 または E1 回線を使用する方法もあります。一般的なシステムには、ユーザがオーディオ会議セッションにダイヤルインできるように、1 つのフリーダイヤル番号、1 つの DID 番号またはセントラル オフィス番号、および内部ダイヤル番号が含まれています。一意の DID 番号は、他のアプリケーションで常時使用可能な専用の危機管理 ID または一意の会議 ID に使用できます。

集中型コール処理を使用するマルチサイト WAN

集中型コール処理を使用するマルチサイト WAN モデルは、単一のコール処理エージェントから構成されています。このコール処理エージェントは、多数のサイトにサービスを提供し、IP WAN を使用してサイト間で音声やビデオ トラフィックを転送します。また、IP WAN は、中央サイトとリモート サイト間のコール制御信号も伝送します。

集中型コール処理を使用する IP テレフォニーのマルチサイト配置モデルの詳細な説明については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

すべてのサイトに集中型の会議およびコラボレーション サービスを提供するには、MeetingPlace をメイン サイトに配置する必要があります。各サイトからの会議参加者の数を考慮するときは、必要な WAN 帯域幅や、中央サイトにある MeetingPlace への公衆網コールの数について計画を立てます。WAN の帯域幅が十分でない場合、ユーザは公衆網からフリーダイヤル サービスや専用の CO または DID 番号を使用した再ダイヤルが必要になります。リモート サイトが中央の Cisco Unified CallManager クラスタへの接続を失い、Survivable Remote Site Telephony（SRST）モードに入るか Cisco Unified CallManager Express に切り替わった場合、MeetingPlace 会議へのアクセスは公衆網からのものだけになり、ビデオ サポートが自動的には含まれなくなります。ただし、Web コラボレーション トラフィックは、バックアップ データ パスが使用可能であれば、引き続き使用できます。

分散型コール処理を使用するマルチサイト WAN

分散型コール処理を使用するマルチサイト WAN モデルでは、複数の独立したサイトから構成されています。各サイトには独自のコール処理エージェントがあり、そのエージェントは、分散サイト間の音声およびビデオ トラフィックを伝送する IP WAN に接続されます。

分散型コール処理を使用する IP テレフォニーのマルチサイト配置モデルの詳細な説明については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

MeetingPlace は、1 つ、複数、またはすべての分散型コール処理サイトに配置できます。さまざまな Cisco Unified CallManager クラスタにある各種の MeetingPlace システムへのアクセスには、クラスタ間トランクや公衆網が使用されます。Web コラボレーションには、常に IP WAN が使用されます。柔軟性を高めるには、定型ダイヤル プランを実装し、すべての Cisco Unified CallManager クラスタのすべてのユーザが、同一または別の　Cisco Unified CallManager　クラスタに接続した MeetingPlace を使用して、確実に MeetingPlace にアクセスできるようにします。MeetingPlace には、「マルチサーバ会議」と呼ばれる機能もあります。これは、複数のサイトの複数のユーザが同じ会議に参加しているときに、帯域幅や公衆網コールを節約できるカスケード式の会議です（マルチサーバ会議の詳細については、P.14-25 の「会議」の章を参照してください）。

IP WAN を介したクラスタ化

このモデルでは、単一の Cisco Unified CallManager クラスタが配置されていて、複数のサイト間は QoS 機能に対応している IP WAN によって接続されています。

WAN を介したクラスタ処理の詳細な説明については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

WAN を介したクラスタリングを使用すると、さまざまな Cisco Unified CallManager サイトに複数の MeetingPlace Audio Server を配置できます（デュアル会議サーバについては、P.14-41 の「障害回復」の項を参照してください）。サーバ間でユーザ プロファイル情報を同期するには、MeetingPlace Directory Service Integration オプションを使用します。

Cisco Unified CallManager　では、ルート　グループとルート　リストを設定することにより、MeetingPlace Audio Server の 1 つで障害が発生した場合でも、別の MeetingPlace システムへコールをルーティングできます。会議情報はサーバ間で伝送されないので、管理者は障害の発生したシステムから別のシステムへ会議情報を手動でアップロードして使用する必要があります。

WAN が停止しても各サーバは動作し続け、ローカル ユーザにサービスを提供できます。リモート ユーザが同じオーディオ サーバ上の会議に参加できるようにするには、Cisco Unified CallManager 上にルート グループとルート リストを設定し、コールを再ルーティングします。

複数のオーディオ サーバがある場合は、Vanity ID 機能（ユーザが会議 ID を独自に選択および設定できる機能）をオフすることで、フェールオーバー モードをサポートし、アップロード中に会議 ID が競合する可能性を少なくすることを強くお勧めします。

MeetingPlace のコンポーネント

ここでは、MeetingPlace システムの設計に影響を与える、次の主要なコンポーネントについて説明します。

- MeetingPlace Audio Server（P.14-6）
- MeetingPlace H.323/SIP IP Gateway（P.14-6）

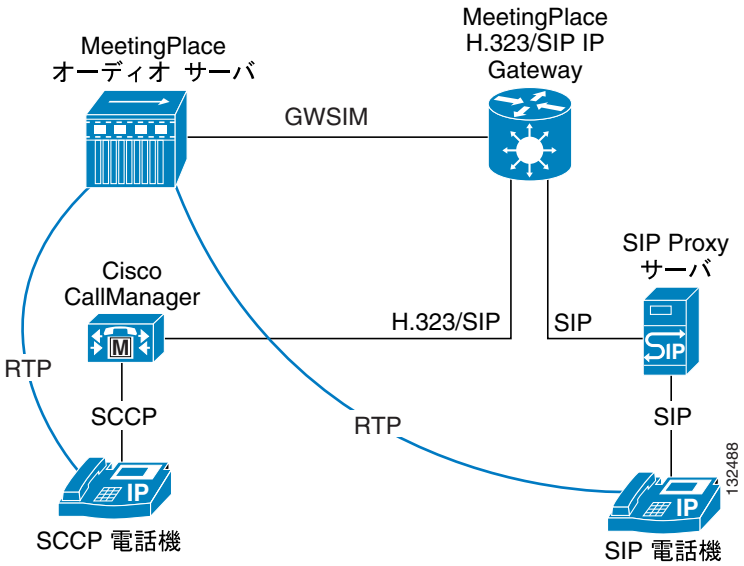
MeetingPlace Audio Server

MeetingPlace Audio Server（8112 または 8016）は、オーディオ会議機能のための Digital Signal Processor（DSP; デジタル シグナル プロセッサ）リソースを提供します。さらに、MeetingPlace サーバは Web、オーディオ、およびビデオ会議のスケジューリング モジュールとして機能します。MeetingPlace サーバは予約に基づいて、会議に参加できるユーザの数と会議の継続時間を制御します。

MeetingPlace H.323/SIP IP Gateway

MeetingPlace Audio Server は当初、T1/E1 トランクを介したサービス プロバイダーまたは PBX の基礎となる TDM 接続のために設計されました。既存の Cisco Unified Communications ネットワークに組み込むには、2 つのネットワークをリンクする MeetingPlace H.323/SIP IP Gateway が必要です。これは「ゲートウェイ」と呼ばれますが、ハードウェアのゲートウェイではなく、MCS サーバ上に存在するソフトウェア アプリケーションであり、MeetingPlace Audio Server と Cisco Unified CallManager の間の通信に使用されます（図 14-2 を参照）。

図 14-2　インターフェイスとして使用される MeetingPlace H.323/SIP IP Gateway



MeetingPlace H.323/SIP IP Gateway は、H.323 と SIP を同時にサポートします。MeetingPlace H.323/SIP IP Gateway がサポートするプロトコルの詳細については、P.14-18 の「相互運用性プロトコル」の項を参照してください。

MeetingPlace オーディオ サーバは、TDM 接続と IP 接続の混在をサポートできます。混在環境のキャパシティは、システム内の TDM ポートと IP カード（ユーザ ライセンス）の組み合せによって異なります。

MeetingPlace H.323/SIP IP Gateway は、同じ Cisco Media Convergence Server（MCS）上で他の MeetingPlace アプリケーション（MeetingPlace Web、SMTP 電子メール、Video Integration など）と共存できますが、純粋な IP のセットアップでは、MeetingPlace H.323/SIP IP Gateway を単一の MCS 上に独立してインストールすることをお勧めします。そうすることにより、Web またはビデオの部分で何かの問題が発生した場合でも、オーディオ通信が影響を受けずに済みます。ただし、小規模な配置の場合、MeetingPlace H.323/SIP IP Gateway は MeetingPlace Web Conferencing Service と共存でき、MCS の CPU リソースをあまり使用しないので、Web 会議のパフォーマンスとキャパシティも大きな影響を受けません。

単一の MeetingPlace Audio Server を複数の MeetingPlace H.323/SIP IP Gateway に接続できます。1 つの MeetingPlace H.323/SIP IP Gateway に障害が発生し、進行中のコールがドロップされた場合は、新しいコールがセカンダリ MeetingPlace H.323/SIP IP Gateway へルーティングされます。MeetingPlace Audio Server からの発信ダイヤリングの場合、サーバはアクティビティが最小の MeetingPlace H.323/SIP IP Gateway を選択します。詳細については、P.14-41 の「冗長性とロード バランシング」の項を参照してください。

それぞれの MeetingPlace H.323/SIP IP Gateway は、ゲートキーパーなしではサポートする Cisco Unified CallManager が 1 つだけですが、ゲートキーパーを使用すると複数の Cisco Unified CallManagers をサポートできます。それぞれの MeetingPlace Audio Server は最大で 16 の MeetingPlace H.323/SIP IP Gateways に接続し、冗長性、ロード バランシング、および複数の Cisco Unified CallManager クラスタのサポートが得られます。

1 つの Audio Server で、MeetingPlace アプリケーションがインストールされた GWSIM MCS サーバを最大 16 サポートできるので、複数の IP ゲートウェイをサポートできます（組み合された MCS アプリケーション サーバ数は 16 まで）。

（注） MeetingPlace Audio Server と MeetingPlace H.323/SIP IP Gateway の間で、Network Address Translation（NAT; ネットワーク アドレス変換）を使用しないでください。

MeetingPlace H.323/SIP IP Gateway は、次の 1 つまたは複数の方法で Cisco Unified CallManager と通信できます。

- SIP を介して、Cisco Unified CallManager が MeetingPlace H.323/SIP IP Gateway と直接通信する。

  この方法を実装するには、MeetingPlace H.323/SIP IP Gateway への接続を Cisco Unified CallManager で SIP トランクとして設定します。
- H323 を介して、Cisco Unified CallManager が MeetingPlace H.323/SIP IP Gateway と直接通信する。

  この方法を実装するには、MeetingPlace H.323/SIP IP Gateway への接続を Cisco Unified CallManager で H.323 ゲートウェイとして設定します。
- ゲートキーパーを介して、Cisco Unified CallManager が MeetingPlace H.323/SIP IP Gateway と通信する。

  この方法では、Cisco Unified CallManager と MeetingPlace H.323/SIP IP Gateway をゲートキーパーに登録し、そのゲートキーパーがコール ルーティングを処理します。

MeetingPlace 配置のサイズの選定

Cisco Unified MeetingPlace 配置のサイズの選定では、主に次の事項を考慮します。

- 音声ユーザのライセンス、またはオーディオ ポート
- Web 会議のライセンス
- ビデオ会議の IP/VC MCU のサイズ選定

MeetingPlace システムのサイズの選定を行うときは、常に 8100 Audio Server から始めて、月あたりの平均会議時間（分）に関する最も正確な見積りを使用します。この見積りは、会議サービス プロバイダーから入手した現行の課金情報から算出できます。たとえば、課金情報に 1 年間の合計会議時間の分数が含まれている場合は、その合計を 12 で割るか、ピークの月を選んで見積りとして使用します。ユーザの調査とフィードバックも、月平均の使用状況を割り出すのに役立ちます。

さらに、少なくとも最初の年に対して（できればそれ以降の年に対しても）、何らかの成長係数（一般には 10% ～ 30%）を加えてください。Cisco Unified MeetingPlace Outlook Integration オプション（音声、Web、またはビデオ会議のスケジューリング、通知、および参加を簡単に行える）を組み込む場合は、予定される使用状況に基づいて、成長係数がさらに大きくなる（場合によっては 30% ～ 50%）こともあります。

MeetingPlace ソリューションのサイズ選定を行うときは、次の一般的なガイドラインを使用します。

- 現行のサービス プロバイダーの請求書から得た実際の会議の使用状況が、最良の基準になります。
- サイズ選定の公式を適用する前に必ず、少なくとも 1 年目に対して成長率（一般的には 10% ～ 30%）を加えてください。
- まれなケースですが、現在の会議の使用状況がわからない場合は、次の前提を適用できます。
  - 統計的には、20 人のテレフォニー ユーザごとに少なくとも 1 つのオーディオ会議ポート（ライセンス）が、MeetingPlace オーディオ サービスに必要（たとえば、2500 ユーザ / 20 = 125 音声ユーザ ライセンスが必要）。
  - 1 人のユーザの月あたり会議時間は平均 100 分（たとえば、5500 ユーザ * 100 = 550,000 分 / 月）。

  この前提は、課金データとの比較に使用することもできます。

音声会議の使用率のサイズ選定

必要な音声ユーザ ライセンスの数を計算する一般的な計算式は、次のとおりです。

MeetingPlace 音声ユーザ ライセンスの数 =
（月あたりの平均会議時間（分）+ 成長係数）/ ベースライン

小数点以下の端数は整数に切り上げてください。

表 14-2 は、この計算式に使用するベースラインのリストです。

表 14-2　必要なユーザ ライセンス数計算のベースライン

月あたりの平均時間（分）	ベースライン（ユーザ ライセンスあたりの時間（分））
50,000 ～ 300,000	2,000
300,000 ～ 700,000	2,500
700,000 ～ 1,000,000	3,000
1,000,000 ～ 2,000,000	3,500
2,000,000 超	4,000

たとえば、使用しているシステムの月平均使用状況が会議時間にして 528,000 分間と見積られる場合、必要なユーザ ライセンスの数は次のようになります。

MeetingPlace 音声ユーザ ライセンスの数 = 528,000 * (1 + 20%) / 2500 =　254

Web 会議の使用率のサイズ選定

必要となる Web ユーザ ライセンスの数は、音声ユーザ ライセンスの合計数に対する比率、または Web 会議の使用率に関するサービス プロバイダーからの課金情報に基づいて算出できます。一般的な配置では、音声会議ライセンス数の 25% ～ 50%（25% が最も一般的）が Web 会議ライセンス数として使用されますが、音声ユーザ ライセンスと Web ユーザ ライセンスを同じ数だけ配置している企業もあります。

たとえば、音声ユーザ ライセンス数が 240 の配置では、Web ユーザがそのうちの 25% として、Web ユーザ ライセンス数を 60 とする必要があります。このシステムの場合、1 台の MCS 7845 があれば Web サービスを処理でき、最大 200 Web ユーザ ライセンスまでの増大にも対処できます。

Web 会議は、必要となる Cisco MCS 7800 シリーズ サーバの数にも直接影響を与えます。他の MeetingPlace 統合モジュールと同じ場所に置かれた 1 台の MCS 7835 は約 50 Web セッションに対応できますが、MCS 7845 は最大で約 200 Web セッションまで対応できます（ピーク時間における実際の使用方法のタイプによって異なります）。したがって、Web 会議 リソースのサイズ選定は、企業のデータ環境における全体設計やソリューションの配置にとって大変重要です。

Web 会議の使用率は、一般的に音声会議の使用率よりも速い成長率を示し、企業内の Web コラボレーションの量に依存します。Web 会議の場合は、今後 2 ～ 5 年間の成長（一般的には 1 年あたり 20% ～ 30%）を見積るようにしてください。

Video Integration と MCU のサイズ選定

MeetingPlace Video Integration はシステム全体のソフトウェア モジュールであり、ビデオ会議にユーザ ライセンスは不要です。サポートされるビデオ ユーザの数は、MCU 上で MeetingPlace が制御に使用できる H.323 ポートの数で決まります。IP/VC 3511 MCU は 15 ポート（H.323 または SCCP のどちらか一方）を備え、3540 MCU は、30、60、または 100 個のポート（H.323 か SCCP、または両方が混在）を備えています（表 14-3 を参照）。

MeetingPlace Video Integration を使用すると、ユーザは単一の IP/VC MCU でビデオ会議をスケジューリングできます。現時点で、MeetingPlace は複数の MCU やカスケード式ビデオ会議をサポートしていません。他のサードパーティ製 MCU を配置し、MeetingPlace Video Integration ソリューションと統合されない、その他のビデオ会議アプリケーションをサポートすることもできます。

MeetingPlace Video は、システム内の 1 台の MeetingPlace Web MCS 上だけに存在できます。それが、内部と外部のどちらの Web サーバでもかまいません（ただし、どちらか一方）。ビデオ会議は、MeetingPlace Video がインストールされている Web サーバ上だけで可能になり、システム内にある他の Web サーバ上ではサポートされません。音声会議と Web 会議は、すべてのサーバ上でサポートされることに変わりありません。MeetingPlace Video Integration ソフトウェアは、Web Conferencing モジュールと同じ MCS 上に、他の MeetingPlace 統合モジュール（Outlook、Notes、Directory Services など）と一緒に存在できますが、予想される Web ユーザ ライセンスの数と Web サーバの合計数によって異なります。

このソフトウェアは 1 台の Web サーバにしか存在できないので、MeetingPlace Video ソリューションは現時点で冗長性を提供できません。

同じ Cisco Unified Videoconferencing 3540 または 3511 MCU を他の SCCP ビデオ テレフォニー エンドポイントとの MeetingPlace ビデオ統合に使用でき、単一の IP/VC 3540 MCU で ad-hoc ビデオ テレフォニー コール（SCCP 制御）と MeetingPlace H.323 会議の両方をサポートできます。そのような

配置では、MCU 上のいくつかのポートをビデオ テレフォニー用の SCCP のサポートに割り当て、残りのポートで MeetingPlace 用の H.323 をサポートします。IP/VC 3511 MCU では、このデュアル モードがサポートされません。IP/VC 3511 MCU で両方のモードをサポートするには、1 台の 3511 MCU をビデオ テレフォニー用に配置し、別の 3511 MCU を MeetingPlace Video Integration 用に配置する必要があります（表 14-3 を参照）。

表 14-3　SCCP および H.323 用の MCP ポート割り当て

IP/VC-3511-MCU（15 ポート）[1]		IP/VC-3540-MC03A（30 ポート）		IP/VC-3540-MC06A（60 ポート）		IP/VC-3540-MC10A（100 ポート）	
H.323	**SCCP**	**H.323**	**SCCP**	**H.323**	**SCCP**	**H.323**	**SCCP**
100%	0%	100%	0%	100%	0%	100%	0%
0%	100%	50%	50%	75%	25%	70%	30%
		0%	100%	50%	50%	50%	50%
				25%	75%	30%	70%
				0%	100%	0%	100%

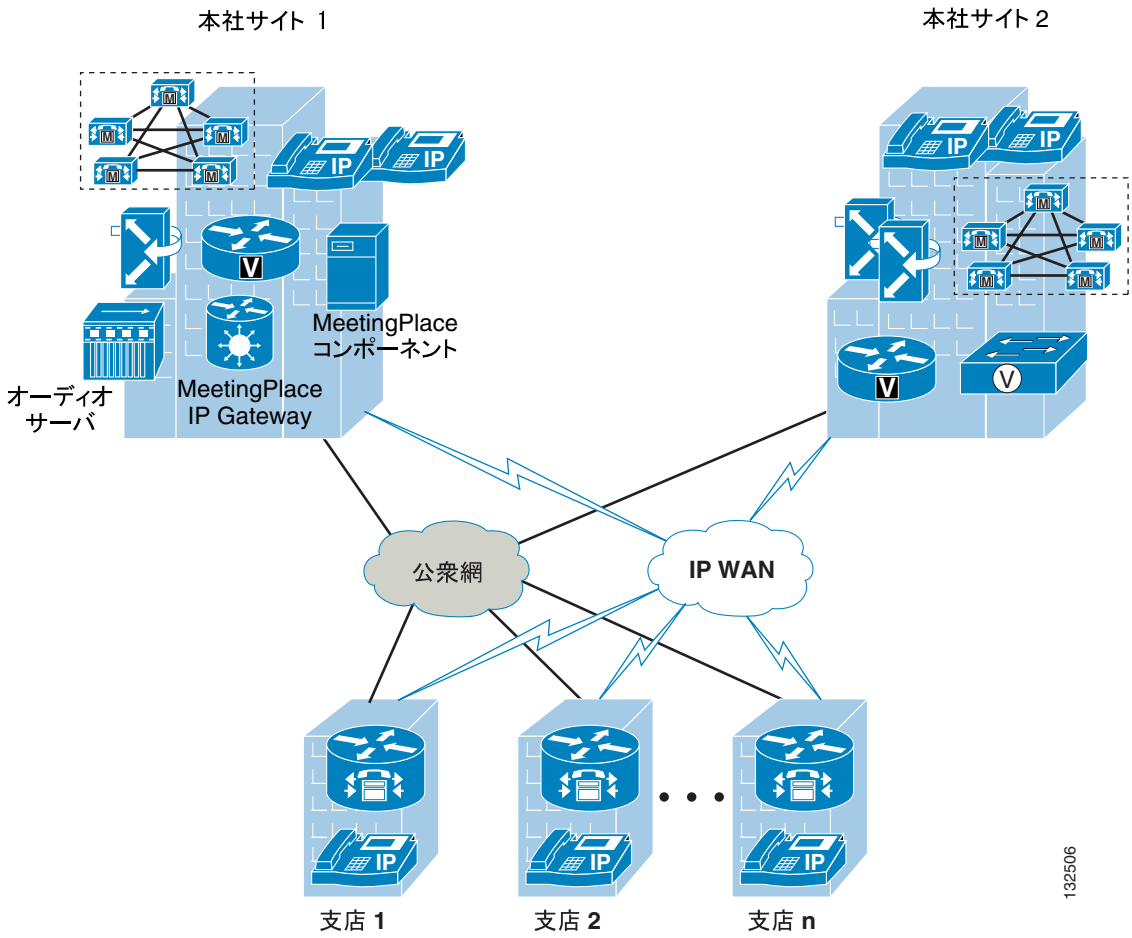
1. この MCU は、128 または 384 kbps で SCCP 用に 16 ポートをサポートします。

MeetingPlace のネットワーク インフラストラクチャ

ここでは、既存の Cisco Unified Communications の企業環境に MeetingPlace 会議ソリューションを構築するために必要となる、ネットワーク インフラストラクチャの要件について説明します。この項の要件は、P.3-1 の「ネットワーク インフラストラクチャ」の章で説明しているネットワーク インフラストラクチャの要件と併せて使用する必要があります。

図 14-3 に、MeetingPlace 会議ソリューションの代表的なネットワーク設定を示します。

図 14-3　代表的な企業 IP テレフォニー ネットワークの MeetingPlace 会議ソリューション



次の各項では、MeetingPlace Audio Server とそのコンポーネントを IP テレフォニー インフラストラクチャに接続するネットワークの主な要件を示します。

- MeetingPlace と IP テレフォニー コンポーネント間の接続（P.14-12）
- Quality of Service（QoS）（P.14-12）

MeetingPlace と IP テレフォニー コンポーネント間の接続

MeetingPlace を IP テレフォニー ネットワークに接続するときは、必ず次のようにしてください。

- スイッチ ポートおよび MeetingPlace コンポーネントを、手動で 100 MB 全二重または 1000 MB 全二重に設定する。
- MeetingPlace の各コンポーネントを物理的に同じ場所に置く。
- MeetingPlace インフラストラクチャと他の IP テレフォニー製品との間に冗長ネットワーク接続を構築し、WAN に障害が発生しても確実に機能するようにする。

Quality of Service（QoS）

ここでは、MeetingPlace に関連する次の QoS メカニズムについて説明します。

- トラフィック分類（P.14-12）
- コール アドミッション制御と帯域幅プロビジョニング（P.14-13）
- ジッタ（P.14-15）

トラフィック分類

トラフィックの分類は、輻輳したネットワークにおける音声品質にとって非常に重要です。音声パケットは、分類またはデータ パケットと区別する必要があり、高いプライオリティで処理される必要があります。音声トラフィックには、ソース位置でマーキングされるものもあれば、ネットワークのエントリ ポイントのできるだけ近くでの分類が必要なものもあります。

MeetingPlace Audio Server のトラフィック分類には、次の特性があります。

- レイヤ 2 Class of Service（CoS; サービス クラス）のマーキングをサポートしない。
- レイヤ 3 音声シグナリングのマーキングをサポートしない。
- Real-Time Transport Protocol（RTP）パケットのソースでのマーキングをサポートする（有効な場合のみ）。

MeetingPlace Audio Server では、次のいずれかのレイヤ 3 の設定を RTP パケットに適用できます。

- IP 優先順位
- Type of Service（ToS; タイプ オブ サービス）
- Differentiated Services Code Point（DSCP、または DiffServ）

（注） IP 優先順位の設定は DSCP 値よりも優先されます。したがって、DSCP 設定を使用する場合は、IP 優先順位と ToS の設定値を手動で **unused** に設定する必要があります。DSCP フィールドに必要な値を設定し、IP 優先順位と ToS を 0 に設定した場合、RTP トラフィックは MeetingPlace Audio Server からマーキングされません。

MeetingPlace Audio Server の内部には、音声シグナリング トラフィックをそのソース位置でマーキングするメカニズムが存在しません。すべての MeetingPlace コンポーネント間のトラフィックは、ネットワークに入るとすぐにマーキングされる必要があります。MeetingPlace コンポーネント間のトラフィックは通常、Gateway System Integrity Manager（GWSIM）アプリケーションからのもので、このアプリケーションは MCS 7800 シリーズ サーバ上にロードされ、常に MeetingPlace 統合ソフトウェア モジュール（Web、Outlook、Notes、Video など）と組み合わされています。このトラフィックが WAN を経由するときは、このトラフィックに他の音声シグナリング トラフィックと同じプライオリティが与えらる必要があります。

他のデバイスと整合性のあるパケット マーキングを使用するようにしてください。詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章を参照してください。

コール アドミッション制御と帯域幅プロビジョニング

MeetingPlace Audio Server および他の MeetingPlace コンポーネントは、独自のコール アドミッション制御メカニズムを持っていません。MeetingPlace Audio Server は、すべてのポートまたはリソースを使い果たすまで、IP コールまたは会議の要求を受け入れることができます。その結果、十分な帯域幅が使用可能でない場合は、所定のリンクを経由するすべてのオーディオ ストリームの音声品質が劣化する可能性があります。

WAN リンクなど、帯域幅に制限のあるリンクを含んだ配置では、コール アドミッション制御を実装する必要があります。コール アドミッション制御の詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章を参照してください。

音声とビデオのレートとコーデックの選択

音声

音声だけの会議では、音声コール用に選択される音声コーデックが、Cisco Unified CallManager でのリージョンの設定によって異なります。Cisco Unified CallManager のリージョン設定で指定されたコーデックは、MeetingPlace Audio Server の設定対象である音声コーデックと一致している必要があります。最も一般的に使用されるコーデックは、G.711 A-law または mu-law と G.729 です。MeetingPlace は、両方のタイプのコーデックをサポートしますが、デフォルトでは G.711 だけが有効になります。G.729 サポートも必要な場合は、Audio Server の初期設定時に有効にする必要があります。

ビデオ

Cisco Unified CallManager Release 5.0 は、H.261、H.263、および H.264 コーデックをサポートしています。ビデオ会議の場合、ビデオ レートを次の場所で設定できます。

- MCU サービス ビュー
- Cisco Unified CallManager リージョン
- MeetingPlace ユーザ プロファイル

MeetingPlace ユーザ プロファイルでの最大ビデオ レートは、384 kbps に設定されます。Cisco Unified CallManager リージョン設定で指定されたビデオ レートは、要求された帯域幅、または MCU か MeetingPlace のユーザ プロファイル内で設定されたビデオ レートが、リージョン設定を超えた場合にのみ有効になります。

たとえば、次のようなビデオ帯域幅の設定を考えてみます。

- Cisco Unified CallManager リージョン：512 kbps
- MCU サービス ビュー：384 kbps
- MeetingPlace ユーザ プロファイル：256 kbps

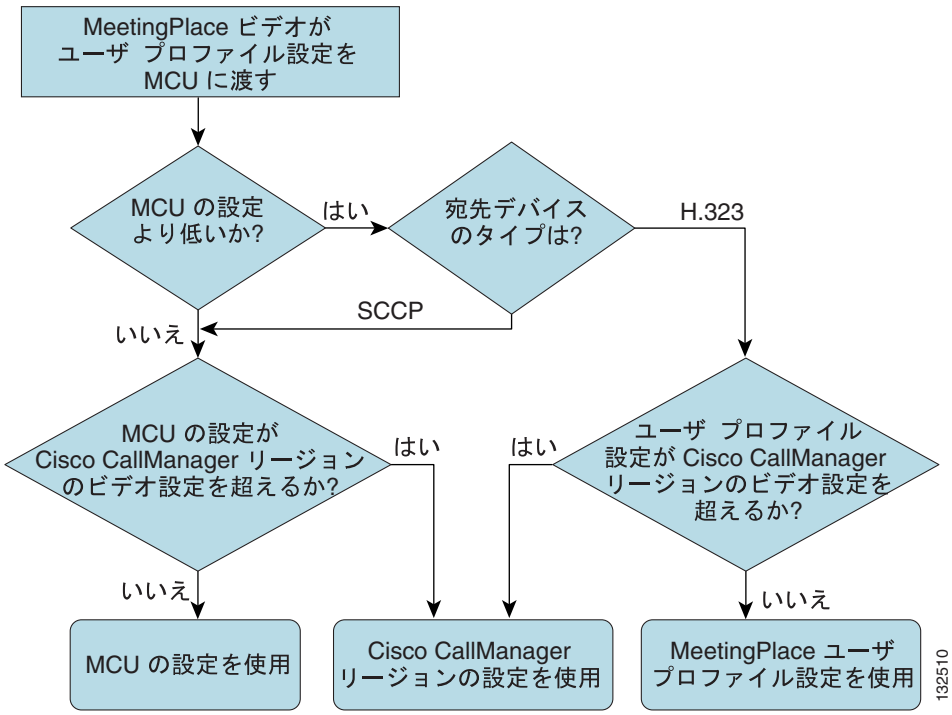
この場合、ビデオ ユーザが MCU にダイヤルインして会議に参加すると、選択されるビデオ レートは 384 kbps となり、MCU サービス ビューでの設定に対応したものになります。MeetingPlace ユーザ プロファイル内のビデオ帯域幅設定は、MeetingPlace Video がコール フローに含まれていないため、有効にはなりません。

ユーザへの発信ダイヤリングでは、MeetingPlace Video アプリケーションは、そのユーザの MeetingPlace ユーザ プロファイル内のビデオ帯域幅値（256 kbps）を MCU に渡します。MCU は、その値を自分のサービス ビュー値（384 kbps）と比較し、低い方の帯域幅値（この例では 256 kbps）

をビデオ会議用として選択し、コール要求を Cisco Unified CallManager ビデオ テレフォニー エンドポイントまたは H.323 ビデオ エンドポイントへ伝達します。コール用として選択されるビデオ帯域幅は、ビデオ エンドポイントによって異なります。Skinny Client Control Protocol（SCCP）ビデオ エンドポイントでは、帯域幅は MCU サービス ビューおよび Cisco Unified CallManager リージョンでのビデオ レート設定に従って選択されます（この例では 384 kbps が選択されます）。ただし、H.323 ビデオ エンドポイントでは、帯域幅が 3 つのビデオ レート設定値のすべてに基づいて選択されます（この例では 256 kbps が選択されます）。

図 14-4 に、ビデオ帯域幅の選択アルゴリズムを示します。

図 14-4　ビデオ帯域幅の選択アルゴリズム



Cisco Unified CallManager のリージョン帯域幅設定（この例では 512 kbps）が有効になるのは、MCU または MeetingPlace Video アプリケーションがリージョン設定より大きな帯域幅（この例では 512 kbps 超）を要求し、エンドポイントがビデオ会議にダイヤルインしたときだけです。エンドポイント ユーザが接続に発信ダイヤル機能を使用した場合は、MeetingPlace プロファイルの帯域幅設定が使用されます。

MeetingPlace Web セッションのネットワーク使用率

MeetingPlace Web セッションは、次の量のネットワーク トラフィックを生成します。

- 参加者は最初に約 1 MB のデータをダウンロードし、セキュリティの注意事項への同意を求められ、ブラウザを閉じてリセットする。
- 各参加者は、会議の開始時に 0.5 ～ 0.75 MB のデータをダウンロードする。
- 平均使用量のベースラインは、参加者あたり約 600 Bytes/ 秒である。

- アプリケーション モードでは、プレゼンターがビューを変更したときに送信されるデータの量は、表示されるカラーとグラフィックの量によって異なる。その場合、次の一般的なガイドラインを適用できます。
  - 複雑度が低いプレゼンテーションは、参加者あたり約 10 kB のデータを送信する。
  - 複雑度が中程度のプレゼンテーションは、参加者あたり約 50 kB のデータを送信する。
  - 複雑度が高いプレゼンテーションは、参加者あたり約 430 kB のデータを送信する。
  - ほとんどのプレゼンテーションは、低から中の範囲である。

Cisco Unified MeetingPlace Web Conferencing は、帯域幅が使用可能であれば 24 ビット カラーを送信し、低速接続の場合は 8 ビット カラーに自動的に低減します。その判断は、まず高いレートで伝送を試み、データが大幅に遅延するか失われる場合にレートを低くするという方法で自動的に行われます。

ジッタ

パケット遅延の変動はジッタと呼ばれ、音声品質に深刻な影響を及ぼす場合があります。ジッタ バッファは、ネットワーク遅延の変動を吸収します。MeetingPlace Audio Server には、ジッタ バッファを設定するための次のパラメータがあります。

- Jitter Buffer Minimum Size：ジッタ バッファは変化するジッタ値に自動的に適応しますが、このパラメータでジッタ バッファの最小値が定義されます。
- Jitter Buffer Optimization：この値は、ネットワーク ジッタに対するジッタ バッファの応答速度を制御します。

ほとんどの場合、これらのパラメータのデフォルト値は変更しないでください。これらの値は、音声品質の問題が実際に発生してから調整します。

ドメイン ネーム システム（DNS）

MeetingPlace Audio Server は、内部で DNS をサポートしていません。実装内にあるすべての MeetingPlace Audio Server コンポーネントと MCS コンポーネントに、静的 IP アドレスを割り当てることをお勧めします。Audio Server は、他のサーバへのアクセスに IP アドレスを使用しようとします。MeetingPlace のコンポーネント（MeetingTime System Administration クライアントなど）は、ホスト名を使用して MeetingPlace Audio Server に接続する場合があります。また、MeetingPlace のコンポーネントは、ホスト名を使用して他の Cisco Unified Communications 製品と通信する場合もあります。

ネットワーク タイム プロトコル（NTP）

MeetingPlace Audio Server は、NTP を使用してクロックをネットワーク タイム サーバと同期します。MeetingPlace Audio Server は、最大 3 台の NTP サーバで設定できます。MeetingPlace の Windows ベースのコンポーネントは、w32time.exe サービスを使用して NTP クライアントまたはサーバとして機能できます。すべてのコンポーネントでクロックが同期されるように、企業ネットワーク全体で NTP サーバを 1 台だけ使用することを強くお勧めします。

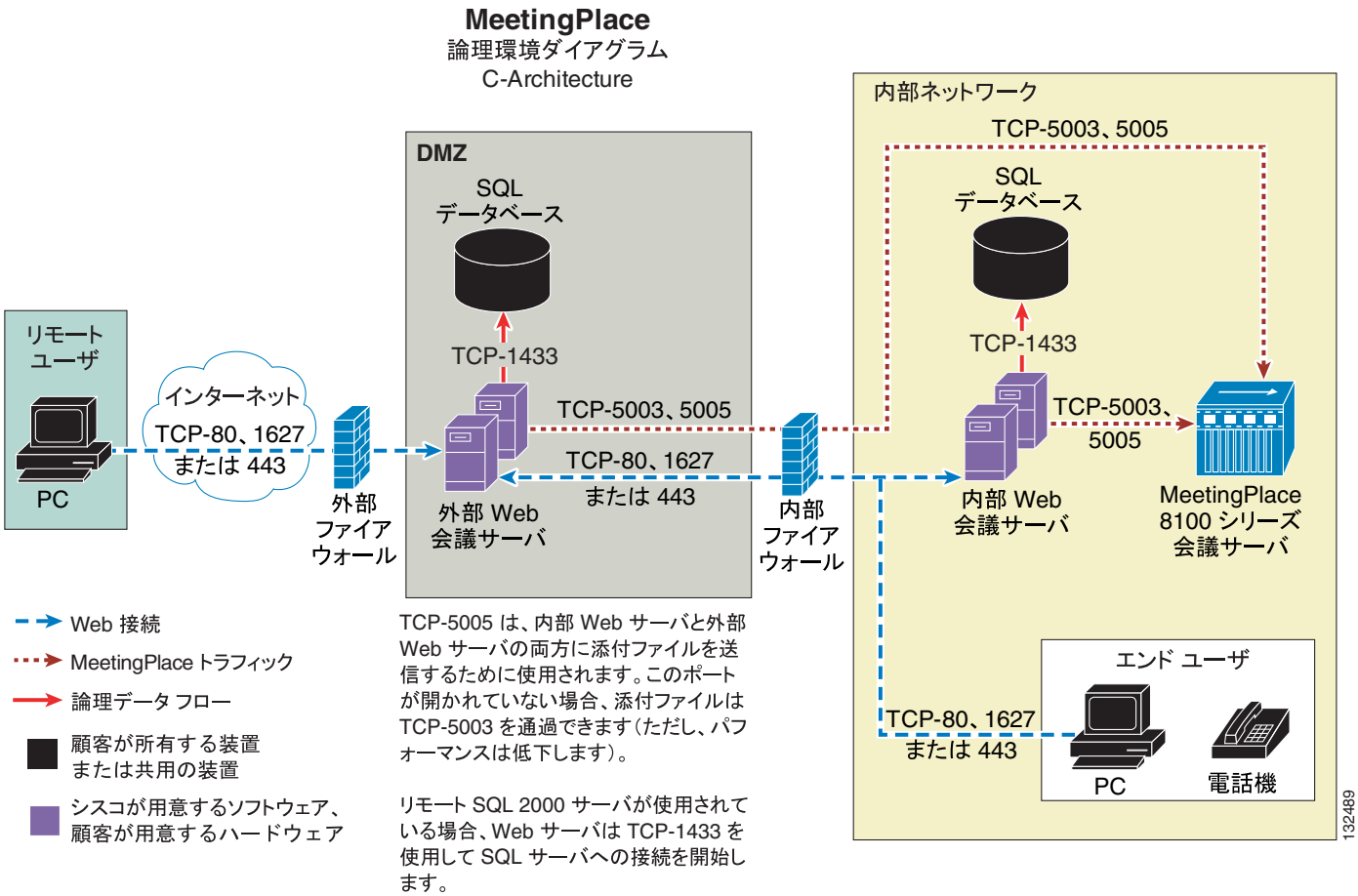
非武装地帯（DMZ）の要件

DMZ に配置された MeetingPlace コンポーネントにより、外部ユーザは会議にアクセスできます。外部ユーザが Web 会議にアクセスできるようにするには、独立した MeetingPlace Web サーバを DMZ に配置することもできます。その場合でも、内部ユーザは内部 MeetingPlace Web サーバを使用して非公開の会議を行えます。

DMZ 配置では、内部ユーザが完全な Web アクセスおよび MeetingPlace 機能（スケジューリング、検索、参加、添付ファイルへのアクセス、および記録）を使用できるのに対し、外部ユーザは会議への参加だけを許可されます。会議が開始されると、内部ユーザは外部 Web サーバに転送されます。

図 14-5 は、このタイプの配置を示しています。

図 14-5　外部ユーザ用の DMZ がある MeetingPlace Web 会議



DMZ 内の MeetingPlace コンポーネントが、ファイアウォールなどのセキュリティ ポリシーによって内部 MeetingPlace コンポーネントから分離されている場合は、統合が正しく機能するように、そのファイアウォールで特定の TCP ポートまたは UDP ポートを開く必要があります。

DMZ から内部ネットワークにポートを開く必要はありませんが、内部ネットワークから DMZ に次のポートを開く必要があります。

- TCP 80 または 443（Web 会議用）
- TCP 5003（双方向、Audio Server と Web サーバの間の通信用）

- TCP 5005（添付ファイルと記録用）
- TCP 1503（Microsoft NetMeeting 用、省略可能）
- TCP 1627（Web 会議のパフォーマンス向上用、省略可能）

DMZ とインターネットとの間では、次のポートが開かれます。

- TCP 80 または 443
- TCP 1503（Microsoft NetMeeting 用、省略可能）
- TCP 1627（Web 会議のパフォーマンス向上用、省略可能）

DNS サービスは、次の理由から分割する必要があります（1 台は内部 DNS サーバ、もう 1 台は外部 DNS サーバ）。

- 使いやすさ：1 回のクリックだけで、内部と外部のユーザが会議に参加できます。
- セキュリティ：外部ユーザは内部ネットワークに関する情報にアクセスできません。
- パフォーマンスの向上：この配置では、外部 DNS サーバに内部要求の負荷がかかりません。

内部 DNS サーバは社内ネットワークの内部からの照会だけを解決し、外部 DNS サーバは、会社のドメインの公的にアドレス指定可能なエンティティを保持します。各 DNS サーバは、URL と IP アドレスの両方をマップする必要があります。

（注） IP アドレスがデータに組み込まれているため、MeetingPlace Audio Server と他の MeetingPlace コンポーネントとの間では、NAT はサポートされません。

表 14-4 は、MeetingPlace Audio Server とそのコンポーネントが使用するすべての TCP ポートと UDP ポートを示しています。

表 14-4　MeetingPlace Audio Server が使用する TCP ポートと UDP ポート

TCP または UDP ポート	プロトコルやアプリケーション
TCP 21	FTP
TCP 23	Telnet
TCP 25	MeetingPlace Email Gateway と SMTP サーバとの間
TCP 161	簡易ネットワーク管理プロトコル（SNMP）
TCP 389	MeetingPlace Directory Services Gateway と企業の社内ディレクトリとの間
TCP 443	Secure Socket Layer（SSL）
TCP 1443	MeetingPlace データベース
TCP 1627	会議に WebShare を収容するための直接着信アクセス
TCP 3336	Cisco Unified MeetingPlace Video と IP/VC MCU の統合
TCP 5001	Cisco MeetingTime（クライアントから Audio Server に対して開かれる）
TCP 5003	Cisco Unified MeetingPlace Gateway System Integrity Manager（SIM）
TCP 5005	Audio Server と Cisco Unified MeetingPlace Web またはゲートウェイとの間のファイル転送（クライアントからサーバに対して開かれる）
UDP 53	DNS
UDP 123	ネットワーク タイム プロトコル（NTP）

相互運用性プロトコル

ここでは、MeetingPlace Audio Server とそのコンポーネントが、他のシスコ製品との相互運用性を得るために使用する通信プロトコルについて説明します。Cisco Unified MeetingPlace 会議ソリューションとの相互運用性には、次に示す最大 2 つまでのネットワークとの統合が含まれます。

- IP ネットワーク

  MeetingPlace コンポーネント（MeetingPlace H.323/SIP IP Gateway、MeetingPlace Web サーバ、および MeetingPlace Video アプリケーション）は、他の製品に直接統合されます。また、MeetingPlace コンポーネントは MeetingPlace Audio Server と通信します。
- 公衆電話交換網（PSTN）

  MeetingPlace Audio Server は、Audio Server 上の TDM インターフェイスを通じて他の製品と直接統合されます。

IP ネットワーク

ここでは、MeetingPlace コンポーネントを IP ネットワークと統合するために使用されるプロトコルについて説明します。次のタイプのプロトコルがあります。

- MeetingPlace Audio Server がサポートするプロトコル（P.14-18）
- その他の MeetingPlace コンポーネントがサポートするプロトコル（P.14-19）

MeetingPlace Audio Server がサポートするプロトコル

MeetingPlace Audio Server は、次のプロトコルまたはアプリケーションを使用して IP 通信システムに統合されます。

GWSIM

Gateway System Integrity Manager（GWSIM）は、MeetingPlace Audio Server とそのコンポーネントの間のインターフェイスとして機能する専用アプリケーションです。Cisco Unified MeetingPlace GWSIM はクライアント / サーバ アーキテクチャに基づいており、リモート MeetingPlace コンポーネントと情報を交換する手段が提供されます。MeetingPlace Audio Server は、System Integrity Manager（SIM）を使用してすべての会議情報を管理します。SIM は IP ネットワークを使用して、MeetingPlace コンポーネント上にインストールされた GWSIM エージェントとの間で、すべてのシグナリングおよび会議情報を交換します。この通信には TCP ポート 5001 および 5003 を使用するシスコ専用のプロトコルが使用され、一般的に GWSIM 通信と呼ばれます。

Real-time Transport Protocol（RTP）

MeetingPlace Audio Server は、エンドポイント（IP Phone、IP/VC MCU など）への直接的なリアルタイム オーディオの伝送に UDP を使用します。RTP に最も一般的に使用されるコーデックは、G.711 と G.729 ですが、MeetingPlace Audio Server は G.722、G.723、G.726、G.728、GSM、GSM-EFR、および QCELP もサポートします。Audio Server は、デフォルトでは RTP に G.711 コーデックだけを使用できるように設定されます。ただし、コマンドライン インターフェイスを使用すると、このデフォルトを必要なコーデックに変更できます。

MeetingPlace Audio Server で H.323 と SIP をサポートするには、MeetingPlace H.323/SIP IP Gateway を使用する必要があります。

その他の MeetingPlace コンポーネントがサポートするプロトコル

ここでは、MeetingPlace Audio Server 以外の MeetingPlace コンポーネントと IP 通信ネットワークとの統合に使用されるプロトコルについて説明します。

H.323

H.323 ネットワークを MeetingPlace と統合すると、機能が豊富な会議ソリューションが得られます。すでに述べたように、MeetingPlace Audio Server は H.323 をネイティブでサポートするわけではないので、H.323 プロトコルをサポートするには MeetingPlace H.323/SIP IP Gateway が必要です。Cisco Unified MeetingPlace H.323/SIP IP Gateway は H.323 をサポートし、ネットワーク内にあるその他の H.323 エレメントと直接通信します。これにより、Audio Server を使用した会議が可能になります。

MeetingPlace H.323/SIP IP Gateway は、H.323 を使用して Cisco Unified CallManager または Cisco Unified CallManager Express と直接統合されます。MeetingPlace H.323/SIP IP Gateway が同時に処理できる H.323 コールの数は、Audio Server の最大 IP ポート制限で決まります。オプションとして、ゲートキーパーを Cisco Unified CallManager または CallManager Express に統合し、アドレス解決と帯域幅制御に使用することもできます。

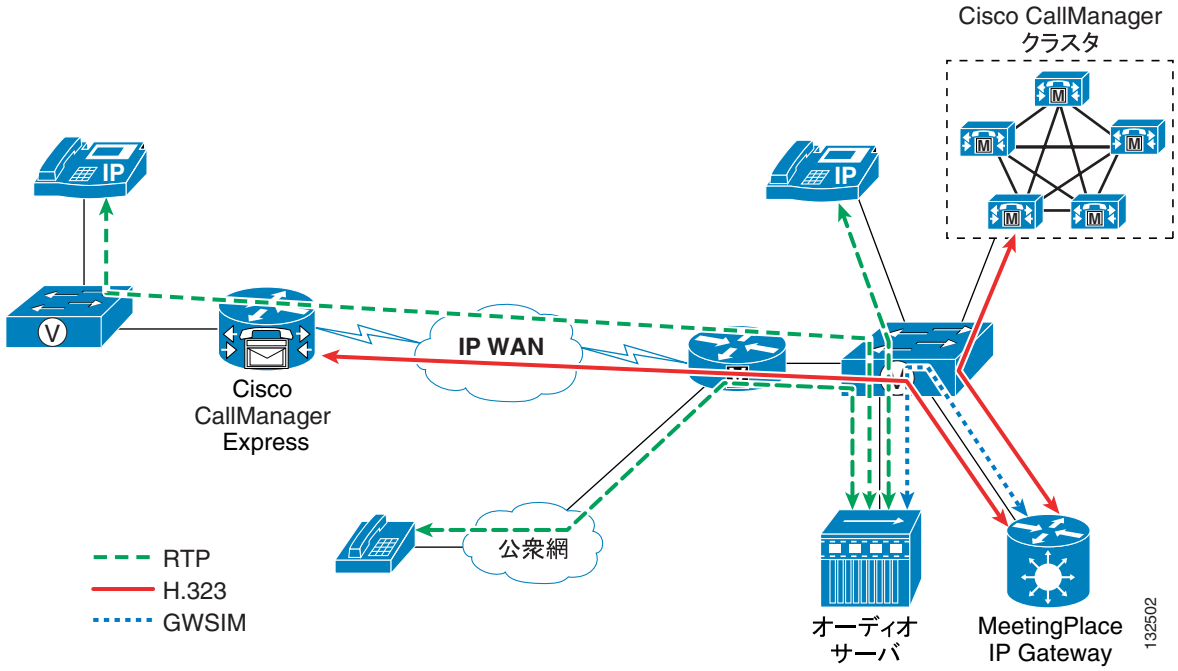
MeetingPlace H.323/SIP IP Gateway は次の TCP ポートと UDP ポートを、ここに示した目的に使用します。

- H.323
  - H.225 用のコール セットアップは、静的 TCP ポート 1720 を使用します。
  - H.245 用のコール セットアップは、アドレス範囲 1024 ～ 65535 の TCP ポートをランダムに使用します。
  - RTP 音声ストリームは、5000 ～ 65535 の範囲の UDP ポートをランダムに使用します。
- ゲートキーパー
  - Registration Admission Status（RAS）用に静的 UDP ポート 1719 が必要です。

（注）　MeetingPlace H.323/SIP IP Gateway は、H.323 Fast Start をサポートしません。ただし、着信 H.323 fast-start コールを受信した場合でも、そのコールは通常の H.323 シグナリング手順を使用して完了します。

図 14-6 は、MeetingPlace with Cisco Unified CallManager と CallManager Express の相互運用性を示しています。

図 14-6　H.323 を使用した Cisco Unified CallManager と CallManager Express との統合



SIP

MeetingPlace H.323/SIP IP Gateway は、Session Initiation Protocol（SIP）ネットワークを Cisco Unified MeetingPlace Audio Server に相互接続する機能も備えています。MeetingPlace H.323/SIP IP Gateway は、SIP プロキシ サーバまたは SIP ゲートウェイと直接統合され、SIP メッセージを GWSIM メッセージに変換します。その結果、SIP エンドポイントは MeetingPlace Audio Server を会議に使用できます。

Cisco Unified CallManager Release 5.0 以降では、Cisco Unified CallManager 上の SIP トランクを使用して、MeetingPlace H.323/SIP IP Gateway と直接統合できます。Cisco Unified CallManager と MeetingPlace H.323/SIP IP Gateway との間で SIP トランクを使用するには、次の 3 つの重要な要件があります。

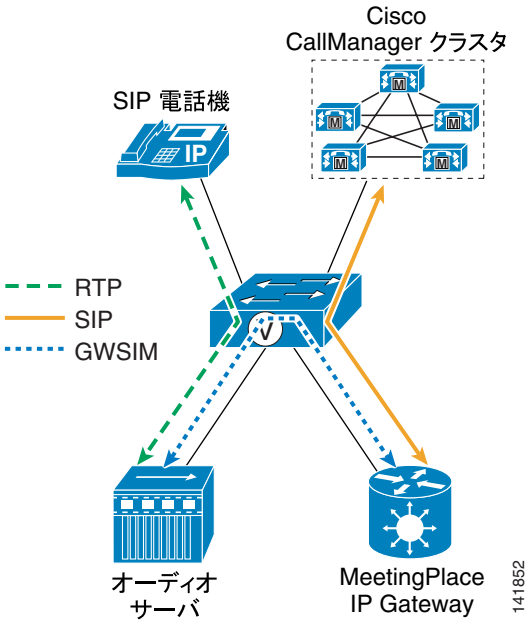
- メディア ターミネーション ポイント（MTP）を使用する必要があります。
- 静的に有効にされた MTP が必要なため、G.711 コーデックだけがサポートされます。
- UDP Transport を使用する必要があり、TCP はサポートされません（UDP Transport を使用して別個の SIP セキュリティ プロファイルを作成する必要があります）。

MeetingPlace H.323/SIP IP Gateway は次の UDP ポートを、SIP に使用します。

- コール セットアップは静的 UDP ポート 5060 を使用します。
- RTP 音声ストリームは、5000 ～ 65535 の範囲の UDP ポートをランダムに使用します。

図 14-7 は、MeetingPlace と Cisco Unified CallManager との相互運用性を示しています。

図 14-7　SIP 統合



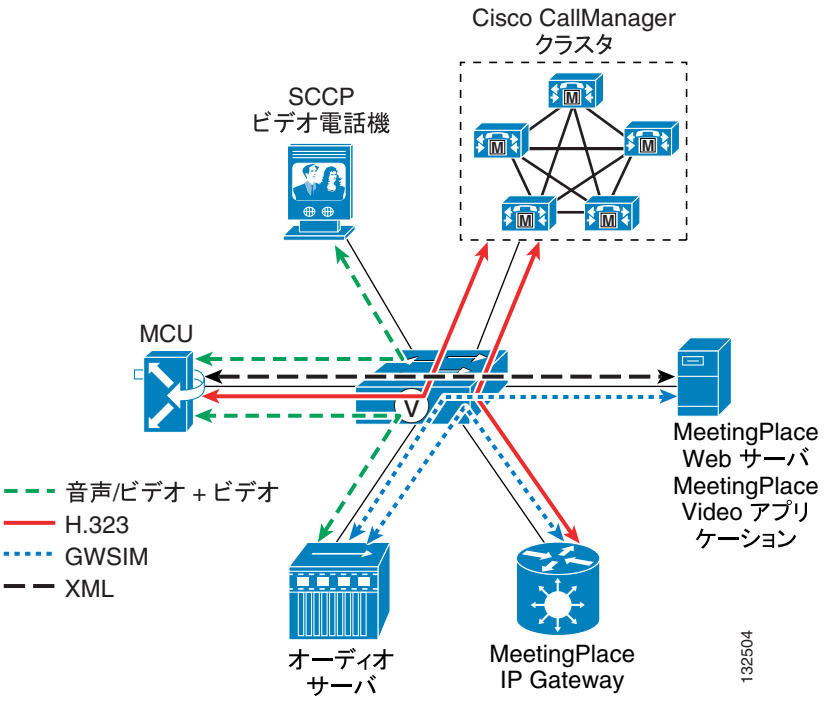
(注)　MeetingPlace H.323/SIP IP Gateway は、H.323 接続と SIP 接続を同時にサポートできます。

XML アプリケーション

MeetingPlace Audio Server はオーディオ通信だけを処理できます。ビデオ会議をサポートするには、IP/VC Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）と直接統合される外部 MeetingPlace Video アプリケーションが必要です。Cisco Unified MeetingPlace Video Integration は、TCP ポート 3336 を介した XML メッセージングを使用して Cisco Unified Videoconferencing MCU と通信します。

図 14-8 は MeetingPlace と IP/VC MCU との相互運用性を示しています。

図 14-8　ビデオ統合



公衆電話交換網（PSTN）

Cisco Unified MeetingPlace Audio Server は、デジタル（T1 か E1）またはアナログのトランクを使用して、公衆網に直接接続するか、または PBX を介して接続します。また、MeetingPlace Audio Server には、音声ゲートウェイに接続した Cisco Unified CallManager を介して、公衆網からも到達可能です。

デジタル トランク

Cisco Unified MeetingPlace は、次の各項で説明するように、T1 および E1 のデジタル トランクをサポートしています。

T1

Cisco Unified MeetingPlace は、T1 デジタル トランク用に次のプロトコルをサポートしています。

- T1-CAS（ループ スタート、ウィンク スタート、またはグラウンド スタート）
- T1-PRI（AT&T PRI、Nortel PRI、または Bell PRI）

T1 Smart Blade は、公衆網または PBX から直接接続された T1 をサポートします。マルチアクセス ブレード（MA-4 または MA-16）は、PBX または公衆網への T1-PRI または E1-PRI デジタル接続をサポートします。デジタル回線用のフレーム構成は、Extended Superframe（ESF; 拡張スーパーフレーム）または D4 フレーミングが可能です。デジタル回線には、Binary 8-Zero Substitution（B8ZS）または Alternate Mark Inversion（AMI; 交互マーク反転）コーディングを使用できます。

（注）　ESF フレーム構成と B8ZS コーディングを使用するようにしてください。

通常、デジタル接続には E&M またはグラウンド スタート（GST）シグナリングが用意されています。E&M シグナリング用に設定された T1 回線上では、MeetingPlace は Direct Inward Dial（DID/DDI; ダイヤルイン）または Dialed Number Identification Service（DNIS; 着信番号識別サービス）の着信番号情報だけを受信できます。MeetingPlace は着信番号情報を使用して、発信側を会議へ直接接続するか、発信側がアクセスできる MeetingPlace サービスを判別します。

Cisco Unified MeetingPlace は、フラクショナル T1 サービスもサポートします。

E1

Cisco Unified MeetingPlace は、E1 デジタル トランク用に次のプロトコルをサポートしています。

- Euro-ISDN（ETSI 300-102）
- QSIG（ECMA バージョン）：チャネルには 1 ～ 30 の番号が付きます。
- QSIG（ETSI バージョン）：チャネルには 1 ～ 15 および 17 ～ 31 の番号が付きます。

（注） Cisco Unified MeetingPlace システムは、E1-PRI プロトコルだけをサポートします。E1-CAS プロトコルはサポート *しません*。

それぞれの E1 プロトコルは、シグナリング オプションのソフトウェア設定が可能です。シグナリング オプションは、PBX または公衆網スイッチ上に設定されたオプションと一致している必要があります。

（注） MeetingPlace Audio Server 上ではプロトコルの混在がサポートされません。ただし、IP ポートと組み合せた場合は除きます。たとえば、Cisco Unified MeetingPlace Audio Server では、同じシステム上に T1 ポートと E1 ポートの両方を設定できませんが、T1（PRI または CAS）ポートと IP ポートを設定したり、E1 ポートと IP ポートを設定したりすることはできます。また、Cisco Unified MeetingPlace Audio Server では、同じシステム上に T1-CAS ポートと T1-PRI ポートの両方を設定することはできません（表 14-5 ～表 14-7 を参照）。

表 14-5　T1 ポートと IP ポートのある混在システムのポート キャパシティ

IP ポート数	0	96	192	240	480	576	600	960
T1 DS0 の最大数	1152	960	768	576	576	394	192	0
合計ポート数	1152	1056	960	816	1056	960	792	960

表 14-6　T1-PRI ポートと IP ポートのある混在システムのポート キャパシティ

IP ポート数	0	120	400	480	960
PRI ポートの最大数	736	368	368	368	0
合計ポート数	736	488	768	848	960

表 14-7　E1 ポートと IP ポートのある混在システムのポート キャパシティ

IP ポート数	0	120	384	480	960
E1 ポートの最大数	960	480	480	480	0
合計ポート数	960	600	864	960	960

詳細については、『*Getting Started Guide for Cisco Unified MeetingPlace Audio Server*』および『*Configuration Guide for Cisco Unified MeetingPlace Audio Server*』を参照してください。どちらも次の Web サイトから入手可能です。

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/index.htm

会議

Cisco Unified MeetingPlace は、次のタイプの会議をサポートします。

- オーディオ会議（P.14-25）
- Web 会議（P.14-28）
- ビデオ会議（P.14-30）

オーディオ会議

MeetingPlace Audio Server 用としては、次の 2 つのプラットフォームがあります。

- Cisco Unified MeetingPlace 8106 Audio Server
  - 最大 480 の IP ポート（増分の単位は 24 または 30 ユーザ ライセンス）
  - 最大 536 の T1-CAS ポート（増分の単位は 24 ユーザ ライセンス）
  - 最大 480 の T1-PRI ポートまたは E1 ポート（増分の単位は 24 ユーザ ライセンス）
- Cisco Unified MeetingPlace 8112：最大 960 の IP ポートをサポート
  - 最大 960 の IP ポート（増分の単位は 24 または 30 ユーザ ライセンス）
  - 最大 1152 の T1-CAS ポート（増分の単位は 24 ユーザ ライセンス）
  - 最大 960 の T1-PRI ポートまたは E1 ポート（増分の単位は 24 ユーザ ライセンス）

同時会議の最大数は、ポート数を 2 で割った数になります。サーバは、1 つの会議あたり最大 550 セッション（参加者）をサポートします。ただし、最大で 3 台の Audio Server にカスケード接続することにより、1 つの会議で合計 1650 オーディオ セッションを確立できます。

コール フロー

メディア ストリームが MeetingPlace Audio Server と IP Phone の間を直接流れる場合、メディア要求（シグナリング）は、MeetingPlace Audio Server に代わって MeetingPlace H.323/SIP IP Gateway で処理されます。図 14-9 は着信コールのコール フロー、図 14-10 は発信コールのコール フローをそれぞれ示しています。

図 14-9　Cisco Unified CallManager と統合された MeetingPlace のオーディオ ダイヤルイン コール フロー

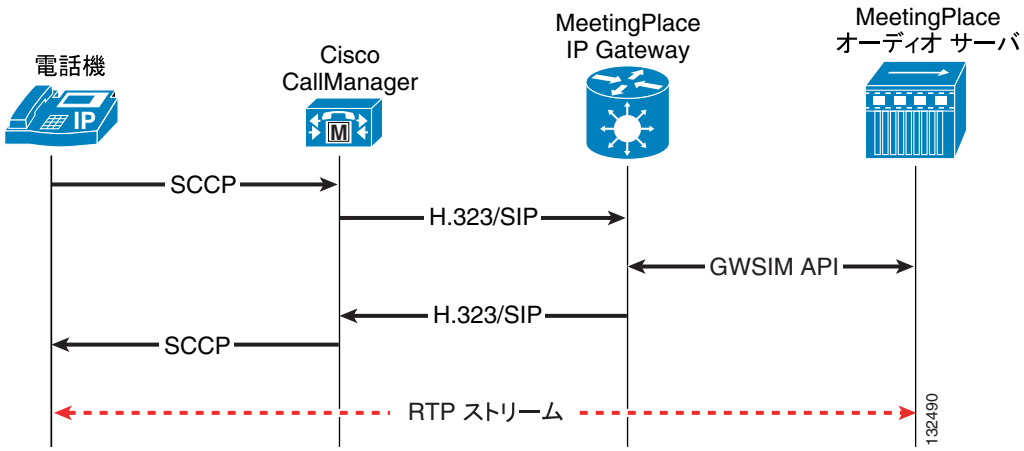
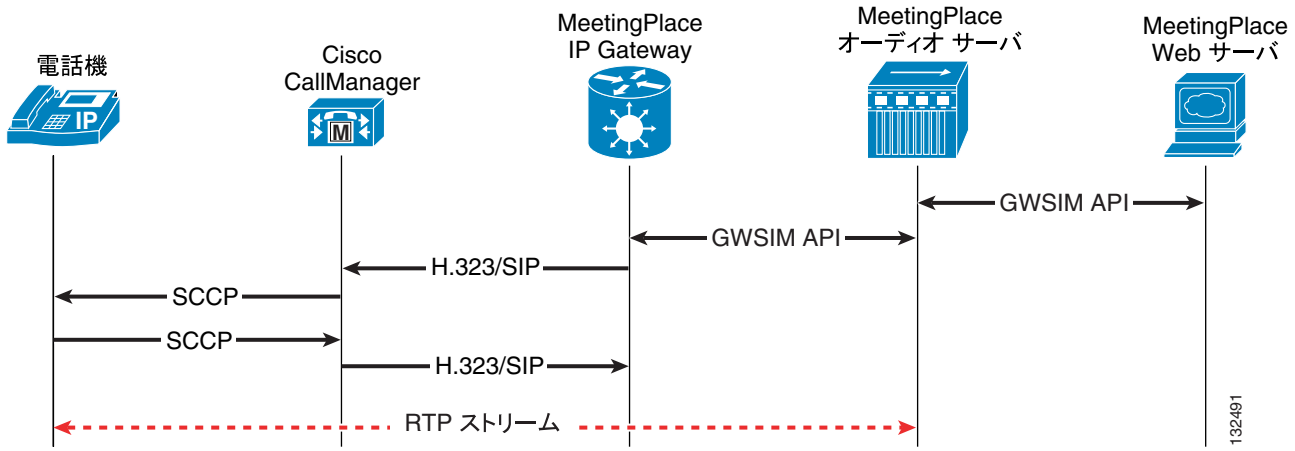


図 14-10　Web インターフェイスからのオーディオ発信ダイヤル コール フロー



会議のタイプ

MeetingPlace は、次に示す 2 つの主要なタイプのオーディオ会議をサポートしています。

- 標準の（スケジュール済み）会議

  この種の会議をスケジューリングするときは、会議 ID、参加者数など、会議のパラメータを指定できます。参加者が参加すると、メイン会議に直接接続されます。即時会議は、リソース予約の点では基本的にスケジュール会議で、唯一の違いは開始時間です（将来ではなく、すぐに開始されます）。

- 予約なしの会議

  すべてのプロファイル ユーザは、電話機から予約なしの会議を開始できます（機能が有効な場合）。ユーザは、プロファイル ID とパスワードを使用してサイン インする必要があり、それによって会議が開始されます。データベースには、誰が会議を開始したのかに関する情報も格納されます。

予約なしモードは、システム全体のパラメータとユーザ グループ パラメータの両方です。システム全体に対してオンし、特定のエンド ユーザ セットに対してオフすることができますが、その逆はできません。このパラメータは、参加者が会議に参加したときに再生されるプロンプトを変更します。

両方のタイプの会議が同じ MeetingPlace Audio Server 上に存在でき、同じ会議ポート プールを共有します。予約なしモードを有効にしても、標準タイプの会議を同時にスケジューリングする機能は影響を受けません。ただし、予約なし会議では、自動的にユーザのプロファイル番号が会議 ID として設定されます。したがって、予約なしモードを有効にした場合、ユーザ プロファイル番号は予約済みとなり、手動で標準スケジュール会議用の会議 ID として割り当てることができなくなります。

ポート管理

MeetingPlace Audio Server は、次のタイプのポートを提供します。

- アクセス ポート

  スケジューリング、参加、および記録済み会議の受信用に予約されています。
- 会議ポート

  会議で使用中または予約済みのポートです。会議ポートは、次のタイプの特殊用途ポートも含んでいます。
  - 非常用ポートは、自動転送の処理用に予約されている会議ポートです。このポートは常にシステムで予約され、会議参加者が会議中に連絡窓口または係員に連絡して支援を受けたり、システム管理者が会議にダイヤルインできるようになっています。
  - フローティング ポートは、予期しなかった会議参加者を処理するために設定されます。このポートは特定の会議用に固定されず、すでに満杯の会議に追加参加者が出たときに不足を補います。
- 過剰予約ポート

  このポートは、物理的に存在しません。スケジュール済み会議では、予約されていても未使用のポートが存在するのが一般的であるという前提に基づいて、実際に使用可能な数よりも多くのポートをスケジューリングできるようにするために設定されるソフトウェア ポートです。このポートは物理的には存在しないので、設定可能な数に制限はありません。

スケジューリング

オーディオ会議は、次のインターフェイスでスケジューリングすることができます。

- MeetingPlace Web ユーザ インターフェイス（UI）
- Email Calendar Integration（Outlook または Lotus Notes）
- MeetingTime クライアント
- Cisco Unified IP Phone XML Service

オーディオ会議のカスケード化

会議のカスケード化は、*マルチサーバ会議*とも呼ばれます。この機能は、さまざまな MeetingPlace システムの間に仮想リンクを提供し、各サーバ上のユーザが同じ会議に参加しているかのように通信できます。ユーザがマルチサーバ会議をスケジューリングするときは、プライマリ サーバ上の Web スケジュールを使用して、会議に必要なセカンダリ サーバを選択します。会議の開始時に、プライマリ サーバは各セカンダリ サーバにコールを発信します。セカンダリ サーバは、参加者がシステムにダイヤルインした場合と同じように、プライマリ サーバを会議に追加します。

1 つの会議に対して、最大 3 台の Audio Server をカスケードできます。

すべての MeetingPlace Audio Server 上にある NTP サーバが、すべてのサーバ間で時刻を同期するように設定することをお勧めします。

マルチサーバ会議の詳細については、次の Web サイトで入手可能な『*Administrator's Guide for Cisco Unified MeetingPlace Audio Server*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/index.htm

ビデオ エンドポイントを使用したオーディオ専用会議へのダイヤルイン

ビデオ エンドポイントは、MeetingPlace Audio Server に直接ダイヤルインすることにより、オーディオ専用会議に参加できます。MeetingPlace は、エンドポイントからのアウトオブバンドとインバンドの両方の DTMF 番号をサポートします。Web サーバから発信ダイヤル機能を使用する場合、ユーザはオーディオ エンドポイントの電話番号ボックスにビデオ エンドポイントの内線番号を入力する必要があります。

ヒント　Polycom H.323 デバイスの場合、ユーザが最初に # キーを押すと、画面に小さな電話機キーパッドが表示されます。Polycom デバイスはインバンド DTMF 番号を送信します。この番号は、G.711 コーデックを使用しているときにのみ機能します。

Web 会議

Web 会議には、次の MeetingPlace コンポーネントが関係します。

- MeetingPlace Web サーバ（P.14-28）
- SQL データベース（P.14-29）

MeetingPlace Web サーバ

MeetingPlace Web アプリケーションは、主に次のような機能を提供します。

- MeetingPlace Web ユーザ インターフェイス

  この機能は、スケジューリング、会議室、会議コントロール、リファレンス センター、およびアカウント管理を提供します。
- MeetingPlace Web 会議

  この機能は、コラボレーション、ホワイトボード、アプリケーション共有、ファイル アップロードなどを提供します。
- オーディオ ファイルの変換

  MeetingPlace Web は、オーディオ サービス オプション付きでインストールされた場合、最初に MeetingPlace の音声（.mpv）ファイルを .wav 形式に変換します。その後、Windows Media（.wma）、RealAudio（.ra または .rm）、MP3 など、それ以外のサポートされているオーディオ形式に変換することもできます。そのようなファイルは、ダウンロードして他のアプリケーション（カスタム Web サイトや CD など）から使用可能にすることができます。
- 同期オーディオ Web 記録

  オプションの音声および Web 記録がシステム上で有効な場合は、.wav ファイルを MeetingPlace Web で使用し、同期オーディオ /Web 記録を作成できます。

MeetingPlace Web は、Media Convergence Server（MCS）と IIS サービスが稼働している必要があり、MeetingPlace 8100 Audio Server マスター データベースと自動的に同期する Microsoft SQL データベースを使用します。

Cisco MCS 7835 サーバは最大 50 までの同時ユーザ セッションをサポートし、MCS 7845 は、最大 200 までの同時ユーザ セッションをサポートしますが、1 つの会議あたり 150 ユーザ セッションという制限があります。さらに、アプリケーション共有には 100 の同時 Web 会議という制限や、単一の Web サーバ上のプレゼンテーション モードには 150 までという制限もあります（プレゼンテーション モードにはアップロードされたプレゼンテーションが含まれ、そのプレゼンテーションは JPEG 形式に変換されて、それぞれ参加者が Web 会議に参加すると、ローカル ブラウザのキャッシュに個別にダウンロードされます）。

100 を超える Web 会議ユーザ ライセンスの配置では、Microsoft Desktop Engine（MSDE）2000 を使用しないでください。スケジューリングと Web 会議のための同時接続が 8 つまでに制限されているためです。SQL 2000 が必須となり、お客様が用意する必要があります。大規模なインストレーション（500 を超えるユーザ ライセンス）では、専用のサーバで SQL 2000 を実行してください。

キャパシティとロード バランシングの点でパフォーマンスを向上するには、MeetingPlace Web サーバをいくつかのクラスタにグループ化します。MeetingPlace Web クラスタは、最大で 6 つの Web サーバを内部構成または外部構成でサポートできます。

(注) シスコまたはサードパーティ製の Web バランシング製品を、MeetingPlace ソリューションと組み合せて使用しないでください。MeetingPlace Web には正しい Web バランシング機能が製品に組み込まれており、他のバランサーはこのアプリケーションとの組み合せで機能しません。

クライアントは、HTTP または HTTP over Secure Socket Layer（HTTPS）を介して MeetingPlace Web に接続できます。MeetingPlace Web サーバ上では、次の宛先ポートが使用されます。

- TCP ポート 5003 は、GWSIM を介して MeetingPlace Audio Server と通信するために使用されます。
- TCP ポート 5005 は、添付ファイルと記録に使用されます。
- TCP ポート 80 または 443 は、スケジューリングと Web ページの表示に使用されます。
- TCP ポート 1627（開いていない場合はポート 80 を通じたトンネル）または 443 は、そのサーバに Secure Socket Layer（SSL）が配置されていると、Web 会議に使用されます。MeetingPlace Web サーバに配置するには、SSL 認証を用意する必要があります。

SQL データベース

Web サーバ上の Microsoft SQL データベースには、プロファイル情報と会議情報が格納されます。会議情報のタイプは、Web サーバが内部（すべての内部および外部会議を収容）か外部（外部会議だけを収容）かによって異なります。プライマリ データベースは、Audio Server 上に置かれます。会議がスケジューリングされると、その会議情報は該当する Web サーバにもコピーされます。これにより、すべての要求が Audio Server を通過しなくても、特定の機能を容易に実行できるようになります。

MeetingPlace 5.3 からは、データベースに次のデータが含まれます。

- キャッシュされた MeetingPlace データ
- Web サーバ / サイトの設定データ
- Microsoft Outlook および Lotus Notes が、新規の短い Click-To-Attend リンクを長いリンクに変換するために使用するテーブル
- Web ユーザ インターフェイスで使用される英語および各国語のほとんどの文字列
- システム管理者がカスタマイズした文字列
- WebPoll とその結果

Microsoft Outlook と Lotus Notes は、データベースを直接には使用しません。Click-To-Attend リンクを格納するように MeetingPlace Web に要求してから、そのリンクを使用して会議に参加します。

MeetingPlace Video は、SQL データベースをまったく使用しません。

(注) Cisco Security Agent は、現時点ではすべての MeetingPlace サーバに対してサポートされているわけでは*ありません*が、シスコ認定のウィルス保護プログラムはサポートされています。

会議のタイプ

MeetingPlace Web アプリケーションは、次のタイプの Web 会議をサポートします。

- オープン フォーラム会議

  各参加者は、同様に話したり聞いたりすることができます。
- 講義形式の会議

  大部分の参加者はデフォルトで聴取者として参加でき、1 人または複数の指定された話者が存在します。聴取者は、会議中に話すことができません。
- 即時会議

  この会議は、デフォルトのシステム パラメータを使用してスケジューリングされます。このスケジューリング方式では、ユーザが独自の会議パラメータを指定することは許可されません。
- 予約なしの会議

  このタイプの会議では、前もってリソースを予約したり会議 ID を割り当てる必要がありません。このタイプの会議を開始するには、事前に MeetingPlace Audio Server を予約なしモードに設定する必要があります。予約なし会議の参加者は、会議の議長が会議にログインするまで待合室に入れられます。待合室内の参加者が互いに話すことはできません。
- 連続会議

  常時使用可能な連続会議を（MeetingTime クライアントで）設定できるのは、システム管理者だけです。この会議ポートはこの会議専用であり、オーディオ システムのスケジューリング タスクから使用することはできません。
- すべてのポートを予約

  この機能は、システム管理者が、MeetingPlace Audio Server 上のすべてのポートをビジーアウトして、メンテナンス時間帯を提供するために使用します。

Web 会議のカスケード化

Web 会議をカスケード化することはできません。すべての参加者が同じ MeetingPlace Web サーバ上にいる必要があります。

セグメント化会議

外部ユーザがインターネット経由で Web 会議に参加できるようにする場合は、非武装地帯（DMZ）に別の外部 MeetingPlace Web サーバを配置することをお勧めします。この配置により、ファイアウォールの内側で内部ネットワークの機密を保護できます。このタイプの配置の詳細については、P.14-16 の「非武装地帯（DMZ）の要件」を参照してください。

ビデオ会議

MeetingPlace ソリューションは H.323 と SIP の両方をサポートしますが、現時点ではビデオ会議に H.323 ビデオ エンドポイントだけがサポートされ、会議が MCU で処理されます。MeetingPlace で作成されるビデオ会議は、すべて H.323 会議になるため、MeetingPlace Video Integration では MCU 上に H.323 リソースが必要です。このソリューションでは、MeetingPlace が制御アプリケーションの役割を担い、MCU が実リソースを提供してブリッジ処理を行います。MeetingPlace Audio Server 上のオーディオ専用参加者と通信するために、音声リンクが MCU と Audio Server の間に確立され、MCU 上のビデオ会議に参加する 1 人のオーディオ参加者として動作します。

MeetingPlace が MCU を制御するようになると、すべての H.323 ポートが制御され、MCU 上で会議を直接作成できなくなります。MeetingPlace は、H.323 ポートの可用性を確認するため、定期的に確認を行います。

MCU が SCCP 会議にもリソースを割り当てるように設定されている場合、Cisco Unified CallManager はそのリソースを使用して、SCCP ad-hoc ビデオ会議をセットアップできます。

音声リンク

ビデオ エンドポイントが会議に参加すると、*音声リンク*と呼ばれる特殊リンクが MeetingPlace Audio Server と MCU の間に確立されます。これは、MeetingPlace Audio Server から MCU 上のビデオ会議にダイヤルインするオーディオ参加者として機能します。会議のオーディオ エンドポイントがすべて MeetingPlace Audio Server に接続するのに対し、ビデオ エンドポイントはすべて MCU に接続します。それらは、音声リンクを介して互いに通信します。音声リンクは、最初のビデオ参加者が会議に参加するまで確立されません。最初のビデオ ユーザが会議に参加した時点で、MCU は MeetingPlace Video アプリケーションに信号を出し、それによって MeetingPlace Audio サーバが MCU への音声リンクを開始します。

同じ Audio Server にさまざまな E.164 番号を使用する複数の MeetingPlace H.323/SIP IP Gateway が存在する場合は、その E.164 番号をすべて MeetingPlace Video 設定ページに入力する必要があります。使用される E.164 番号は、Audio Server が発信ダイヤリング用に選択した MeetingPlace H.323/SIP IP Gateway によって決まります。MeetingPlace Video アプリケーションは、どの番号が選択されたかに関係なく、Audio Server の可能なすべての E.164 番号を認識して、音声リンクを受け入れる必要があります。

音声専用エンドポイントのない純粋なビデオ会議でも、すべての MeetingPlace 機能を利用するためには、2 つのシステムを接続する音声リンクが必要です。音声リンクは MeetingPlace Audio Server のいくつかの高度な機能、たとえば、ビデオ会議の Web 部分やオーディオ部分の記録とスケジューリングなどをサポートしているためです。

ビデオ記録は、MeetingPlace Video Integration ではサポートされません。MeetingPlace を使用すると、ビデオ会議のオーディオ部分と Web 部分を記録できます。サードパーティの記録システムを使用してビデオ セッションを記録することもできます。

MeetingPlace Video

MeetingPlace Video は MCS 上にインストールされるアプリケーションで、MCU に対する会議の承認者として機能します。MCU は、ビデオ会議の作成要求または既存のビデオ会議への追加参加者の承認要求を受信すると、その要求を MeetingPlace Video へ送って承認を受けます。

1 つの MeetingPlace Video アプリケーションは、1 つの MeetingPlace Web サーバとだけ通信できます。また、MeetingPlace Web 5.3 を実行するマシン上にインストールされている必要があります。MeetingPlace Audio Server に複数の MeetingPlace Web サーバが接続している場合、MeetingPlace Video をインストールしたり、有効にしたりすることができる Web サーバは 1 つだけです。それ以外の MeetingPlace Web サーバは、ユーザにビデオ機能を提供できません。

ファイアウォールの外側のユーザにビデオ機能が必要な場合は、DMZ に置かれた Web サーバ上で MeetingPlace Video を有効にする必要があります。外部ユーザ用の Web コラボレーションはインターネット経由でサポートされますが、現時点では、外部の電話およびビデオ参加者が公衆網（または ISDN）を使用して、Cisco Unified CallManager に接続されたゲートウェイ、または MeetingPlace に直接接続されたゲートウェイにアクセスすることが前提になっています。

DMZ で稼働する MeetingPlace Video がある場合は、外部ビデオ会議だけをスケジューリングできます。内部ビデオ会議のスケジュール要求は失敗します。

ビデオ ポート要求で会議がスケジューリングされた場合、その会議の Web 会議は、MeetingPlace Video アプリケーションがインストールされた MeetingPlace Web サーバ上で行われます。

MCU の設定

Cisco Unified MeetingPlace ビデオ会議機能は、Cisco Unified Videoconferencing MCU と統合できます。MCU は、MeetingPlace がサードパーティ エージェントとして会議のスケジューリングと管理を制御することを許可するように設定されている必要があります。MCU の会議管理設定の中で、**External conference authentication policy** が **Authorize** に設定されている必要があります。

着信コールは、次のいずれかの方法で MCU にルーティングできます。

- Cisco Unified CallManager 経由

  Cisco Unified CallManager で、MCU サービス プレフィックスのルート パターンを MCU に直接ルーティングするように設定します（ゲートウェイとして定義）。
- ゲートキーパー経由

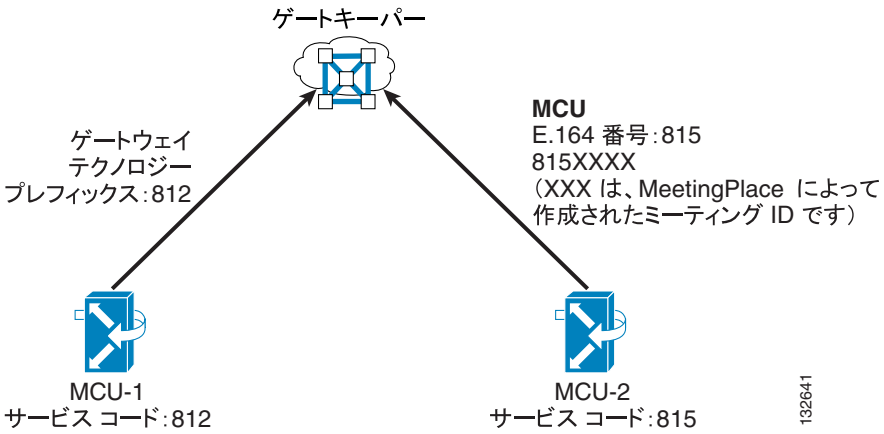
  Cisco Unified CallManager で、MCU サービス プレフィックスのルート パターンをゲートキーパーへの H.225 トランクにルーティングするように設定します。

MCU からの発信コールでは、次の理由から常にゲートキーパーが必要です。

- MCU 上で定義された H.323 サービス コードは、発信者が会議にダイヤルインするときにコールがゲートキーパーにルーティングされるように、ゲートキーパーに登録されている必要があります。
- ゲートキーパーはアドレス解決のために必要です。MCU 自体は H.323 ビデオ端末からのアドレスを解決しないためです。

MCU は、ゲートウェイまたは MCU としてゲートキーパーに登録できます（図 14-11 を参照）。通常、MCU はゲートウェイとして登録されますが、MeetingPlace の場合は、MCU を MCU として登録してください。MCU をゲートウェイではなく MCU として登録すると、MCU の動作が端末に近くなり、サービス プレフィックスが E.164 番号としてゲートキーパーに登録されます。

図 14-11　MCU をゲートキーパーに登録する 2 つの方法



MeetingPlace に使用する MCU には、一意のサービス コード（プレフィックス）を設定する必要があります。プロトコルは、H.323 にする必要があります。サービス プレフィックスは、ビデオ会議コールが MCU にルーティングされるように、Cisco Unified CallManager のルート パターンで設定されたプレフィックスと同じにする必要があります。詳細については、P.14-35 の「ビデオ会議のコール フロー」を参照してください。

MeetingPlace Video では、少なくとも 1 つの会議ビューが、指定されたサービス コードになっている必要があります。また、そのビューは単一パネルのビューの必要があります。管理者は、Voice-Activated（VA; 音声起動）と Continuous-Presence（CP; 連続表示）の表示モードを切り替える MeetingPlace Web オプションを利用できるように、2 番目のビューを提供できます（CP モードを実行する場合は、Enhanced Media Processor モジュールを使用することをお勧めします）。2 番目のビューは、マルチパネル ビューの必要があります。

Enhanced Media Processor（EMP）の要件

Cisco Unified Videoconferencing Enhanced Media Processor（EMP）は、強力な DSP リソース モジュールであり、MCU 上にインストールして、より複雑なコンピューティングと処理を行うことができます。EMP は、ほとんどのビデオ会議機能（H.323 の場合の Continuous-Presence または Voice-Activated）に必須のものではありませんが、最新の MeetingPlace Video ソフトウェアに高い品質を提供できるので、強くお勧めします。

SCCP ビデオ デバイス上で Continuous-Presence を実行するには、常に EMP が必須です。MCU から見ると、会議は SCCP 会議ではなく H.323 会議になります。

（注） MeetingPlace ビデオ統合は、Cisco Unified Videoconferencing MCU プラットフォーム上の速度整合モジュールと Data Collaboration Server をサポートしません。

ポート管理

MeetingPlace Video は、次のタイプのポートを提供します。

- ビデオ会議ポート

  このポートは、MCU 上のサービス コードの設定に基づいて動的に割り当てられます。MeetingPlace Video はリソース（ビデオ ポートと会議の最大数）が MCU 内で変更されたかどうかを定期的に検証し、それに応じて MeetingPlace Audio Server を更新します。
- ビデオ フローティング ポート

  このポートは、ビデオ会議ポートのプールから割り当てられます。システム管理者は、最初にスケジューリングされた以上の数のビデオ ポートを必要とする会議に、多数のビデオ ポートを予約できます。音声リンクを活用するには、最小数のフローティング ポートが必要です。このフローティング ポートの最小数を計算する公式は、次の Web サイトで入手可能な『*Administrator's Guide for Cisco Unified MeetingPlace Video Integration*』に記載されています。

  http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/video/53/index.htm
- ビデオ過剰予約ポート

  このポートは、物理的に存在しません。スケジュール済み会議では、予約されていても未使用のポートが存在するのが一般的であるという前提に基づいて、実際に使用可能な数よりも多くのポートをスケジューリングできるようにするために設定されるソフトウェア ポートです。このポートは物理的には存在しないので、設定可能な数に制限はありません。

スケジューリング

MeetingPlace ビデオ会議をスケジューリングできるのは、次のインターフェイスだけです。

- Web インターフェイス
- Outlook または Notes のインターフェイス
- MeetingTime

現在のところ、Voice User Interface はビデオ スケジューリング機能をサポートしていません。

ビデオ会議は、最初のビデオ参加者が会議に参加するまでセットアップされません。ユーザが会議に参加中に、ビデオ リソースを取得することはできません。会議は事前にスケジューリングされているか、予約なしの会議であることが必要です。

ビデオ会議は、MCU 上で定義された指定サービス コードを使用して作成されます。MeetingPlace ビデオ統合に許可されるサービス コードは 1 つだけです。そのサービス コードによって、すべての MeetingPlace ビデオ会議の動作とデフォルト パラメータが制御されます。

作成される個々の会議のダイヤルイン番号は一意で、次の形式になります。

指定サービス コード（MCU で設定）+ *会議 ID*（MeetingPlace が割り当て）

即時会議と予約なし会議のどちらも作成できます。

ビデオ会議への参加

ビデオ エンドポイントは、次のいずれかの方法で会議に参加できます。

- MeetingPlace からの発信ダイヤル

  ユーザは最初に、MeetingPlace Web または MeetingPlace Outlook から会議に参加します。エンドポイント アドレスはユーザのプロファイルの一部であり、ビデオ エンドポイント アドレス ボックスに表示されます。次に、ユーザがクリックすることで、MeetingPlace がビデオ エンドポイントへ発信ダイヤルします。これは、ビデオ エンドポイントが会議に参加するための簡単な方法です。

- MCU へのダイヤル

  ダイヤルする番号は、P.14-33 の「スケジューリング」の項で説明している形式になります。この方法は、オーディオ専用エンドポイントでの一般的なユーザ操作と異なっています。MeetingPlace Audio Server へのダイヤルインとは異なり、ビデオ ユーザに対して会議 ID の入力が求められません。現在のところビデオ会議は認証を使用していないので、次の特性を持つ会議ではビデオ ダイヤルインが許可されません。

  — パスワードの必要な会議

  — 招待専用またはプロファイル専用の会議（公開の誰でも参加できる会議以外）

  これらのタイプの会議では、ユーザは MeetingPlace Web インターフェイスまたは Outlook から参加します。

ビデオ会議の場合のビデオ エンドポイントへの発信ダイヤリングは、自動ではありません。会議をスケジューリングするときにエンドポイントを定義できないためです。会議が開始された後で、ユーザはプロファイル（電話番号）をクリックして発信ダイヤルします。

会議のタイプ

すべてのビデオ会議は、次のいずれかのタイプを使用して毎回作成されます。

- 標準の予約済み会議またはスケジュール済み会議
- 連続会議

  スケジュール済み会議と同様に、ビデオ会議は最初のビデオ ユーザが会議に参加すると作成されます。ビデオ会議は、会議全体（オーディオとビデオ）が MeetingPlace プラットフォームから打ち切られるまで終了しません。Audio Server と MCU との間の音声リンクは、最後のビデオ参加者が会議から切断してから 5 分後に終了します。

- 即時会議（予約なしの会議が有効でないシステム）

  MeetingPlace で予約なしモードが有効にされていない場合でも、現在の会議数と使用中のビデオ ポート数が MCU 内のキャパシティを超えていない限り、ユーザは Web インターフェイスを介して即時タイプの会議を開始できます。

- 予約なしの会議

  このタイプの会議では、事前にビデオ ポートが予約されません。ユーザは、使用可能なビデオ会議スロットとフローティング ポートがある限り、このタイプの会議に参加できます。予約なし会議の開始前にビデオ ユーザが参加した場合、対応するビデオ会議が作成されますが、会議の主催者がオーディオ側から会議に参加するまで、そのユーザは待合室に入れられます。待機モードの間、ユーザは互いに通信できず、会議がまだ開催されていないというメッセージがユーザに表示されます。

- 講義形式の会議

  この会議には、話者と聴取者という 2 つのタイプの参加者が存在します。ビデオ ユーザは、参加すると常に聴取者として扱われ、実際には自分が話者としてスケジューリングされていても、自分自身を話者として有効にする手段を持ちません。講義形式の会議に話者として参加する唯一の方法は、ビデオ参加者ではなく、オーディオ参加者として会議に参加することです。話者は会議の開始時に、参加者を待合室に入れたり（消音になり、ビデオがブロックされる）、聴取者としたり（消音になるが、画像は表示できる）、オープン フロアにしたり（オーディオとビデオを使用してすぐに通信できる）することができます。

- マルチサーバ会議

  P.14-38 の「ビデオ会議のカスケード化」の章を参照してください。

ビデオ会議のコール フロー

最初のビデオ参加者が会議に参加すると、MeetingPlace Video は MCU への XML 制御チャネルを開き、オーディオ サーバから MCU への発信ダイヤルを開始し、オーディオ会議をビデオ会議に結合します。このリンクは、両方の会議でオーディオ参加者として動作します。

図 14-12 は、最初の会議参加者がビデオ会議を開始したときに、音声リンクの作成に必要なプロセスを示しています。ユーザがビデオ会議を開始できるようにするには、事前に MCU がゲートキーパーに MCU として登録されている必要があります。また、MCU が Cisco Unified CallManager 内で H.323 ゲートウェイとして定義されていることも必要です。

図 14-12　ビデオ会議の開始プロセス

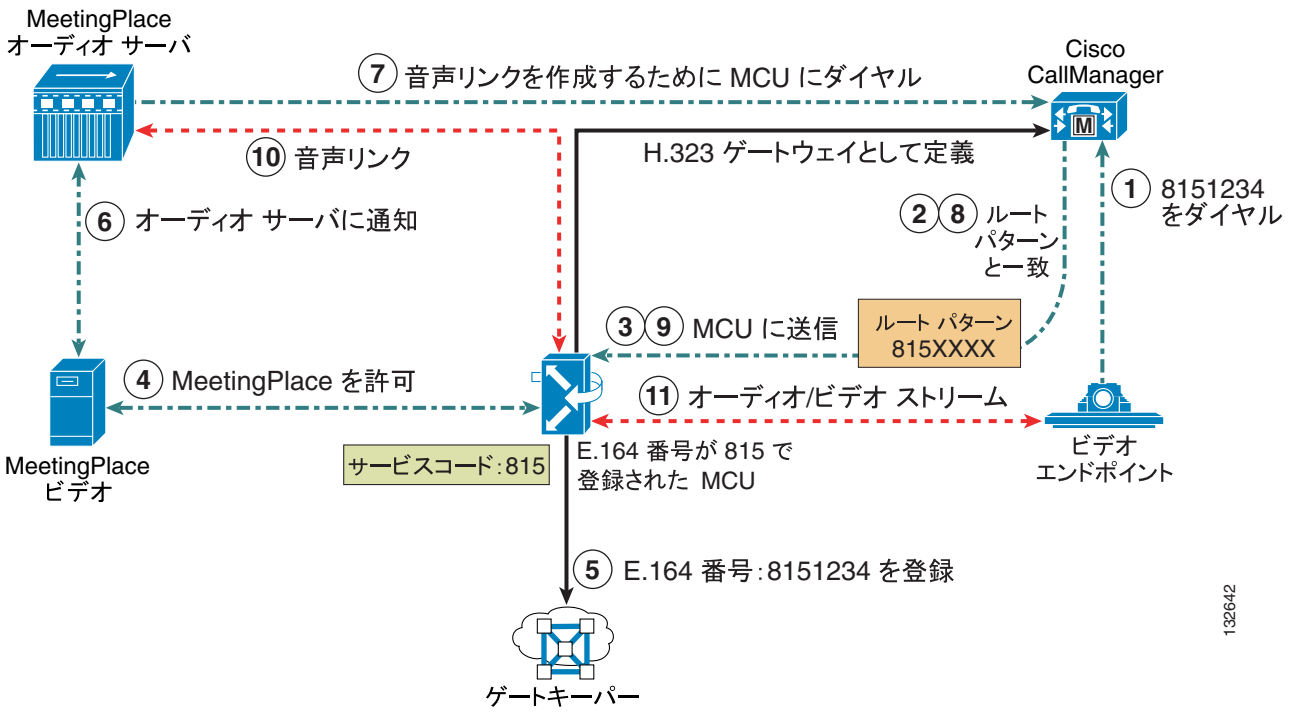


図 14-12 は、ビデオ会議開始プロセスの次の各ステップを示しています。

1. 最初のビデオ参加者が 8151234（1234 は MeetingPlace で作成された会議 ID）をダイヤルし、そのコールが Cisco Unified CallManager にルーティングされます。
2. Cisco Unified CallManager で、コールは H.323 ゲートウェイを指すルート パターン 815XXXX と一致し、そのゲートウェイは Cisco Unified CallManager で MCU を表すように定義されています。
3. コールは MCU にルーティングされます。
4. MCU は MeetingPlace Video に許可を送信し、会議と参加者の情報を検証します。
5. また、MCU は、新規に生成された会議番号（8151234）をゲートキーパーに追加 E.164 番号として登録します。
6. MeetingPlace Video は音声リンクを作成するように Audio Server に通知します。
7. Audio Server は 8151234（MCU）にダイヤルし、ビデオ会議に参加します。
8. コールは Cisco Unified CallManager に転送され、再びこの番号の同じルート パターンと一致して、コールがルーティングされます。
9. この Audio Server からのコールは MCU にルーティングされます。
10. Audio Server と MCU の間に音声リンクが作成されます。
11. 最初のビデオ参加者用のオーディオ　ストリームとビデオ　ストリームが、エンドポイントと MCU との間に確立されます。

2 番目以降のビデオ参加者の場合、コール フローはステップ 1、2、3、4、11 に従います。

ビデオ発信ダイヤリングの場合、要求は MeetingPlace Video Integration から MCU に渡されます（図 14-14 を参照）。エンドポイントから MCU へのダイヤルインの場合、コール フローは通常のダイヤルイン ビデオ コールのフローと同じで、MeetingPlace はユーザ認証の確認だけに関係します（図 14-15 を参照）。

図 14-13　ビデオ会議の開始コール フロー（音声リンク作成）

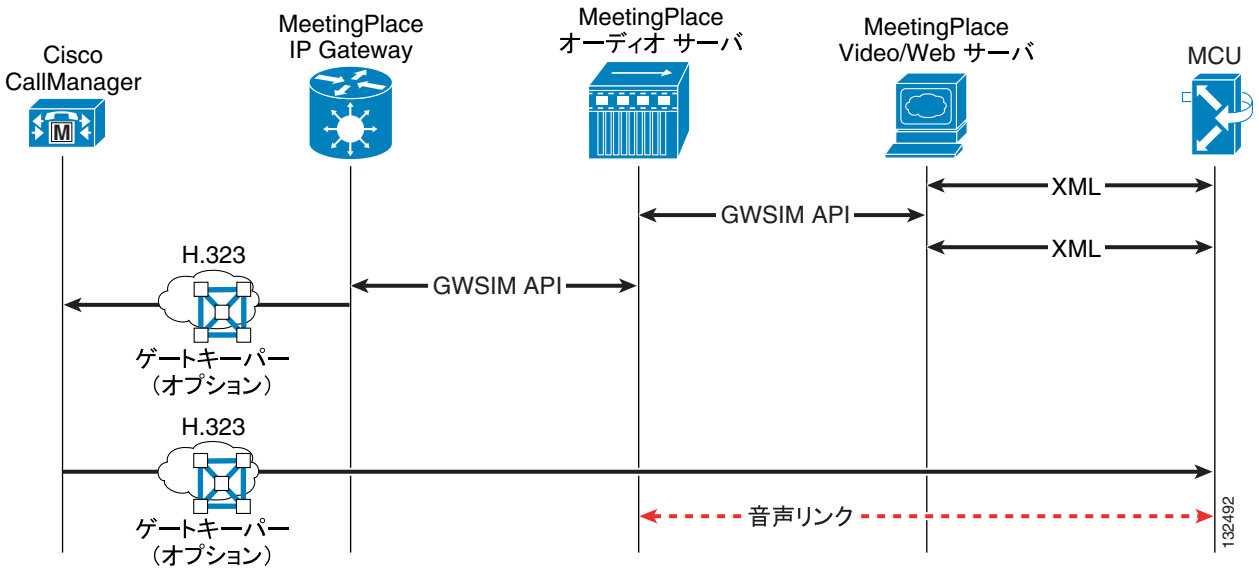


図 14-14　ビデオ会議の発信ダイヤリングのコール フロー

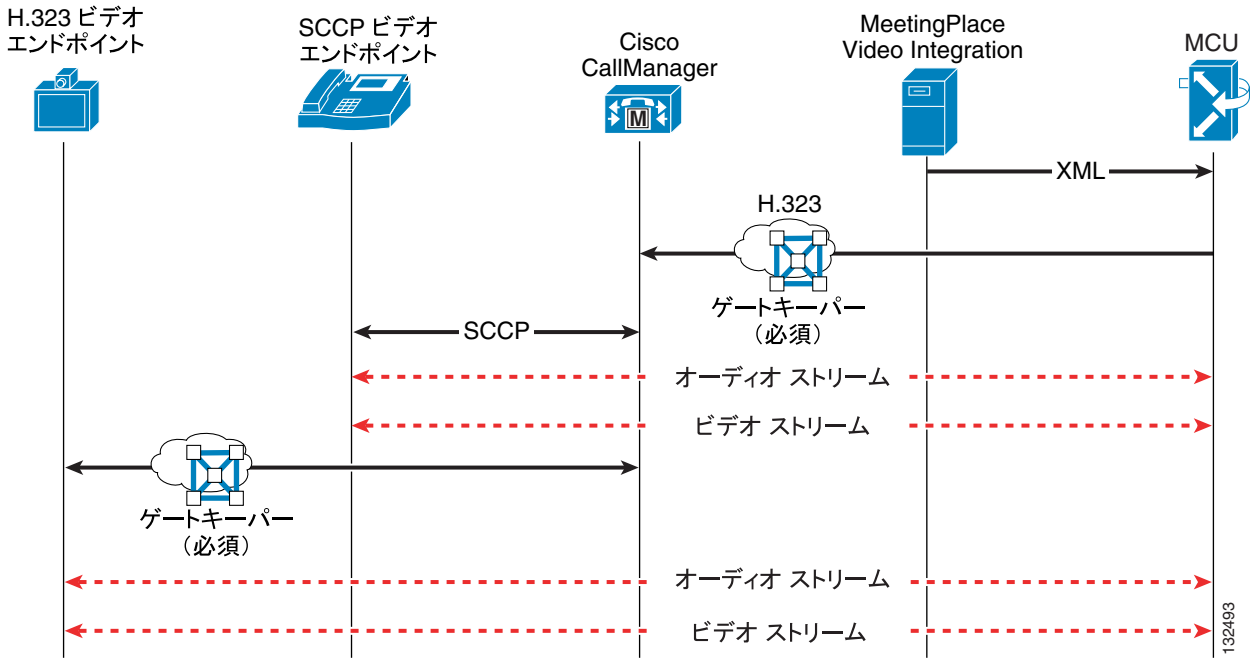
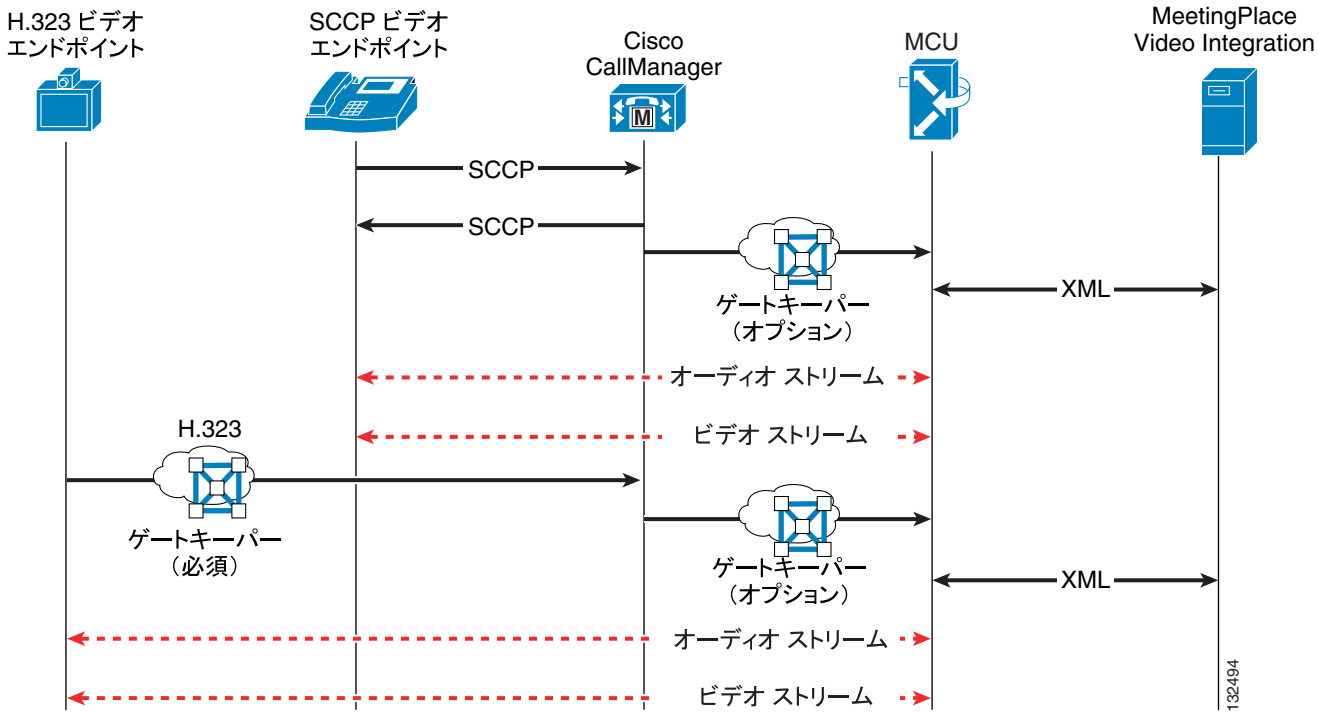


図 14-15　ビデオ会議のダイヤルインのコール フロー



ビデオ会議のカスケード化

現在のところ、ビデオを MeetingPlace の実装内で複数の MCU にカスケード化することはできません。各種の MeetingPlace システムが音声リンクを介して互いに通信している場合は、さまざまな MeetingPlace Audio Server を同じ会議用にカスケードでき、そのような会議を *マルチサーバ会議*と呼びます。マルチサーバ会議では、すべての参加者は プライマリ Audio Server に関連付けられた Web サーバに存在します。ビデオ参加者が発生する可能性があるのは、使用された Web サーバにビデオ統合がインストールされている場合です。

マルチサーバ会議の詳細については、次の Web サイトで入手可能な『*Administrator's Guide for Cisco Unified MeetingPlace Audio Server*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/conf/mtgplace/index.htm

ゲートキーパーとダイヤル プラン

ゲートキーパーは、H.323 ビデオ端末が IP 通信システムと統合された場合に必須のコンポーネントです。ゲートキーパーは主に、H.323 エンドポイントがコールを開始したときに、そのエンドポイントのアドレス解決を行います。

Cisco IOS Release 12.3(8)T 以降では、Cisco Unified CallManager は、それ自体を中継ゾーン ゲートキーパーに対して IP-to-IP ゲートウェイト（シスコ音声ゲートキーパーの新しいソフトウェア機能）として登録できます。また、H.323 エンドポイントを、静的 IP アドレスではなく別名（動的アドレス）を使用して登録できます。これらの新機能は、次の各項で説明するように、MeetingPlace Video Integration に関する H.323 のビデオ設計に大きな影響を与えます。

複数の Cisco Unified CallManager クラスタを使用し、集中型ゲートキーパーがクラスタ間トランク コール アドミッション制御を提供している場合、ビデオ エンドポイント用に使用しているゲートキーパーを、クラスタ間トランクに使用しているゲートキーパーと分離することをお勧めします。そうすることで、より柔軟なダイヤル プランを使用できるようになります。ビデオ ゾーンとクラスタ間トランク ゾーンが同じゲートキーパー上に設定されている場合、クラスタ間トランク ゾーンのゾーン プレフィックスはエンドポイント番号と重複できません。

ゲートキーパーとダイヤル プランの詳細については、P.10-1 の「ダイヤル プラン」の章を参照してください。

Cisco Unified CallManager での動的 H.323 アドレッシング

Cisco Unified CallManager 4.0 では、H.323 クライアントは静的 IP アドレスを使用して設定されます。Cisco Unified CallManager 4.1 以降では、E.164 アドレスを使用して H.323 クライアントを設定することもできます。E.164 アドレスを使用すると、H.323 クライアントが DHCP 用に設定されている配置の場合、H.323 クライアントの管理が簡単になります。E.164 アドレッシングは中継ゾーン ゲートキーパーと連携して動作し、中継ゾーン ゲートキーパーは、すべてのコールを **outvia** ゾーン（Cisco Unified CallManager ゾーン）内の Cisco Unified CallManager（IP-to-IP ゲートウェイとして動作）にルーティングするように設定できます。

このように設定すると、Cisco Unified CallManager は RasAggregator トランクと呼ばれる特殊なトランクを自動的に作成し、それをゲートキーパーに登録します。名前が表すとおり、このトランクは Registration Admission Status（RAS）に使用され、Cisco Unified CallManager で定義されたすべての動的アドレスを持つ H.323 デバイスを、同じゲートキーパーに登録された 1 つの集合デバイスとして管理するために使用されます。その H.323 デバイスが関連するコールが行われると、ゲートキーパーはこの RasAggregator トランク経由で Cisco Unified CallManager と通信します。

Cisco Unified CallManager 冗長性グループと H.323 クライアント

H.323 クライアントのデバイス プール内で定義される Cisco Unified CallManager 冗長性グループは、Cisco Unified CallManager を使用したコールに影響を与え、設定に誤りがあるとコール失敗の原因になるため重要です。冗長性グループの設定には、次の規則が適用されます。

- H.323 エンドポイントがゲートキーパーではなくピアツーピア モードを使用している場合は、Cisco Unified CallManager 上でその H.323 クライアント デバイス用の冗長性グループでのリストと同じ優先順位でサブスクライバを使用するように、その H.323 クライアントを設定する必要があります。
- それぞれの Cisco Unified CallManager 冗長性グループに対して、ゲートキーパーごとに一意のゾーンを設定する必要があります。

MCU の登録

MCU をゲートウェイとしてゲートキーパーに登録すると、そのサービス プレフィックス（たとえば 85）はテクノロジー プレフィックスとして登録されます。ゲートキーパーへの着信コールが、着信番号の中に一致するテクノロジー プレフィックスを持っている場合、ゲートキーパーは最初に中継ゾーン内で、その特定のプレフィックスを使用して登録された IP-to-IP ゲートウェイを検索します。したがって、H.323 エンドポイントが MCU にダイヤルインした場合（たとえば、851234 のアクセス コードを使用）、ダイヤルされた番号はテクノロジー プレフィックスの 85 と一致しますが、コールは失敗します。IP-to-IP ゲートウェイ（Cisco Unified CallManager）は、実際にはテクノロジー プレフィックス 1# を使用して登録されているためです。

テクノロジー プレフィックスとの不要な一致を避けるため、MCU をゲートウェイではなく MCU として登録することをお勧めします。MCU を MCU として登録するとテクノロジー プレフィックスが登録されないため、そのテクノロジー プレフィックスを使用して、ゲートキーパーが IP-to-IP ゲートウェイを検出することもなくなります。

また、MCU を会議 ID の登録を行うように設定することもお勧めします。これにより、会議 ID が作成されると必ず個々の E.164 番号がゲートキーパーに登録されるようになります。

MeetingPlace

MeetingPlace はゲートウェイに 1 つの端末として登録されるので、MeetingPlace H.323/SIP IP Gateway を 1 つのゾーンに、他のすべての H.323 ビデオ エンドポイントと共に配置することができます。Cisco Unified CallManager からの RasAggregator トランクも、その同じゾーンに登録されます。

Reservationless Single Number Access（RSNA）

Reservationless Single Number Access（RSNA）機能を使用すると、ユーザ コミュニティから複数の MeetingPlace Audio Server が 1 つのサーバとして見えるようにすることができます。この機能は、主に予約なしの会議用に設計されています。この機能を使用すると、ユーザは単一の電話番号にダイヤルすることで、1 つの場所に配置された複数の Audio Server にアクセスできます。ユーザがダイヤルインして予約なし ID を入力すると、システムはコールをその会議に適したサーバに転送します。この機能では、リモート ロケーションのユーザがローカル サーバにダイヤルすることもできます。

RSNA は、REFER メソッドをサポートする SIP エンドポイントに依存しています。Cisco Unified CallManager 5.0 は REFER をサポートしているため、RSNA を実装できます。以前のバージョンの Cisco Unified CallManager は、REFER や RSNA をサポートしていませんでした。

詳細については、次の Web サイトで入手可能な MeetingPlace の製品資料を参照してください。

http://www.cisco.com/en/US/products/sw/ps5664/ps5669/tsd_products_support_series_home.html

冗長性とロード バランシング

ここでは、次の MeetingPlace コンポーネントの冗長性とロード バランシングに関する考慮事項について説明します。

- MeetingPlace Audio Server（P.14-41）
- MeetingPlace H.323/SIP IP Gateway（P.14-42）
- MeetingPlace Web（P.14-43）
- Cisco Unified CallManager（P.14-43）
- MeetingPlace Video（P.14-44）
- MCU（P.14-44）

MeetingPlace Audio Server

MeetingPlace Audio Server に障害が発生すると、進行中のコールはドロップされます。Audio Server が MeetingPlace H.323/SIP IP Gateway から到達不能の場合、MeetingPlace H.323/SIP IP Gateway はすべての着信コールをすぐに拒否します。MeetingPlace H.323/SIP IP Gateway がダウンすると、Cisco Unified CallManager は MeetingPlace H.323/SIP IP Gateway との H.323 接続を確立できなくなります。MeetingPlace Audio Server には、利用可能な自動フェールオーバー メカニズムがありません。

障害回復

障害回復計画は、データベース、コンピューティング、およびサービスの順序正しい回復作業を規定したものです。通常、この計画では次のプロビジョニングを行います。

- 冗長性（ハードウェアの予備部品）
- データとソフトウェアのバックアップ
- 代替の緊急ロケーション
- 複数のサイトに分割された操作

MeetingPlace Network Backup Gateway と呼ばれるコンポーネントを使用すると、システム管理者は、MeetingPlace データベース（オーディオ設定ファイルとスケジューリングされた会議の情報）の複数のコピーを、Audio Server からネットワーク上の指定されたストレージ サーバに転送できます。各ファイルは、セキュリティのために暗号化されます。1 つのシステムあたり最大 3 台の Network Backup Gateway を実装できますが、データベースを転送できるのは一度に 1 台だけです。

冗長性

複数の MeetingPlace Audio Server が配置されている場合は、次のいずれかの冗長性計画を実装できます。

- シャドウ サーバ

  シャドウ サーバとは冗長 MeetingPlace Audio Server のことで、プライマリ Audio Server に障害が発生するまでアクティブになりません。障害時には Command Line Interface（CLI; コマンドライン インターフェイス）を使用して、シャドウ サーバをシャドウ モードからアクティブ モードに切り替える必要があります。アクティブになったシャドウ サーバは、プロファイル情報、会議情報（過去、現在、および未来）、参加者情報など、限られた情報だけを格納できます。記録、添付ファイル、ハードウェアとネットワークの設定、および自動ソフトウェア アップグレードの各機能は使用できません。シャドウ サーバには、次のネットワーク接続要件があります。

  — ラウンドトリップ遅延は 250 ms 未満である。

  — パケット損失は 1% 未満である。

  — 最小帯域幅は 384 kbps である。

- デュアル会議サーバ

  この計画では、2 台の MeetingPlace Audio Server がアクティブな実稼働サーバとなり、それぞれがもう一方にオーバーフローできます。プロファイルは、これらのサーバ間で Directory Service によって自動的に同期されます。2 台の Audio Server 間での自動フェールオーバーは*行われません*。緊急時には、会議をもう一方のサーバにアップロードする必要があり、ユーザは会議に手動で参加し直す必要があります。Cisco Unified CallManager では、1 台の MeetingPlace Audio Server に障害が発生したときに、コールがもう一方のアクティブな MeetingPlace Audio Server にルーティングされるように、ルート グループとルート リストを設定します。

- 連続会議サーバ

  この計画では、事前に作成済みで常に利用可能な一連の重要な会議が、MeetingPlace Audio Server に実装されます。この配置には危機管理チームへのブラスト発信ダイヤルなどの機能があり、すべての危機管理アプリケーションに適しています。

MeetingPlace H.323/SIP IP Gateway

MeetingPlace H.323/SIP IP Gateway には、次のような冗長性とロード バランシングに関する考慮事項があります。

冗長性

MeetingPlace H.323/SIP IP Gateway に障害が発生すると、進行中のコールはドロップされます。

複数の MeetingPlace H.323/SIP IP Gateway を同じ MeetingPlace Audio Server に接続できます。ダイヤルイン冗長性は、次の方法で実装できます。

- すべての MeetingPlace H.323/SIP IP Gateway を Cisco Unified CallManager 上に設定し、同じルート グループに入れます。Cisco Unified CallManager と MeetingPlace H.323/SIP IP Gateway との間のリンクに障害が発生した場合、Cisco Unified CallManager は現行ルート グループでその次の MeetingPlace H.323/SIP IP Gateway を選択します。この方法はロード バランシングにも適用できます。
- すべての MeetingPlace H.323/SIP IP Gateway を特定のゾーンにある 1 つの H.323 ゲートキーパーに登録すると、そのゲートキーパーがフェールオーバーを処理できます。そのゲートキーパーで **gw-priority** を設定し、決められたプライオリティをそれぞれの MeetingPlace H.323/SIP IP Gateway で指定します。

発信ダイヤルの場合、MeetingPlace Audio Server は次のアルゴリズムを使用します。

- すべての MeetingPlace H.323/SIP IP Gateway が正しく機能し、発信ダイヤルの失敗がまったくない場合、Audio Server はビジー度の最も低いゲートウェイを発信ダイヤル用に選択し、ゲートウェイ間のロード バランシングが実現されます。
- いずれかの MeetingPlace H.323/SIP IP Gateway に障害がある場合、Audio Server はそのゲートウェイをスキップし、障害のない残りのゲートウェイ間でロード バランシングを行います。
- すべてのサーバが障害を起こしたことがある場合、Audio Server は障害発生時刻が最も古いサーバを選択し、そのゲートウェイで再び障害が発生するまで、そのゲートウェイを使用し続けます。

ロード バランシング

ダイヤルイン ロード バランシングには、冗長性の場合と同じ次の方法を使用できます。

- Cisco Unified CallManager でルート グループを使用しますが、Distribution Algorithm として **Top down** ではなく **Circular** を選択します。Cisco Unified CallManager は、発信コールをラウンドロビン方式でゲートウェイ間に分散します。
- ゲートキーパーを使用します。ロード バランシングのためには、優先ゲートウェイを指定する **gw-priority** を設定しないでください。その代わりに、ゲートキーパーがラウンドロビン方式で、コールをすべての登録済みゲートウェイに分散するようにしてください。

前の項で説明したように、発信ダイヤルのロード バランシングは、以前に発信ダイヤルに障害の発生したことがない MeetingPlace H.323/SIP IP Gateway 間でのみ行われます。

MeetingPlace Web

MeetingPlace Web には、次のような冗長性とロード バランシングに関する考慮事項があります。

冗長性

Web 会議中に Web 会議サーバで障害が発生した場合、すべてのユーザは会議の Web 部分から切断され、現行の Web 会議は続行不能になります。ユーザは、別のアクティブな Web サーバで Web 会議に参加し直すことができます。障害の発生したサーバ上に SQL サーバ データベースがある場合、クラスタ内のすべての Web 会議サーバが機能しなくなり、ユーザはデータベースが復元されるまで Web 会議を開催できなくなります。

ロード バランシング

MeetingPlace Web サーバをいくつかのクラスタにグループ化すると、会議要求をさまざまな Web サーバに分散するロード バランシングのパフォーマンスが向上し、処理できる会議数を増やすことができます。MeetingPlace Web クラスタには、最大で 6 つの Web サーバを内部構成または外部構成で含めることができます。

MeetingPlace WebConnect 機能を使用すると、単一の URL で複数の内部および外部 MeetingPlace システムを統合できます。複数の Audio Server にまたがるスケジューリングが可能です。最初の Audio Server に十分なキャパシティがない場合は、2 番目以降の Audio Server が順に試行されます。

Cisco Unified CallManager

Cisco Unified CallManager には、次のような冗長性とロード バランシングに関する考慮事項があります。

冗長性

Cisco Unified CallManager に障害が発生した場合、その Cisco Unified CallManager を使用した進行中の MeetingPlace コールはドロップされ、ユーザは会議に参加し直す必要があります。エンドポイントからのダイヤルインの場合、冗長性は Cisco Unified CallManager クラスタ内で設定された冗長性グループを使用して実現されます。

MeetingPlace H.323/SIP IP Gateway を通じた MeetingPlace からのアウトダイヤリングの場合、それぞれの MeetingPlace H.323/SIP IP Gateway が通信できるのは、1 つの Cisco Unified CallManager だけです。したがって、冗長性には次のガイドラインを適用できます。

- MeetingPlace H.323/SIP IP Gateway が、ゲートウェイとして直接、Cisco Unified CallManager と通信するように設定されている場合は、複数の MeetingPlace H.323/SIP IP Gateway を同じ MeetingPlace Audio Server に接続することが、冗長性を実装する唯一の方法です。
- MeetingPlace H.323/SIP IP Gateway がゲートキーパーに登録されている場合は、ゲートキーパーがフェールオーバーの状況を処理し、コールをアクティブな Cisco Unified CallManager にルーティングします。

ロード バランシング

エンドポイントから MeetingPlace へのダイヤルインの場合、コールのロード バランシングは Cisco Unified CallManager の冗長性グループとルート グループの設定によって実現されます。

MeetingPlace H.323/SIP IP Gateway を通じた MeetingPlace からのアウトダイヤリングの場合、冗長性の場合と同じガイドラインをロード バランシングにも適用できます。

MeetingPlace Video

MeetingPlace Video には、次のような冗長性とロード バランシングに関する考慮事項があります。

冗長性

MeetingPlace Video アプリケーションは、1 つの MeetingPlace 5.3 システムに 1 つだけ実装できます。MeetingPlace Video は、MeetingPlace Web 5.3 を実行しているサーバにインストールする必要があります。MeetingPlace Video は、1 つの MeetingPlace Web サーバとだけ通信します。

要求されたビデオ ポートで会議がスケジューリングされた場合、その会議の Web 会議は、MeetingPlace Video がインストールされた MeetingPlace Web サーバ上で行われます。そのサーバに障害が発生した場合、会議はサイトの管理 UI ページで設定された Load Stats Poll Period（デフォルトは 1 分間）の 5 倍の期間が経過した後、別のサーバにロール オーバーされます。ビデオ ポートがスケジューリングされた会議が別の Web サーバにロール オーバーした場合、GUI でビデオ機能は提供されません。ユーザは発信ダイヤルできなくなりますが、ダイヤルインは可能です。

ロード バランシング

MeetingPlace Video アプリケーションは、一度に 1 つしかアクティブにできないので、MeetingPlace Video にロード バランシングは存在しません。

MCU

現在のところ、MeetingPlace 5.3 ビデオ統合を使用した場合、1 つの MeetingPlace Audio Server あたり 1 つの MCU だけを実装できます。したがって、MCU に冗長性やロード バランシングはありません。

CHAPTER 15

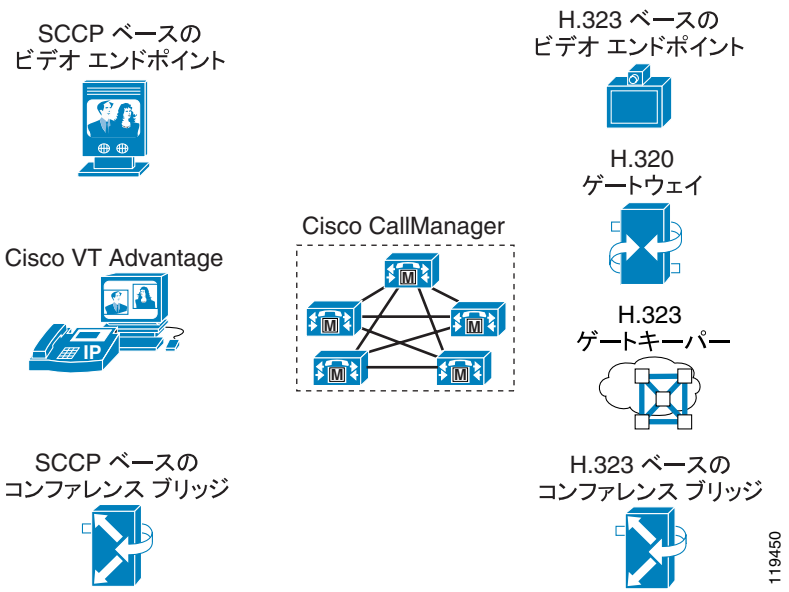
IP ビデオ テレフォニー

シスコは、IP ビデオ テレフォニー ソリューションを Cisco Unified CallManager Release 4.0 で導入しました。ビデオは Cisco Unified CallManager に完全に統合され、シスコおよびシスコの戦略パートナーから多くのビデオ エンドポイントも入手できるようになりました。Cisco Unified Video Advantage は、Cisco Unified IP Phone と同様に、簡単に配置、管理、および使用できます。

IP ビデオ テレフォニー ソリューションのコンポーネント

Cisco IP ビデオ テレフォニー ソリューションは、Cisco Unified CallManager 5.0、H.323 電話会議と Skinny Client Control Protocol（SCCP）電話会議の両方に対応する Cisco Unified Videoconferencing 3500 シリーズ Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、Cisco Unified Videoconferencing 3500 シリーズ H.320 ゲートウェイ、Cisco IOS H.323 ゲートキーパー、Cisco Unified Video Advantage、Cisco IP Video Phone 7985、Sony 社製および Tandberg 社製の SCCP エンドポイント ソリューション、および Polycom、Tandberg、Sony などのパートナーが取り扱っている既存の H.323 または SIP 準拠製品で構成されます（図 15-1 を参照）。

図 15-1　IP ビデオ テレフォニーのコンポーネント



Cisco Unified CallManager 5.0 のビデオ機能拡張

Cisco Unified CallManager Release 4.0 は、ビデオ機能と IP Telephony を統合した最初のソフトウェア リリースです。Cisco Unified CallManager Release 5.0 では、IP ビデオ テレフォニーをサポートするために、次の項目についてさらに機能が拡張されています。

- プロトコル（P.15-2）
- ビデオ コールの MTP およびトランスコーダ サポート（P.15-3）
- トポロジ対応ロケーション（P.15-3）

プロトコル

Cisco Unified CallManager Release 5.0 では、SIP トランクと SIP エンドポイントのビデオ サポートが導入されました。以前のバージョンの Cisco Unified CallManager では、SIP サポートはトランキングに限られ、ビデオはサポートされていませんでした。

Cisco Unified CallManager は、多くのプロトコルをサポートします。任意のデバイスから任意の別のデバイスを呼び出すことができますが、ビデオは SCCP、H.323、および SIP デバイスでのみサポートされます。具体的には、Cisco Unified CallManager Release 5.0 において、次のプロトコルではビデオがサポートされません。

- コンピュータ / テレフォニー インテグレーション（CTI）アプリケーション（TAPI および JTAPI）
- メディア ゲートウェイ コントロール プロトコル（MGCP）

したがって、現在 Cisco Unified CallManager でサポートされるコールのタイプは、表 15-1 に示すとおりです。

表 15-1　Cisco Unified CallManager Release 5.0 でサポートされるコールのタイプ

発信デバイス タイプ	着信デバイス タイプ				
	SCCP	H.323	MGCP	TAPI/JTAPI	SIP
SCCP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ
H.323	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ
MGCP	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
TAPI/JTAPI	音声のみ	音声のみ	音声のみ	音声のみ	音声のみ
SIP	音声とビデオ	音声とビデオ	音声のみ	音声のみ	音声とビデオ

表 15-2 は、現在 Cisco Unified CallManager でサポートされている音声とビデオのアルゴリズムおよびプロトコルを示しています。

表 15-2　Cisco Unified CallManager Release 5.0 でサポートされる機能

H.323	SCCP	SIP
H.261	H.261	H.261
H.263、H.263+	H.263、H.263+	H.263、H.263+
H.264	H.264	H.264
Cisco VT Camera Wideband ビデオ コーデック（H.323 クラスタ間トランクのみ）	Cisco VT Camera Wideband ビデオ コーデック	
G.711 A-law および mu-law	G.711 A-law および mu-law	G.711 A-law および mu-law
G.723.1	G.723.1	G.723.1

表 15-2　Cisco Unified CallManager Release 5.0 でサポートされる機能（続き）

H.323	SCCP	SIP
G.728	G.728	G.728
G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab	G.729、G.729a、G.729b、G.729ab
G.722	G.722	G.722
G.722.1		
H.224 遠端カメラ制御（Cisco Unified CallManager でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし	H.224 遠端カメラ制御（Cisco Unified CallManager でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし	H.224 遠端カメラ制御（Cisco Unified CallManager でサポートされますが、すべてのエンドポイントでサポートされるわけではありません） プロトコル インターワーキングなし
アウトオブバンド DTMF（H.245 英数字） RFC2833 AVT Tones（SIP コールへの H.323 クラスタ間トランクの場合のみ）	アウトオブバンド DTMF RFC2833 AVT Tones	RFC2833 AVT Tones Unsolicited SIP Notify KPML
	Cisco ワイドバンド オーディオ	

ビデオ コールの MTP およびトランスコーダ サポート

Cisco Unified CallManager Release 5.0 からは、パススルー コーデックを使用して、Cisco IOS Enhanced Media Termination Point（MTP）がビデオ コールをサポートするようになりました。パススルー コーデックを使用すると、Cisco Unified CallManager が動的に挿入した MTP またはトランスコーダによってビデオ コールのビデオ ストリームを終了できます。このとき、RTP ストリームをデコードする必要はありません。

トポロジ対応ロケーション

Cisco Unified CallManager Release 5.0 からは、ロケーション間のコールで使用できる帯域幅の量を制限する方式が 2 つになりました。Cisco Unified CallManager 4.0 では、ロケーションでのビデオ コールのサポートが導入されました。具体的には、Cisco Unified CallManager 4.0 および 4.1 のロケーション オプションによって、あるロケーションと別のロケーションの間のすべてのコールに許可される合計帯域幅が定義されます。この合計帯域幅の値は、従来のハブアンドスポーク ネットワーク トポロジに十分に対応します。Cisco Unified CallManager Release 5.0 では、リソース予約プロトコル（RSVP）に基づくトポロジ対応ロケーションを使用して、2 つのサイト間のパスに十分な帯域幅があるかどうかを判断する新しいオプションが用意されています。RSVP を使用すると、複雑なトポロジに対応するホップ単位のチェックが可能になり、RSVP アプリケーション ID を使用して音声帯域幅とビデオ帯域幅を個別にサポートできます。

（注） 静的ロケーションと RSVP ベースのロケーションは、異なるモデルを使用して、音声コールとビデオ コールを区別します。詳細については、P.9-1 の「コール アドミッション制御」を参照してください。

RSVP ベースのロケーションでは、RSVP ポリシーの概念が採用されています。多くのポリシー オプションがありますが、主に次の 2 つのカテゴリに分けられます。

- コールを完了するために、ビデオ ストリームの RSVP 予約が必須。コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます。
- ビデオ ストリームの RSVP 予約が望ましい。

最初に、リージョンに設定された音声コーデックとビデオ帯域幅で、ビデオ コールの最大速度（ビット レート）が定義されます。予約要求として、最大ビット レートを使用してコールのオーディオ ストリームとビデオ ストリームの RSVP 予約が Cisco RSVP Agent から送信されます。ビデオ ストリームの RSVP 予約が失敗した場合、Cisco Unified CallManager は RSVP ポリシーの設定をチェックし、このコールの処理方法を決定します。オーディオ ストリームのポリシーが省略可能な場合、コールは音声のみとして継続します。オーディオ ストリームの RSVP ポリシーが必須の場合は、オーディオ ストリームも RSVP 予約の取得に失敗した場合を除いて、コールは音声のみとして継続します。予約に失敗した場合、コールは失敗するか（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）、Automated Alternate Routing（AAR）によってコールの再ルーティングが試行されます（トポロジ対応ロケーションの詳細については、P.9-1 の「コール アドミッション制御」を参照してください。

（注）　ビデオ優先ポリシーを使用しているときに、ビデオ予約に失敗した場合、コールは音声のみとして完了します。ただし、ユーザはビデオが失敗した原因を示す、視覚的な表示または音声によるフィードバックを受けることができません。

Administration に関する考慮事項

この項では、ビデオ テレフォニーに関係する Cisco Unified CallManager Administration の次の構成要素について説明します。

- リージョン（P.15-5）
- ロケーション（P.15-8）
- Retry Video Call as Audio（P.15-9）
- Wait for Far-End to Send TCS（P.15-12）

リージョン

リージョンを設定するときは、Cisco Unified CallManager Administration の 2 つのフィールド、Audio Codec と Video Bandwidth を設定します。オーディオ設定ではコーデック タイプを指定し、ビデオ設定では許可する帯域幅の量を指定します。ただし、表記は異なりますが、Audio Codec フィールドと Video Bandwidth フィールドは、実際には似た機能を実行します。Audio Codec フィールドは、音声のみのコールおよびビデオ コールの音声チャネルに許可される最大ビットレートを定義します。たとえば、リージョンの Audio Codec を G.711 に設定した場合、Cisco Unified CallManager はそのリージョンの音声チャネルに許可される最大帯域幅として 64 kbps を割り当てます。この場合、Cisco Unified CallManager は G.711、G.722、G.728、または G.729 を使用するコールを許可します。ただし、Audio Codec を G.729 に設定すると、Cisco Unified CallManager は、音声チャネルに許可される帯域幅の最大量として 8 kbps だけを割り当てます。また、G.728、G.711、および G.722 はすべて 8 kbps より多く帯域幅を使用するため、G.729 を使用するコールだけが許可されます。

（注） 両方のエンドポイントが G.711 と G.722 をサポートしている場合、デフォルトで、G.722 がネゴシエートされます。

（注） Audio Codec 設定は、ビデオ コールの音声チャネルにも適用されます。

Video Bandwidth フィールドは、コールのビデオ チャネルに許可される最大ビットレートを定義します。ただし、従来のビデオ会議製品での慣例に従い、このフィールドに使用する値には、音声チャネルの帯域幅も含めます。たとえば、G.711 の音声を使用する 384 kbps のコールを許可するには、Video Bandwidth フィールドに 320 kbps ではなく 384 kbps を設定します。

つまり、Audio Codec フィールドは音声のみのコールおよびビデオ コールの音声チャネルに使用する最大ビットレートを定義し、Video Bandwidth フィールドは、ビデオ コールに許可される最大ビットレート（コールの音声部分を含む）を定義します。

各デバイスは、表 15-3 で示すように、特定の音声コーデックのみをサポートするため、正しい音声コーデックの帯域幅制限を選択することが重要です（特定のエンドポイントでサポートされるコーデックの最新リストについては、そのエンドポイントの製品マニュアルを参照してください）。

表 15-3　エンドポイント デバイスでサポートされている音声コーデックのタイプ

コーデック タイプ	Cisco 7900 シリーズ IP Phone	Sony 社製および Tandberg 社製の SCCP エンドポイント	一般的な H.323 または SIP エンドポイント	IP/VC 3500 シリーズ ゲートウェイ	IP/VC 3500 シリーズ MCU
G.729	あり	あり、モデルによる	なし	なし	あり（トランスコーダを使用）
G.728	なし	あり、モデルによる	あり	あり（トランスコーダを使用）	あり（トランスコーダを使用）
G.711	あり	あり	あり	あり	あり
G.722	なし	あり	あり	あり（トランスコーダを使用）	あり（トランスコーダを使用）
Cisco ワイドバンド オーディオ	あり	なし	なし	なし	なし

表 15-3 で示すように、リージョンを G.729 に設定した場合、ビデオ会議デバイスによっては、このタイプのコーデックをサポートできないものがあります。たとえば、Cisco Unified Video Advantage エンドポイントと Tandberg 社製エンドポイントとの間のコールは失敗します。または、このコールに Cisco Unified CallManager が音声変換リソースを割り当てます。

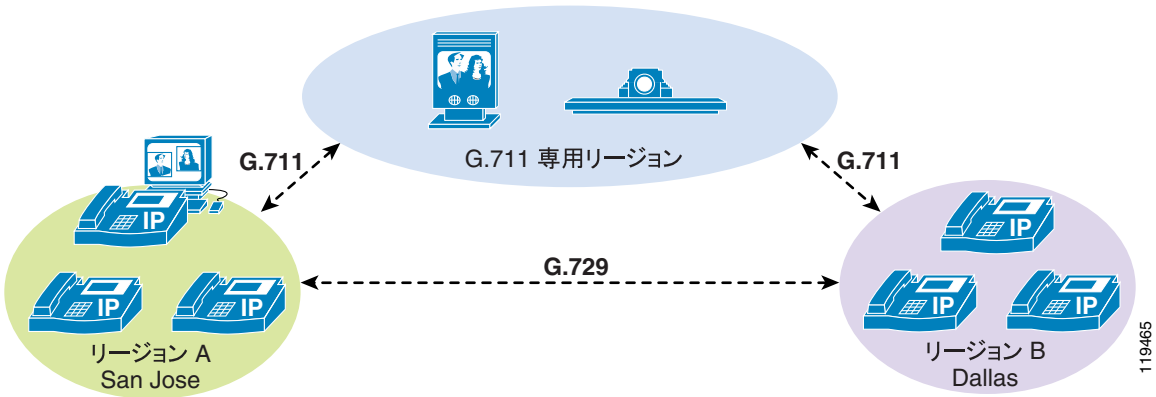
Cisco Unified CallManager Release 5.0 では、Cisco IOS Enhanced Media Termination Point に基づく音声変換リソースが導入されました。これによって、パススルー コーデックによるビデオ ストリームのサポートを継続しながら、ビデオの音声ストリームのトランスコーディングができます。パススルー コーデックは、トランスコーディングが必要なストリームには使用できないため、ビデオ ストリームにのみ使用されます。パススルー コーデックを使用するには、次の 3 つの条件をすべて満たす必要があります。

- 2 つのエンドポイント デバイスのコーデック能力が一致している。
- どちらのエンドポイントでも、**MTP Required** がオフになっている。
- すべての中間リソース デバイス（MTP およびトランスコーダ）がパススルー コーデックをサポートしている。

従来のトランスコーダは、現在、パススルー機能をサポートしていません。そのため、コールは音声のみとして接続され、G.729 と G.711 の間でトランスコーディングされます。Cisco IOS Enhanced Transcoder を使用せずにこの状態を防止するには、G.711 を使用するようにリージョンを設定する必要があります。ただし、G.711 に設定されたリージョンは、2 つの IP Phone 間の音声コールにも G.711 を使用します。この場合、WAN で消費される帯域幅が増えます。

帯域幅を節約するために音声のみのコールに G.729 を使用し、ビデオ コールに G.711 を使用する場合は、G.729 をサポートしないビデオ エンドポイント用に G.711 を使用するリージョンを設定し、IP Phone 用に G.729 を使用する別のリージョンを設定する必要があります（図 15-2 を参照）。この方式を使用すると、必要なリージョンの数が増えますが、望ましいコーデックと帯域幅の割り当てが得られます。

図 15-2　ビデオ コールに G.711 を使用し、音声のみのコールに G.729 を使用



(注)　ビデオを禁止するリージョンのペアを設定できます。このリージョン ペアにある 2 つのビデオ対応デバイスが相互に通話しようとした場合、Retry Video Call as Audio がオンになっていれば、音声のみとして接続されます。オフになっている場合は、AAR 再ルーティング ロジックが実行されます。

表 15-4 は、設定例とその結果を示しています。

表 15-4　さまざまなリージョン設定のシナリオ

リージョン設定	Retry Video as Audio の設定	結果
リージョンでビデオを許可する。	有効	ビデオ コールは許可される。
リージョンでビデオを許可する。	無効	ビデオ コールは許可される。
リージョンでビデオを許可しない。	有効	ビデオ コールは音声として処理される。
リージョンでビデオを許可しない。	無効	AAR が設定されていない場合、ビデオ コールは失敗する（ビジー トーンが再生され、「Bandwidth Unavailable」メッセージが表示される）。

Video Bandwidth フィールドには、1 ～ 8128 kbps の値を指定できます。ただし、H.323 および H.320 ビデオ会議デバイスとの互換性を維持するために、このフィールドには常に、56 または 64 kbps の倍数の値を入力することをお勧めします。したがって、このフィールドの有効な値としては 112 kbps、128 kbps、224 kbps、256 kbps、336 kbps、384 kbps などがあります。

エンドポイントで要求されるコール速度がリージョンに設定されている帯域幅値を超えた場合、Cisco Unified CallManager は自動的に、リージョン設定で許可された値に適合するようにコールをネゴシエートします。たとえば、H.323 エンドポイントが別の H.323 エンドポイントを 768 kbps で呼び出しているが、リージョンは最大 384 kbps を許可するように設定されていたとします。発信側からの着信 H.225 セットアップ要求はコール速度として 768 kbps を提示しますが、Cisco Unified CallManager は、着信側への発信 H.225 セットアップ メッセージで、この値を 384 kbps に変更します。そのため、着信側エンドポイントは、開始するコールが 384 kbps であると認識し、このレートでコールがネゴシエートされます。発信側エンドポイントは、要求した帯域幅として 768 kbps を提示しますが、ネゴシエートされた帯域幅は 384 kbps になります。

ただし、リージョンの Video Bandwidth を「None」に設定した場合は、着信側デバイスの Retry Video Call as Audio が有効かどうかに応じて、Cisco Unified CallManager はコールを終了するか（この場合、H.225 Release Complete メッセージを発信側に送信）、音声のみのコールとして通過を許可します（P.15-9 の「Retry Video Call as Audio」を参照）。

ロケーション

静的ロケーションを設定するときも、Cisco Unified CallManager Administration の 2 つのフィールド、Audio Bandwidth と Video Bandwidth を設定します。ただし、リージョンと異なり、静的ロケーションの Audio Bandwidth は音声のみのコールにのみ適用され、Video Bandwidth はビデオ コールの音声チャネルとビデオ チャネルの両方に適用されます。音声帯域幅とビデオ帯域幅は、別々に維持されます。これは、両方のタイプのコールが帯域幅の単一割り当てを共有すると、音声コールが使用可能な帯域幅のすべてを使用してビデオ コール用の帯域幅が残らなくなる（または、その逆になる）可能性が高いためです。また、音声とビデオの個別の帯域幅プールは、ネットワーク上のスイッチおよびルータでのキューの設定方法に対応します。通常、音声トラフィック用のプライオリティ キューと、ビデオ トラフィック用の独立したプライオリティ キューまたはクラスベース WFQ があります。詳細については、P.3-31 の「WAN の QoS」を参照してください。

Audio Bandwidth フィールドと Video Bandwidth フィールドのどちらにも、None、Unlimited、または数値を指定する 3 つのフィールドがあります。ただし、これらのフィールドに入力する値は、2 つの異なる計算モデルを使用します。Audio Bandwidth フィールドに入力する値には、コールに必要なレイヤ 3 ～ 7 のオーバーヘッドを含める必要があります。たとえば、ロケーションとの間で単一の G.729 コールを許可する場合は、値として 24 kbps を入力します。G.711 コールの場合は、値として 80 kbps を入力します。一方、Video Bandwidth フィールドには、オーバーヘッドを含めない値を入力する必要があります。たとえば、128 kbps コールの場合は 128 kbps を入力し、384 kbps コールの場合は 384 kbps を入力します。リージョンの Video Bandwidth フィールドで使用する値と同様に、ロケーションの Video Bandwidth フィールドにも、56 kbps または 64 kbps の倍数の値を使用することをお勧めします。

たとえば、企業に 3 サイトのネットワークがあるとします。San Francisco ロケーションには、San Jose メイン キャンパスに接続された 1.544 Mbps T1 回路があります。システム管理者は、このロケーションとの間で、4 つの G.729 音声コールと 1 つの 384 kbps（または 2 つの 128 kbps）ビデオ コールを許可します。Dallas ロケーションには、San Jose メイン キャンパスに接続された 2 つの 1.544 Mbps T1 回路があります。管理者は、このロケーションとの間で、8 つの G.711 音声コールと 2 つの 384 kbps ビデオ コールを許可します。この例で、管理者は、San Francisco ロケーションと Dallas ロケーションに次の値を設定します。

ロケーション	必要な音声コールの数	Audio Bandwidth フィールドの値	必要なビデオ コールの数	Video Bandwidth フィールドの値
San Francisco	4、G.729 を使用	96 kbps（4 * 24 kbps）	1、384 kbps	384 kbps
Dallas	8、G.711 を使用	640 kbps（8 * 80 kbps）	2、384 kbps	768 kbps

エンドポイントで要求されるコール速度がロケーションに設定されている値を超えた場合、リージョンの場合とは異なり、Cisco Unified CallManager はロケーション設定で許可された値に適合するように、自動的にはコール速度をネゴシエートしません。コールは拒否されるか、音声のみのコールとして再試行されます（着信側デバイスで Retry Video as Audio 設定が有効の場合）。そのため、リージョンのビデオ帯域幅は、ロケーションのビデオ帯域幅の値よりも低い値に設定する必要があります。たとえば、2 つのリージョン（リージョン A とリージョン B）があり、これら 2 つのリージョン間のビデオ帯域幅が 768 kbps に設定されている場合、リージョン A のデバイスがビデオ帯域幅が 384 kbps に設定されているロケーションにあると、これら 2 つのリージョン間のすべてのコールが失敗するか、音声のみのコールになります（Retry Video Call as Audio の設定による）。

Retry Video Call as Audio

このチェックボックスは、Cisco Unified IP Phone 7940、7941、7960、7961、7970、7971、および Cisco IP Video Phone 7985、Sony 社製または Tandberg 社製の SCCP エンドポイント、すべての H.323 および SIP デバイス（クライアント、ゲートウェイ、およびすべてのタイプの H.323 トランク）など、ビデオをサポートするすべてのエンドポイント タイプで使用できます。このオプションがアクティブ（オン）のときに、デバイスに到達できるだけの帯域幅がない場合（たとえば、Cisco Unified CallManager リージョンまたはロケーションで、そのコールのビデオが許可されない場合）、Cisco Unified CallManager はそのコールを音声のみのコールとしてリトライします。このオプションが非アクティブ（オフ）のときは、Cisco Unified CallManager はコールを音声のみとして再試行することなく、コールを失敗させるか、Automated Alternate Routing（AAR; 自動代替ルーティング）パスが設定されている場合は可能な限り再ルーティングします。デフォルトでは、このリトライ オプションは有効（オン）です。

この機能は、次のシナリオだけに適用されます。

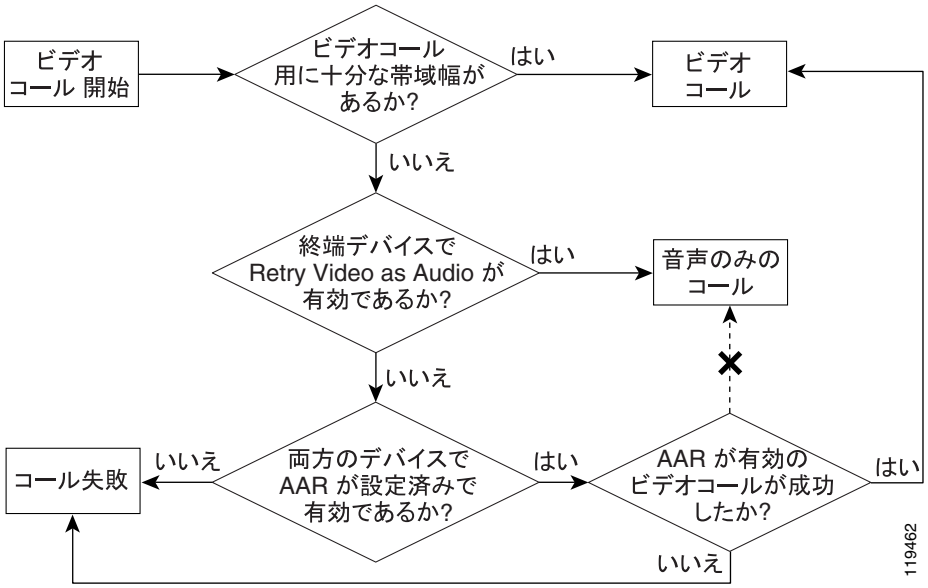
- ビデオを許可しないようにリージョンが設定されている。
- ビデオを許可しないようにロケーションが設定されている。または、要求されたビデオ速度が、そのロケーションで使用可能なビデオ帯域幅を超えている。
- Cisco Unified CallManager クラスタ間のコールの場合、要求されたビデオ速度がゲートキーパーのゾーン帯域幅制限を超えている。

Retry Video Call as Audio オプションは、終端（着信側）デバイスでのみ有効です。そのため、発信側デバイスでは宛先ごとに異なるオプション（再試行または AAR）を使用できる柔軟性があります。

帯域幅の制限が原因でビデオ コールが失敗した場合、自動代替ルーティング（AAR）が有効であれば、Cisco Unified CallManager は失敗したコールをビデオ コールとして AAR の宛先に再ルーティングしようとします。AAR が有効でない場合、失敗したコールによって、発信者にビジー トーンとエラー メッセージが送信されます（図 15-3 を参照）。発信側のデバイスのタイプによって、失敗したコールは次のいずれかになります。

- 発信側デバイスが LCD 画面付き SCCP エンドポイントの場合（Sony 社製または Tandberg 社製の SCCP エンドポイント、Cisco Unified IP Phone の多くのモデルなど）、発信者にはビジー トーンが聞こえ、メッセージ「Bandwidth Unavailable」がデバイスに表示されます。
- 発信側デバイスが LCD 画面なしの SCCP エンドポイントの場合（Cisco Unified IP Phone 7902 など）、発信者にはビジー トーンが聞こえます。
- 発信側デバイスが H.323 または SIP デバイス、またはゲートウェイで接続された公衆網デバイスの場合、発信者にはビジー トーンが聞こえ、Cisco Unified CallManager が適切なエラー メッセージ（Q.931 Network Congestion 原因コードなど）を H.323、SIP、または MGCP デバイスに送信します。

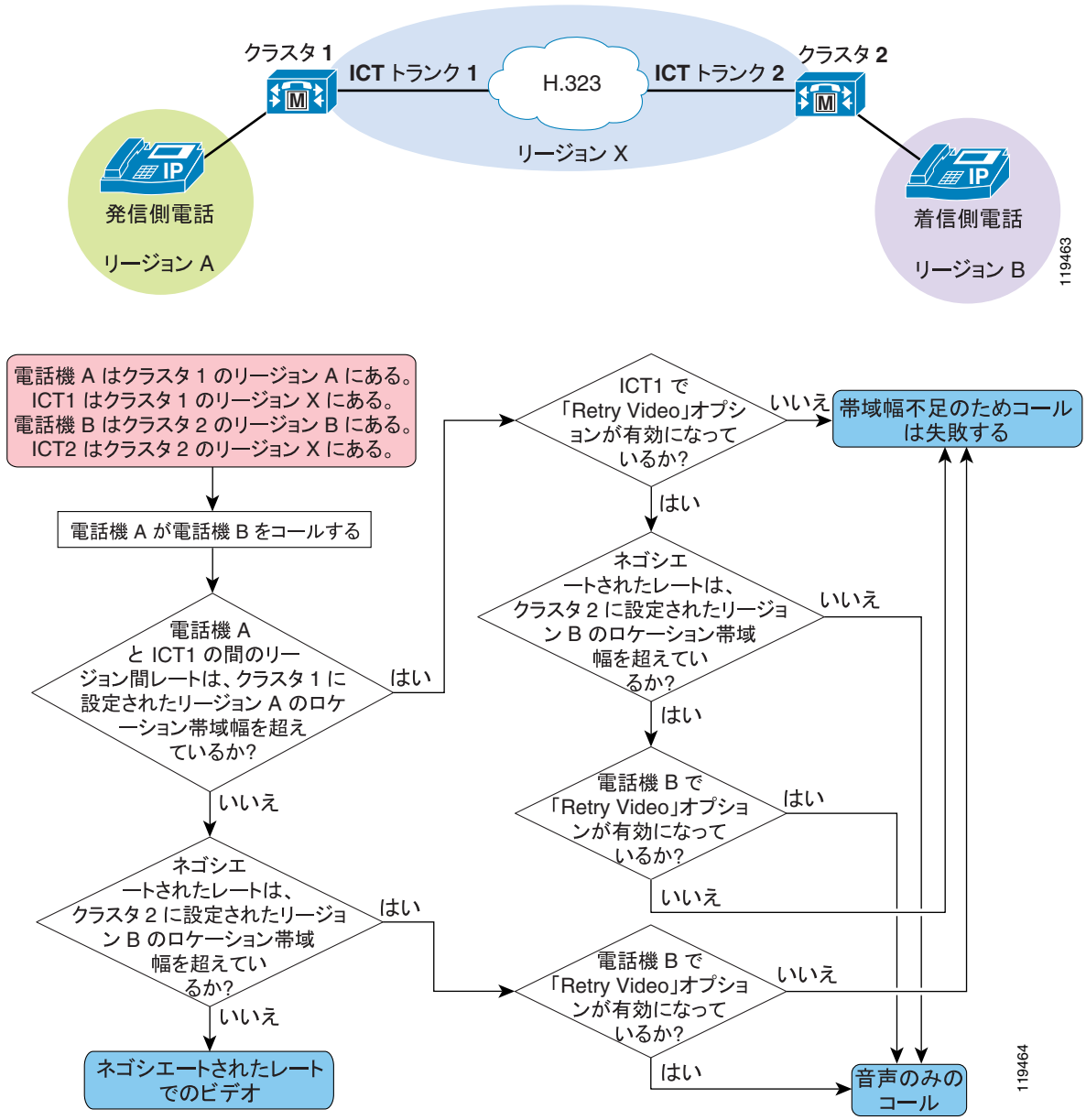
図 15-3　ビデオ コールで起こり得るシナリオ



AAR の使用方法の詳細については、P.9-1 の「コール アドミッション制御」の章を参照してください。

図 15-4 は、非ゲートキーパー制御クラスタ間トランクを使用する、2 つのクラスタ間のコールの手順を示しています。

図 15-4　非ゲートキーパー制御クラスタ間トランクを使用する 2 つのクラスタ間のコール フロー



Wait for Far-End to Send TCS

このチェックボックスは、H.323 クライアント、H.323 ゲートウェイ、H.225 ゲートキーパー制御トランクなど、すべての H.323 デバイスで使用できます。この機能は、H.323 コールの H.245 機能交換フェーズに関係します。この機能を有効にすると、Cisco Unified CallManager は、Cisco Unified CallManager が Terminal Capabilities Set（TCS; 端末機能セット）を H.323 デバイスに送信する前に、リモート H.323 デバイスが TCS を Cisco Unified CallManager に送信するまで待機します。このオプションが無効の場合、Cisco Unified CallManager は待機せず、すぐに TCS をリモート H.323 デバイスに送信します。

デフォルトでは、Wait for Far-End to Send TCS オプションが有効（オン）です。ただし、次の場合はオフ（無効）にする必要があります。

- Cisco Unified CallManager と通信する H.323 デバイスも、遠端が TCS を送信するまで待機する。

  この場合、どちらの側も TCS を送信しないためデッドロックが発生し、数秒後に H.245 接続がタイムアウトします。遠端が TCS を送信するまで待機するデバイスの例としては、一部の H.323 ルーテッドモード ゲートキーパー、H.320 ゲートウェイ、H.323 プロキシ（IP-to-IP ゲートウェイ）、一部の H.323 マルチポイント コンファレンス ブリッジがあります。これらのデバイスが遠端からの TCS の送信を待機する理由は、Cisco Unified CallManager が待機する理由と同じです。TCS を他方に転送する前に、接続の両端が TCS を送信するまで待機するためです。
- クラスタ間トランクを介して別の Cisco Unified CallManager クラスタと通信している。

（注）　クラスタ間トランクおよびゲートキーパー制御クラスタ間トランクでは、Wait for Far-End to Send TCS オプションは常に無効で、有効にすることはできません。

多くのシナリオで、Cisco Unified CallManager は、2 つのエンドポイント デバイス（相互に通話しようとする 2 つのクライアントなど）を接続するソフトウェア スイッチの役割を実行します。このような場合、両方のデバイスが TCS メッセージを送信するまで Cisco Unified CallManager が待機することが最良です。Cisco Unified CallManager が各デバイスの機能を認識することで、それぞれに送信する TCS に関して（特に、リージョンおよびロケーションの設定に応じて）最適な判断ができます。この場合、Wait for Far-End to Send TCS 機能は有効にする必要があります。

ただし、その他の H.323 デバイス（H.323 デバイスを H.320 デバイスに接続する H.320 ゲートウェイなど）が、複数の参加者を接続する機能を実行することもあります。また、ゲートウェイも、コールのセットアップ方法に関して最適な選択ができるように、両端が TCS メッセージを送信するまで待機します。Cisco Unified CallManager とゲートウェイの両方が、相手側から TCS が送信されるまで待機すると、デッドロックが発生します。このデッドロック状態を防止するには、Wait for Far-End to Send TCS 機能を無効（オフ）にします。

たとえば、図 15-5 で示す次のコール シナリオについて考えます。

- シナリオ 1：Cisco Unified Video Advantage が H.320 エンドポイントを呼び出す。
- シナリオ 2：H.323 クライアントが H.320 エンドポイントを呼び出す。

これらのシナリオでは、どちらの場合も、Wait for Far-End to Send TCS 機能は、デフォルト設定である有効（オン）のままにします。

図 15-5　Wait for Far-End to Send TCS 機能が有効（オン）のシナリオ

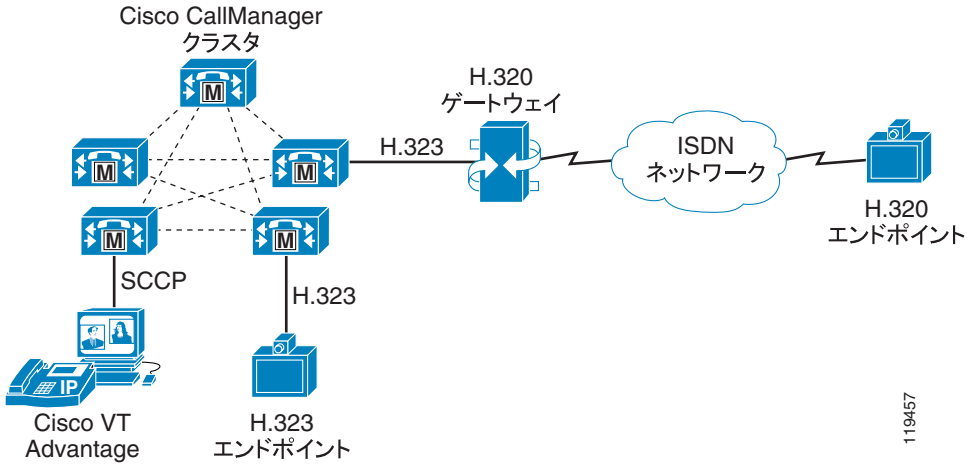


図 15-5 のシナリオ 1 では、登録時に SCCP デバイスがメディア機能を Cisco Unified CallManager に提供しているため、Cisco Unified CallManager はすでに Cisco Unified Video Advantage クライアントの機能を認識しています。しかし、ゲートウェイがコールの H.245 フェーズで TCS を Cisco Unified CallManager に送信するまで、Cisco Unified CallManager は H.320 ゲートウェイの機能を認識しません。同様に、H.320 エンドポイントが TCS をゲートウェイに送信するまで、H.320 ゲートウェイは、Cisco Unified CallManager に送信する TCS を判断できません。この場合、H.320 エンドポイントがゲートウェイに TCS を送信し、ゲートウェイが Cisco Unified CallManager に TCS を送信し、判断に使用できる両端のエンドポイントからの TCS を Cisco Unified CallManager が受信するため、Wait for Far-End to Send TCS 機能は有効のままにしておく方が適切です。

図 15-6 は、次のコール シナリオを示しています。これらのシナリオでは、Wait for Far-End to Send TCS 機能を無効にしないとコールが失敗します。

- シナリオ 1：Cisco Unified Video Advantage が、ISDN ネットワークを介してリモート クラスタにある別の Cisco Unified Video Advantage を呼び出す。
- シナリオ 2：H.323 クライアントが、ISDN ネットワークを介してリモート クラスタにある別の H.323 クライアントを呼び出す。

図 15-6　Wait for Far-End to Send TCS 機能が無効（オフ）のシナリオ

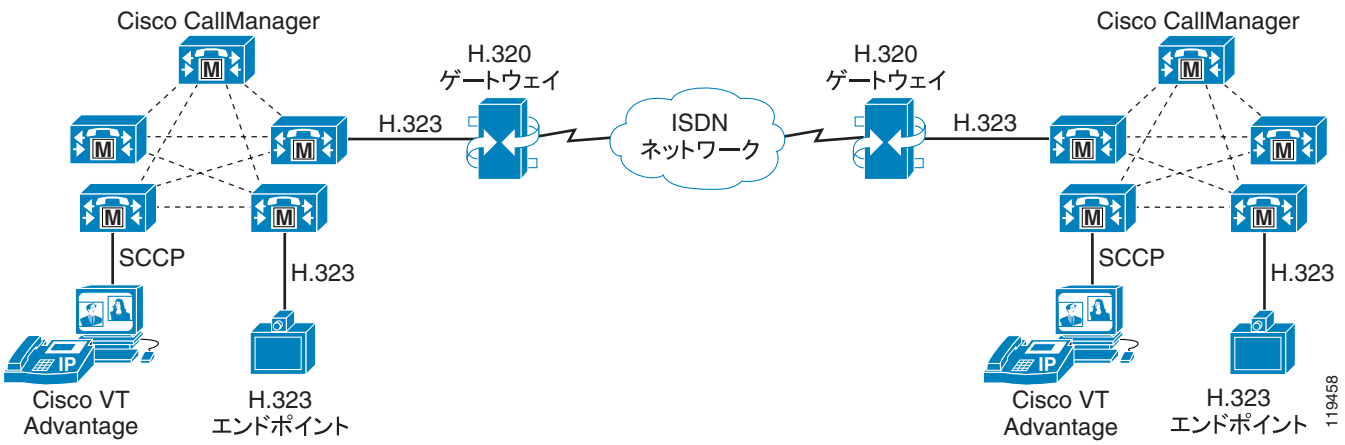


図 15-6 のどちらのシナリオでも、両方の Cisco Unified CallManager がゲートウェイから TCS を受信するまで待機し、両方のゲートウェイも ISDN 側からの TCS を受信するまで待機するため、デッドロックが発生します。コールは数秒後にタイムアウトし、失敗します。ユーザから見ると、発信者にはコールが進行中であることを示すリングバック トーンが聞こえ、着信側には着信コールを示す呼び出し音が聞こえます。着信側がコールに応答しようとすると、デッドロックのために H.245 フェーズが失敗し、コールは両方で切断されて失敗します。

このようなシナリオの問題の回避策としては、Cisco Unified CallManager で H.320 ゲートウェイを表すデバイスで、Wait for Far-End to Send TCS オプションを無効（オフ）にすることをお勧めします。H.320 ゲートウェイに到達するように Cisco Unified CallManager を設定した方法に応じて、このデバイスは H.225 ゲートキーパー制御トランクまたは H.323 ゲートウェイ デバイスになります。

ただし、Wait for Far-End to Send TCS オプションを無効にすると、交換された初期機能がリモート デバイスで機能しなくなることがあります。たとえば、Cisco Unified CallManager リージョンが 768 kbps ビデオに設定されていても、H.320 デバイスが 384 kbps しかサポートしないことがあります。また、選択された音声コーデックがリモート側で機能しないことがあります。この場合、初期ネゴシエートされた論理チャネルを切断し、正しい速度とコーデックで再開する必要があります。多くのレガシー H.323 および H.320 デバイスは、この状態を正しく処理せず、Cisco Unified CallManager が CloseLogicalChannel メッセージを送信して異なる値でチャネルと再ネゴシエートすると、コールを切断します。そのため、Wait for Far-End to Send TCS オプションを無効にする場所とタイミングには注意が必要です。

マルチポイント会議

3 者以上が同じビデオ コールに同時に参加するには、マルチポイント コントロール ユニット（MCU）が必要です。MCU は、次のメイン コンポーネントで構成されています。

- Multipoint Controller（MC）
- Multipoint Processor（MP）

MC は、メディア ネゴシエーション、コール シグナリング、コールに使用する MP の選択など、会議のコール セットアップと切断のすべての面を処理します。MP は、すべての音声パケットおよびビデオ パケットを処理します。MC が MP を制御し、1 つの MC で複数の MP を制御できます。MP は、ソフトウェアベースのものも、ハードウェアベースのものもあります。ソフトウェアベースの MP は、通常、高度なトランスコーディング、レート変換（複数の速度）、構成機能は実行できません。

1999 年以降、シスコは IP/VC 3500 シリーズ H.323 Multipoint Conference Unit（MCU）を提供してきました。このファミリの最初の製品は、Cisco Unified Videoconferencing 3510 です。このモデルは販売終了となり、Cisco Unified CallManager との互換性もありません。2002 年に、シスコは IP/VC 3511 および 3540 モデルを導入しました。これらのモデルは大幅に機能が改善され、古い 3510 モデルにはなかったスケーラビリティが実現されました。

2003 年、シスコは IP/VC 3511 および 3540 モデルにソフトウェア バージョン 3.2+ を導入し、Skinny Client Control Protocol（SCCP）のサポートを追加しました。SCCP サポートは、IP/VC 3510 では使用できません。また、IP/VC MCU では、次の 3 つのタイプの MP が使用できます。

- 各 MCU に内蔵されたソフトウェアベースの MP
- Rate Matching（RM）モジュール（IP/VC 3540 シャーシ専用のソフトウェアベースのモジュール）
- Enhanced Media Processor（EMP）（IP/VC 3540 シャーシ専用のモジュールまたは IP/VC 3511 モデルの内蔵コンポーネントとして使用できるハードウェアベースのソリューション）

Cisco Unified CallManager Release 4.0（およびそれ以降）は、SCCP、H.323、および SIP の各モードで IP/VC 3511 と 3540 モデルをサポートします。各プロトコルにはさまざまな機能が用意され、さまざまな理由で使用されます。そのため、3 つのプロトコルすべてを実行するように、これらの各 MCU が搭載されています。IP/VC 3511 は、SCCP モードまたは H.323 および SIP モードで実行するように設定できます。IP/VC 3540 モデルは、3 つのプロトコルすべてを同時に実行し、使用可能な MP リソースの合計数を 3 つの間で分け合うように設定できます。

シグナリング プロトコルに関係なく、MCU は、音声ストリームとビデオ ストリームを各参加者から受信し、これらのストリームをすべての他の参加者に、組み合せたビューで送信するという同じ基本機能を提供します。マルチポイント テレビ会議のビューには、次の 2 つのタイプがあります。

- Voice-Activated（音声起動）（切り替え）
- Continuous-Presence（連続表示）

Voice-Activated（音声起動）

Voice-Activated 会議は、すべての参加者の音声ストリームとビデオ ストリームを取得し、主要な発言者を決定し、主要な発言者のビデオ ストリームだけをすべての他の参加者に送信します。参加者には、主要な発言者の全画面イメージが表示されます（現在の発言者には、前の主要な発言者が表示されます）。すべての参加者からの音声ストリームが混合され、全員が他の全員の発言を聞くことができますが、ビデオは主要な発言者のものだけが表示されます。

次のいずれかの方法で、主要な発言者を選択できます。

- Voice-Activated モード

  このモードを使用すると、MCU は、最も声が大きく、発言が長い会議参加者を判断して、主要な発言者を自動的に選択します。声の大きさを判断するために、MCU は各参加者の音声信号の強さを計算します。会話中に条件が変わると、MCU は自動的に新しい主要な発言者を選

択し、その参加者が表示されるようにビデオを切り替えます。ホールド タイマーによって、ビデオの頻繁な切り替えが防止されます。主要な発言者になるには、指定された秒数以上発言し、他のすべての参加者よりも際立つ必要があります。

- MCU の Web ベースの会議制御ユーザ インターフェイスによる主要な発言者の手動選択

  会議コントローラ（議長）は MCU の Web ページにログオンし、参加者を強調表示することで、その参加者を主要な発言者として選択できます。この処理によって音声アクティビティ検出は無効になり、議長が新しい主要な発言者を選択するか、Voice-Activated モードを再度有効にするまで、主要な発言者は固定されます。

- 参加者リストを自動的に 1 人ずつ循環するように MCU を設定

  この方式を使用すると、MCU は設定された時間だけ各参加者で止まり、リスト上の次の参加者に切り替えます。会議コントローラ（議長）は、Web インターフェイスでこの機能をオンまたはオフにできます（オフにすると、Voice-Activated モードが再度有効になります）。

Continuous-Presence（連続表示）

Continuous-Presence 会議では、一部の参加者またはすべての参加者が合成ビューで同時に表示されます。ビューには 2 ～ 16 の長方形（参加者）をさまざまなレイアウトで表示できます。各レイアウトには、長方形の 1 つを Voice-Activated にする機能があり、合成ビューに表示できる長方形の数よりも参加者の方が多い会議で役立ちます。たとえば、4 画面のビューを使用していて、コールの参加者が 5 人のとき、同時に表示される参加者は 4 人だけです。この場合、長方形の 1 つを Voice-Activated にすると、主要な発言者に応じて参加者 4 と参加者 5 をその長方形で切り替えることができます。他の 3 つの長方形に表示される参加者は固定で、すべての長方形は、会議制御 Web ベース ユーザ インターフェイスで操作できます。

（注） Continuous-Presence には、IP/VC MCU の Enhanced Media Processor（EMP）が必要です。

MP リソース

どちらのタイプの会議でも、MP リソースによって、MCU がサポートできるビデオ形式、トランスレーティング、およびトランスコーディング機能が決まります。エンドポイントが異なる速度で会議に接続している場合は、レート変換対応 MP が必要です。RM モジュールと EMP モジュールは、どちらも速度間のレート変換に対応しています。レート変換対応 MP が使用できない場合、MCU はすべてのエンドポイントにフローコントロール メッセージを送出し、最も遅いエンドポイントの最大受信レートに合せて転送速度を下げるように指示します。たとえば、3 人の参加者が 384 kbps の会議に接続し、4 番目の参加者が 128 kbps で参加した場合、MCU は他の 3 人の参加者にフローコントロール メッセージを送信し、128 kbps の参加者に合せて転送速度を下げるように指示します。この方式を使用すると、1 人の参加者の性能が低いことで、すべての参加者の品質が低下します。レート変換対応 MP を使用した場合、128 kbps のストリームが 384 kbps に（および、その逆に）変換され、各参加者がそれぞれの接続で許可される最大の品質を使用できます。

Continuous-Presence 会議でも、レート変換対応 MP は非常に重要です。MCU に内蔵されたソフトウェアベースの MP は、すべての入力ストリームを組み合せ、得られた組み合せを各参加者に送信します。たとえば、4 人の参加者が 384 kbps で G.711 音声を使用して Continuous-Presence 会議に接続している場合、各参加者は 320 kbps のビデオと 64 kbps の音声を MCU に転送します。MCU は 4 つの入力ビデオ ストリームを取得し、4 画面の合成ビューに組み合せます。MCU は混在する 64 kbps の音声と共に、1280 kbps のビデオを各エンドポイントに転送します。その結果、エンドポイントごとに合計 1344 kbps になります。この方式は Asynchronous Continuous Presence と呼ばれ、帯域幅要件、コール アドミッション制御メカニズム、一部のデバイスとの相互運用性に悪影響を与えることがあります。

（注）　Asynchronous Continuous Presence は使用しないことを強くお勧めします。

RM モジュールまたは EMP モジュールを使用すると、MCU は各入力ストリームを組み合せる前に、合計出力帯域幅が入力帯域幅と一致するようにレート変換できます。たとえば、MCU が 4 画面のレイアウトを使用し、各参加者が 320 kbps のビデオと 64 kbps の音声を MCU に転送する場合、MCU は原則として各入力ストリームを 80 kbps にレート変換し、4 画面のビューが 320 kbps のビデオになるように組み合せ（4 * 80 kbps）、混合された 64 kbps 音声とこのビデオを組み合せて、最終的な組み合せを各参加者に転送します。この方式は、Synchronous Continuous Presence と呼ばれます。すべての Continuous-Presence 会議で、Synchronous Continuous Presence モードを使用することを強くお勧めします。ただし、このモードを使用するには、各 MCU にレート変換対応 MP（RM、EMP など）が必要で、MCU のコストが上がります。

（注）　MCU が内蔵された H.323 および SIP クライアントの場合、Cisco Unified CallManager は、H.323 クライアントで第 2 のコールの生成を許可しません。そのため、内蔵 MCU の機能は無効になります。

SCCP MCU リソース

すでに説明したように、Cisco Unified Videoconferencing 3511 および 3540 MCU はどちらも、これらのモデルのソフトウェア バージョン 3.2+ および Cisco Unified CallManager Release 4.0 から SCCP をサポートしています。SCCP モードで設定すると、Cisco Unified CallManager が MC 機能を提供し、MCU が MP 機能を提供します。SCCP MCU は、Cisco Unified CallManager で完全に制御されます。

SCCP MCU リソースを呼び出すのは、次のイベントだけです。

- SCCP エンドポイント（IP Phone や Tandberg 社製エンドポイントなど）のユーザが、Conf、Join、または cBarge ソフトキーを押して Ad-Hoc 会議を呼び出した。
- SCCP エンドポイント（IP Phone や Tandberg 社製エンドポイントなど）のユーザが、MeetMe ソフトキーを押して、予約なしの Meet-Me 会議を呼び出した。

これらのタイプの会議の参加者には、任意のタイプのエンドポイント（サポートされる任意のゲートウェイ タイプを介して Cisco Unified CallManager がサポートする任意のシグナリング プロトコルを使用するビデオ デバイスおよび非ビデオ デバイス）が含まれます。ただし、SCCP MCU リソースを呼び出せるのは、SCCP エンドポイントだけです。つまり、H.323 ビデオ エンドポイントは SCCP MCU リソースを呼び出せませんが、SCCP ビデオ エンドポイントがリソースを呼び出し、H.323 ビデオ参加者をコールに参加させることはできます。たとえば、SCCP エンドポイントのユーザは、Conf ソフトキーを押し、H.323 クライアントのディレクトリ番号をダイヤルして、もう一度 Conf ソフトキーを押すと、トランザクションを完了できます。H.323 クライアントは、参加者として SCCP MCU 会議に参加します。

ただし、Conf、Join、または cBarge ソフトキーで開始された Ad-Hoc 会議の場合、他の参加者が使用するシグナリング プロトコルは、保留機能および MCU に音声チャネルとビデオ チャネルを転送する機能をサポートしている必要があります。H.323 デバイス（H.323 クライアント、H.323 ゲートウェイ、H.320 ゲートウェイ、およびすべてのタイプの H.323 トランク）の場合、Cisco Unified CallManager は、H.245 仕様で定義されている Empty Capabilities Set（ECS）方式を使用してこの機能を実現しています。H.323 エンドポイントが Cisco Unified CallManager からの ECS メッセージの受信をサポートしていない場合、切断されるか、クラッシュしてリブートする可能性もあります。この問題の回避策としては、H.323 デバイスで「MTP Required」オプションを有効（オン）にして、MTP デバイスを含まないメディア リソース グループ リスト（MRGL）をこのデバイスに割り当て、Cisco CallManager のサービス パラメータ「Fail Call if MTP Allocation Fails」を False に設定します

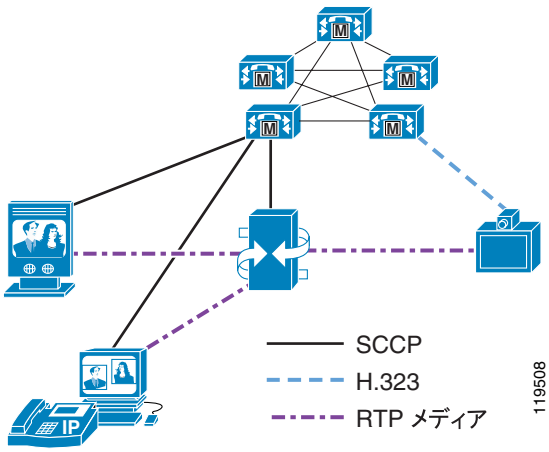
（詳細については、P.15-18 の「メディア リソース グループとメディア リソース グループ リスト」を参照してください）。この設定を行うと、電話機のソフトキーはグレーアウトされます。ユーザはこのエンドポイントで、保留、既存のコールとの会議、既存のコールへの参加、このエンドポイントを含む既存のコールへの割り込みなど、補足サービスを呼び出せなくなります。

（注） ここで説明した回避策には MTP デバイスを含まない MRGL が必要になるため、RSVP ベースのコール アドミッション制御を使用している場合、この回避策は使用できません。

MeetMe ソフトキーによる予約なしの会議の場合は、他のエンドポイントで使用されているシグナリング プロトコルが保留および転送をサポートしている必要はありません。これらのタイプの会議では、各エンドポイントが、会議を開始した SCCP クライアントで割り当てられた MeetMe ダイヤルイン番号をダイヤルします。

図 15-7 は、H.323 エンドポイントと SCCP エンドポイントを同じ SCCP 会議に参加させる方法を示しています。この例では、SCCP エンドポイントで Conf ソフトキーによって会議が開始され、3 人のメンバーが招待されています。

図 15-7　SCCP エンドポイントと H.323 エンドポイントの間の Ad-Hoc 会議



SCCP 会議は、Voice-Activated モードと Continuous-Presence をサポートします。さらに、SCCP 会議は、MCU に内蔵されたソフトウェアベースの MP、Rate Matching（RM）モジュール、および Enhanced Media Processor（EMP）モジュールをサポートします。

メディア リソース グループとメディア リソース グループ リスト

Cisco Unified CallManager は、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）を使用して、指定されたエンドポイントに使用するコンファレンス ブリッジ リソースを決定します。リソースをグループ化する方法は完全に自由ですが、地理的な配置（指定されたサイトのすべてのエンドポイントが、最も近い MCU を使用する）またはエンドポイントのタイプ（ビデオ対応エンドポイントがビデオ対応 MCU を使用し、音声のみのエンドポイントは別のコンファレンス ブリッジ リソースを使用する）でグループ化することが一般的です。SCCP デバイスのユーザが Conf、Join、または MeetMe ソフトキーをアクティブにした場合、Cisco Unified CallManager は発信側エンドポイントの MRGL を使用して、使用するコンファレンス ブリッジを決定します。

Cisco Unified CallManager は、次の基準をリストの順に適用して、使用するコンファレンス ブリッジ リソースを選択します。

1. メディア リソース グループ リスト（MRGL）にリストされているメディア リソース グループ（MRG）の優先順位
2. 選択された MRG の中で、最も使用されていないリソース

このように選択されるため、ユーザがビデオ対応 SCCP エンドポイントで Conf、Join、または MeetMe ソフトキーをアクティブにしたときにビデオ対応 MCU が選択されるようにするには、ビデオ対応 SCCP エンドポイントの MRGL の最上位にビデオ対応 MCU を置く必要があります。ただし、エンドポイントによっては、ビデオ専用エンドポイントでないことがあります。たとえば、Cisco Unified Video Advantage と組み合せて使用される IP Phone は、ほとんどの場合は音声のみのコールに使用され、まれにビデオに使用されることもあります。したがって、この電話機の MRGL の最上位に MCU を配置すると、ビデオ対応の参加者がいない音声のみの会議にも、この MCU が常に選択されます。このシナリオでは、音声のみの会議で MCU リソースが浪費され、ビデオ会議の要求が発生したときに使用できなくなることがあります。

そのため、MRGL でビデオ対応 MCU リソースにアクセスできるユーザは、慎重に選択することをお勧めします。選択するときは、次の考慮事項が役立ちます。

- エンドポイントは、ビデオ専用デバイス（Sony 社製または Tandberg 社製の SCCP エンドポイントなど）か、関連付けられている Cisco Unified Video Advantage クライアントをときどき使用するだけの IP Phone か。
- そのユーザが SCCP 会議を呼び出すときに、ビデオが必要か、音声のみで十分か。
- SCCP 会議の要件を満たす十分なリソースをネットワークに提供するために、どのくらいの費用を MCU リソースに費やすことができるか。

これらの選択基準に対する答えは、企業ごとに異なります。ある企業は、マルチポイント ビデオが不可欠な機能で、いくつかのポートが音声のみの会議で浪費されてもすべてのビデオ会議に使用できるリソースが残るように、十分な MCU リソースをネットワークに提供するために必要な費用を費やします。Sony 社製および Tandberg 社製のエンドポイントだけでビデオ リソースを有効にして、Cisco Unified Video Advantage ユーザには音声のみのコンファレンス ブリッジ リソースを割り当てる企業もあります。あるいは、すべての Sony 社製および Tandberg 社製の SCCP エンドポイントと、選択された Cisco Unified Video Advantage ユーザ（管理職以上など）に対してビデオ リソースを有効にして、その他のユーザの実装には音声のみのリソースを割り当てる企業もあります。

H.323 および SIP MCU リソース

H.323 または SIP モードで設定すると、MCU は MC 機能を提供し、Cisco Unified CallManager への H.323 または SIP ピアのように動作します。H.323 および SIP MCU 会議は多くの方法で呼び出せますが、それらの方法は主に次の 2 つのカテゴリに分類できます。

- スケジュール済み
- 予約なし

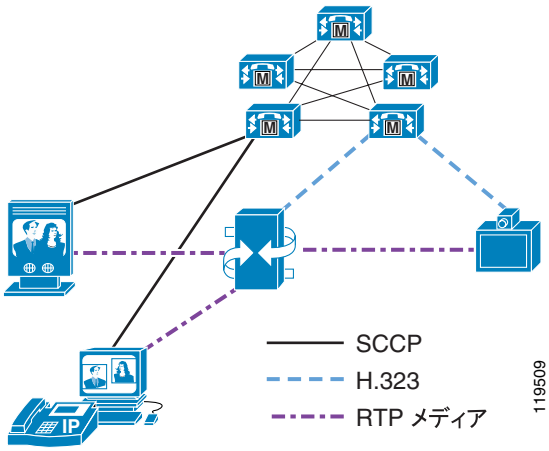
スケジュール済みの会議は、コールの前に、スケジューリング アプリケーションを使用して MCU リソースを予約します。スケジューリング機能は、通常、Cisco Unified MeetingPlace、MagicSoft VCWizard、RADVision VCS、Tandberg 社製 TMS、FVC.COM Click to Meet などの Web ベースのユーザ インターフェイスで提供されます。スケジューリング アプリケーションは、通常、会議の日付と時刻、会議用に予約されているポートの数、ダイヤルイン情報をユーザに提供する招待情報を生成します。または、会議の開始時に参加者の一部、またはすべてにダイヤル アウトするようにスケジューリング システムを設定できます。

予約なしの会議の場合、MCU には、オンデマンドで使用できる一定の数のリソースがあります。会議を作成するため、ユーザはいつでも MCU にダイヤルインするだけで済みます。そのユーザが最初にダイヤルした参加者である場合、MCU は、サービス テンプレートで定義された設定を使用して、動的に新しい会議を作成します（サービス テンプレートの詳細については、P.15-20 の「サービス テンプレートとプレフィックス」を参照してください）。同じ会議番号にダイヤルインした後続のユーザは、この会議に参加します。

スケジュール済みまたは予約なしの H.323 または SIP 会議の作成と参加は、任意のタイプのエンドポイントでできます。たとえば、SCCP エンドポイントが H.323 MCU にダイヤルインして、H.323 エンドポイントと同様に予約なしの会議を作成できます。

図 15-8 は、H.323 エンドポイントと SCCP エンドポイントを同じ H.323 会議に参加させる方法を示しています。この例では、H.323 MCU にダイヤルインして新しい予約なしの会議を作成した SCCP エンドポイントによって会議が開始され、他の 2 人の参加者が、後で会議にダイヤルインしています。

図 15-8　予約なしの会議の SCCP および H.323 エンドポイント



H.323 および SIP 会議は、Voice-Activated モードと Continuous-Presence モードの両方をサポートします。さらに、H.323 会議は、MCU に内蔵されたソフトウェアベースの MP、Rate Matching（RM）モジュール、および Enhanced Media Processor（EMP）モジュールなど、すべての MP タイプをサポートします。

サービス テンプレートとプレフィックス

MCU のサービスは、各会議に関係する設定を定義します。異なるタイプの会議に、異なるサービスを定義できます。各サービスは、少なくとも、次の設定を定義します。

- 会議の速度（ビデオ ビットレート）

  レート変換対応 MP を使用している場合、この設定に複数の速度が含まれることがあります。
- 参加者の最小数および最大数

  最小数は、会議の開始時に予約されるポートの数を定義します。最大数は、MCU がこの会議への参加を許可する参加者の最大数を定義します。
- ビデオ コーデック タイプ（H.261、H.263、または H.264）
- フレーム レート（15 または 30 fps）
- 解像度（QCIF または CIF）

- MP リソース（Auto、MP、RM、または EMP)
- 表示するビデオ レイアウト（Voice-Activated または Continuous-Presence）

  会議には複数のレイアウトを含めることができ、会議の参加者数が増減したときに変化する動的レイアウトもあります。
- H.323 と SIP、または SCCP

  「SCCP service」チェックボックスが有効（オン）の場合、サービスは SCCP 会議で使用されます。このボックスが無効（オフ）の場合、サービスは H.323 および SIP 会議で使用されます。

H.323 および SIP サービスでは、特定のサービスに到達するために、エンドポイントがダイヤルするサービス プレフィックスに各サービスが割り当てられます。サービス プレフィックスは会議番号の前半の番号を形成し、後半の番号で会議 ID を定義します。この形式によって、同じサービス プレフィックスで複数の会議を同時に実行できます。たとえば、サービス プレフィックスを 555 にして、会議の完全なダイヤル文字列を 7 桁にできます。この方式では、4 桁の会議 ID を使用でき、会議番号は 5550000 ～ 5559999 の範囲になります。ユーザは、会議にアクセスするために全文字列をダイヤルする必要があります。コールを受信すると、MCU はダイヤルされた番号を解析し、サービス プレフィックスとの照合を試行します。ダイヤルされたサービス プレフィックスを判断すると、MCU は残りの番号を会議 ID として使用します。会議 ID がまだ存在しない場合、MCU は、その ID で新しい予約なしの会議を作成します。会議がすでに存在する場合は、その会議にユーザが追加されます。

MCU で H.323 と SIP の両方を同時に有効にする場合は、両方のプロトコルでダイヤル プランを同じにする必要があります。H.323 と SIP の間には、SCCP との間にあるような区別がありません。会議が SIP で作成された場合、MCU はこの会議を H.323 を介して登録します。ゲートキーパーまたは SIP プロキシが登録を拒否した場合、会議は失敗します。

SCCP サービスでもサービス プレフィックスを定義する必要がありますが、ユーザは SCCP サービスに「ダイヤル」インしないため、番号自体に意味はありません。プレフィックスは、Cisco Unified CallManager と SCCP MCU リソースとの間の SCCP 登録メッセージでのみ使用されます。ユーザは、Conf、Join、または cBarge ソフトキーを使用して SCCP MCU 会議にアクセスするか（Ad-Hoc）、Cisco Unified CallManager で割り当てられた MeetMe 番号をダイヤルして会議に参加します（予約なし）。そのため、SCCP サービス プレフィックスに指定した番号は関係ありません。999999 など、任意の番号を自由に指定できます。このプレフィックスは、MCU と Cisco Unified CallManager との間の SCCP シグナリングの外側には公開されません（つまり、ダイヤルすることも、ゲートキーパへの MCU の登録に含むこともできません）。

MCU のサイズの選定

すでに説明したように、現在の MCU モデルは IP/VC 3511 と 3540 です。IP/VC 3511 MCU は固定数のポートをサポートし、IP/VC 3540 MCU はさまざまなモジュール サイズを受け付けるモジュラ システムです。使用可能なポートの合計数を計算するときは、Audio Transcoder Daughter Card と Rate Matching（RM）モジュールまたは Enhanced Media Processor（EMP）モジュールをサポートできるように考慮する必要もあります。そのため、MCU のサイズを計算するときは、次の要素について検討します。

- MCU がサポートできるポート数

  この値は、会議の速度によって異なります。速度が高いほど、サポートされるポートの数は減少します。
- Audio Transcoding Daughter Card がサポートできるポート数

  この値は、会議で使用する音声コーデックによって異なります。
- RM または EMP モジュールがサポートできる会議数

  この値は、トランスレーティングが必要な参加者の数および会議で使用するビューの数によって異なります。

サポートされるポート数に関する特定の情報については、Cisco.com で入手可能な MCU ハードウェアの製品マニュアルを参照してください。可能なバリエーションの数は無限に近いため、具体的な設計ガイダンスをこのマニュアルで示すことは非常に困難です。多くのお客様では、最終的に、SCCP Ad-Hoc 会議、H.323 および SIP の予約なしの会議、および H.323 および SIP のスケジュール済み会議が混在することになります。MCU は、正しい速度とビデオ レイアウトでこれらのすべてのタイプの会議に対応できるサイズにする必要があります。言うまでもなく、この判断はとても複雑です。特定の環境での MCU のサイズの選定にあたっては、代理店にご相談ください。

ダイヤルイン会議の IVR

ダイヤルイン会議は、通常、Interactive Voice Response（IVR; 音声自動応答装置）システムを使用して、参加する会議の会議 ID とパスワード（設定されている場合）の入力をユーザに求めます。次のタイプの IVR と Cisco Unified Videoconferencing 3500 シリーズ MCU を使用できます。

- MCU に内蔵された IVR
- Cisco Unified IP-IVR

MCU の内蔵 IVR には、次の特性があります。

- 会議のパスワードのプロンプトだけを再生できる。

  最初に会議 ID のプロンプトを再生することはできません。つまり、ユーザは参加する会議の会議番号をダイヤルする必要があり、次にその会議のパスワードの入力を求められます。
- インバンドとアウトオブバンド（H.245 英数字）の両方の DTMF をサポートする。
- より柔軟性の高いメニューまたは機能を提供するようにカスタマイズできない。

  カスタマイズできるのは、ユーザに対して再生される録音済み音声ファイルだけです。

ダイヤルイン番号を 1 つにして、会議 ID を入力するようにユーザに求めるには、Cisco Unified IP-IVR と MCU を組み合せて使用します。

Cisco Unified IP-IVR には、次の特性があります。

- （特に）会議 ID とパスワードのプロンプトを再生できる。
- アウトオブバンド DTMF だけをサポートする。

  つまり、発信側デバイスはアウトオブバンド DTMF 方式（H.323 デバイスの H.245 英数字など）をサポートしている必要があります。これらのアウトオブバンド DTMF メッセージは、次に、Cisco Unified CallManager によって Cisco IP IVR サーバにリレーされます。発信側デバイスがインバンド DTMF トーンだけをサポートしている場合、Cisco IP IVR サーバが発信側デバイスを認識しないため、そのデバイスは会議に参加できません。
- 高いカスタマイズ性があり、より柔軟性の高いメニューおよび他の高度な機能を提供できる。

  カスタマイズには、ユーザの会議への参加を許可する前にユーザのアカウントをバックエンド データベースで検証すること、議長が参加するまで参加者をキューに入れることなどが含まれます。

（注） Cisco Unified IP-IVR はアウトオブバンド シグナリングのみをサポートするため、インバンド DTMF トーンを使用する H.323 エンドポイントでは機能しません。

Cisco Unified IP-IVR を使用する場合、ユーザは、MCU に直接ルーティングするルート パターンをダイヤルする代わりに、コールを Cisco Unified IP-IVR サーバにルーティングする CTI ルート ポイントをダイヤルできます。会議 ID の DTMF ディジットを収集した後、Cisco Unified IP-IVR は、MCU にコールをルーティングするルート パターンにコールをルーティングします。この転送操作では、発信側デバイスがメディア チャネルの終了と新しい宛先への再開をサポートしている必要があり

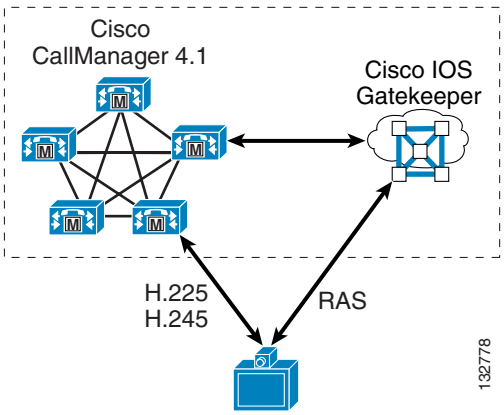
ます。たとえば、Cisco Unified IP-IVR を呼び出す H.323 ビデオ デバイスは、最初に Cisco Unified IP-IVR サーバへの音声チャネルをネゴシエートします。次に、適切な DTMF ディジットが入力された後、MCU に転送します。この時点で Cisco Unified CallManager が、エンドポイントと Cisco Unified IP-IVR サーバとの間の音声チャネルを終了し、エンドポイントと MCU の間で新しい論理チャネルを開く Empty Capabilities Set（ECS）プロシージャを呼び出します。このプロシージャについては、この章ですでに説明しています。H.323 ビデオ エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、コールが切断されるか、最悪の場合、クラッシュしてリブートします。

ゲートキーパー

Cisco Unified CallManager にビデオ サポートが導入されるまで、H.323 ビデオ会議ネットワークは、デバイス登録管理、コール ルーティング、および帯域幅制御を実行するゲートキーパーに依存していました。以前は Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper が、これらの機能を提供します。ただし、シスコ製品を含むほとんどのゲートキーパーは、一般的なエンタープライズクラスの PBX で期待される機能と比較して、基本的なコール ルーティング機能だけを提供します。H.323 ビデオ コールのルーティングに使用する場合、Cisco Unified CallManager が基本的なゲートキーパー機能を補足し、完全なエンタープライズクラスの PBX 機能を H.323 ビデオ コールに提供します。

Cisco Unified CallManager とゲートキーパーはチームとして機能し、H.323 ビデオ エンドポイントを管理します。ゲートキーパーがすべての Registration, Admission, and Status（RAS）シグナリングを処理し、Cisco Unified CallManager がすべての H.225 コール シグナリングと H.245 メディア ネゴシエーションを処理します。そのため、図 15-9 で示すように、ネットワークの H.323 エンドポイントに RAS シグナリング プロシージャが必要な場合は、ゲートキーパーと Cisco Unified CallManager サーバを同時に配置する必要があります。

図 15-9　H.323 エンドポイントに RAS シグナリングを提供する Cisco Unified CallManager と IOS Gatekeeper



次のいずれかの条件が該当する場合、RAS シグナリングが常に必要になります。

- エンドポイントが固定 IP アドレスを使用しない。

  エンドポイントが静的 IP アドレスを使用する場合、Cisco Unified CallManager は、エンドポイントを探すために RAS プロシージャを必要としません。エンドポイントは静的 IP アドレスを使用して Cisco Unified CallManager Administration でプロビジョニングされ、この H.323 クライアントのディレクトリ番号へのコールは、直接静的 IP アドレスにルーティングされます。エンドポイントが静的 IP アドレスを使用しない場合、Cisco Unified CallManager はこのエンドポイントにコールをルーティングするたびに、ゲートキーパーに照会してエンドポイントの現在の IP アドレスを取得する必要があります。

- E.164 アドレスへのコール発信のために、エンドポイントで RAS プロシージャを必要とする。

  ほとんどの H.323 ビデオ会議エンドポイントは、IP アドレスでダイヤルする場合に限り、別のエンドポイントに直接ダイヤルできます（ユーザが宛先エンドポイントの IP アドレスをドット付き 10 進表記で入力し、コール ボタンを押す）。ただし、ユーザが E.164 形式の番号（IP アドレスのドット付き 10 進表記ではない数値）または H.323-ID（*ユーザ名*または*ユーザ名 @ ドメイン*の形式）をダイヤルする場合、ほとんどのエンドポイントは、現在、これらの宛先タイプを解決する方法としてゲートキーパーへの RAS 照会だけを提供します。ただし、E.164 アドレ

スへのコールが RAS プロシージャをスキップし、H.225 SETUP メッセージを指定された IP アドレスに直接送信するように設定できるエンドポイントの数が増えています。この操作方式は、ピアツーピア モードと呼ばれます。このモードを使用する例としては Tandberg 社製 H.323 エンドポイントがあり、登録するゲートキーパー アドレスを設定することも、使用する Cisco Unified CallManager サーバの IP アドレスを設定することもできます。後者の場合、エンドポイントはすべてのコールを指定された IP アドレスに直接送信し、ゲートキーパーの RAS プロシージャを必要としません。

H.323 ビデオ エンドポイントの RAS プロシージャの管理に加え、ゲートキーパーは、大規模なマルチサイト分散コール処理環境でのダイヤル プラン解決および Cisco Unified CallManager クラスタ間の帯域幅制限の管理において、重要な役割を果たしています。ゲートキーパーは、組織内の多数の H.323 VoIP ゲートウェイを統合できます。また、エンタープライズ IP Telephony ネットワークとサービス プロバイダー VoIP 転送ネットワークの間でセッション ボーダー コントローラとして機能します。

そのため、Cisco IP Video Telephony 配置に関しては、Cisco IOS Gatekeeper は次の役割の一方または両方を実行できます。

- エンドポイント ゲートキーパー

  エンドポイント ゲートキーパーは、H.323 クライアント、MCU、および H.320 ビデオ ゲートウェイを宛先または発信元とするコール、およびこれら相互間のコールのすべての RAS プロシージャを管理するように設定されます。エンドポイント ゲートキーパーは、Cisco Unified CallManager がすべての H.225 コール ルーティングおよび H.245 メディア ネゴシエーションを実行できるように、これらのすべてのコールを適切な Cisco Unified CallManager クラスタに転送します。

- インフラストラクチャ ゲートキーパー

  インフラストラクチャ ゲートキーパーは、Cisco Unified CallManager クラスタ間、Cisco Unified CallManager クラスタと H.323 VoIP ゲートウェイのネットワーク間、および Cisco Unified CallManager クラスタとサービス プロバイダーの H.323 VoIP 転送ネットワーク間のすべてのダイヤル プラン解決および帯域幅制限（コール アドミッション制御）を管理するように設定されます。

Cisco Unified CallManager Release 4.0 では、エンドポイント ゲートキーパーとインフラストラクチャ ゲートウェイは別々のルータで実行する必要があり、各エンドポイント ゲートキーパーは単一の Cisco Unified CallManager クラスタだけにサービスを提供できました。企業内に複数の Cisco Unified CallManager クラスタがある場合は、各 Cisco Unified CallManager クラスタごとに、個別のエンドポイント ゲートキーパーを配置する必要がありました。Cisco Unified CallManager Release 4.1 以降では、これらの役割を単一のゲートキーパーに組み合せて、1 つ以上の Cisco Unified CallManager クラスタのエンドポイント ゲートキーパーとして使用しながら、クラスタ間またはクラスタと他の H.323 VoIP ネットワーク間のコールを管理するインフラストラクチャ ゲートキーパーとして使用できます。ただし、（特に）次の理由により、これらの役割は複数のゲートキーパーに分割することをお勧めします。

- スケーラビリティ

  配置する Cisco IOS ルータ プラットフォーム、および混雑時のコール量の概算によっては、負荷を処理するゲートキーパーが複数必要になることがあります。

- 地理的な復元性

  1 台のゲートキーパーでネットワーク全体をカバーすることは、大規模な国際 VoIP ネットワークにおいて、賢明な方法ではありません。複数のゲートキーパーをネットワーク全体に（一般的には地理的に）分散して配置すると、1 つのゲートキーパーが故障した場合に、より適切に障害を切り分けることができます。

- 非互換性

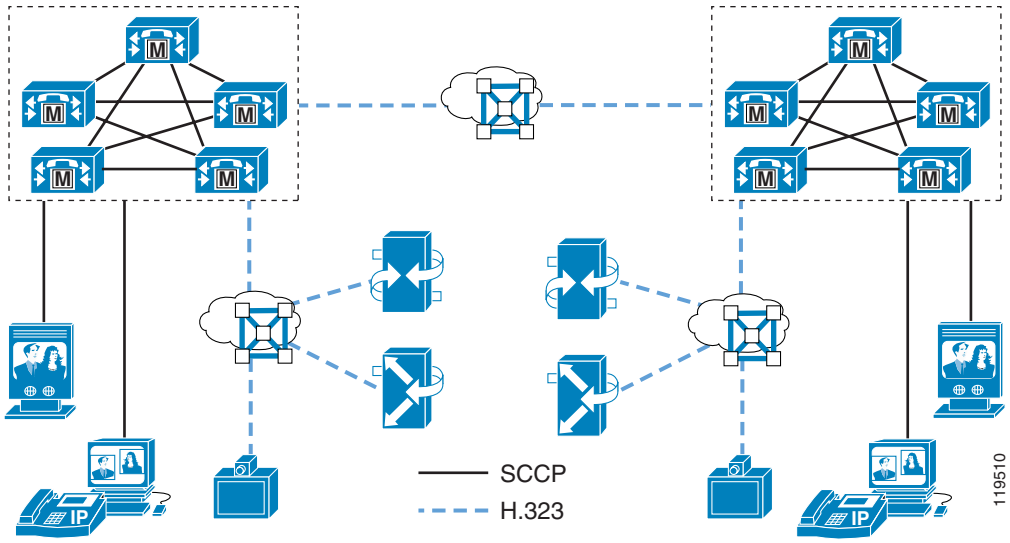
  ゲートキーパーの設定の中には、グローバルな性質（そのゲートキーパーに登録されているすべてのエンドポイントに関連する性質）を持つものがあります。たとえば、コマンド **arq reject-unknown-prefix** は、一部の H.323 VoIP 転送環境では便利ですが、Cisco Unified CallManager

へのコールをルーティングするエンドポイント ゲートキーパーで使用される **gw-type-prefix** < *プレフィックス* > **default-technology** コマンドと衝突します。Cisco IOS では両方のコマンドを同じゲートキーパーで設定することは禁止されていませんが、**arq reject-unknown-prefix** コマンドが優先されるため、不明な番号へのコールは Cisco Unified CallManager にルーティングされず、拒否されます。この場合は、H.323 VoIP 転送ネットワーク用に 1 つのゲートキーパーを使用し、別のゲートキーパーを Cisco Unified CallManager クラスタに使用します。

非互換性のもう 1 つの例は、冗長性のためにゲートキーパーを設定する際に発生することがあります。Cisco Voice Gateways や Cisco Unified CallManager など、ほとんどの Cisco H.323 音声デバイスは、Gatekeeper Update Protocol（GUP）を使用して相互に同期するゲートキーパー クラスタとしてゲートキーパーを設定可能な H.323v3 Alternate Gatekeeper 機能をサポートします。ただし、多くの H.323 ビデオ エンドポイントは Alternate Gatekeeper をサポートしないため、冗長性のために Hot Standby Routing Protocol（HSRP; ホットスタンバイ ルータ プロトコル）を使用するようにゲートキーパーを設定する必要があります。これらの 2 つの冗長性方式を同じゲートキーパーに混在させ、組み合せることはできません。この場合、Alternate Gatekeeper をサポートするエンドポイント用にゲートキーパー クラスタを使用するか、サポートしないエンドポイント用にゲートキーパーの HSRP ペアを使用するかを決定します。

図 15-10 は、2 つの Cisco Unified CallManager クラスタがあるネットワーク シナリオを示しています。各クラスタは、SCCP クライアント、H.323 クライアント、H.323 MCU、および H.320 ゲートウェイで構成されています。H.323 クライアント、MCU、および H.320 ゲートウェイの RAS 部分を管理するために、エンドポイント ゲートキーパーを各クラスタに配置します。別のインフラストラクチャ ゲートキーパーが、クラスタ間のダイヤル プラン解決と帯域幅を管理します。この図ではゲートキーパーの冗長性は示されていませんが、これらの各ゲートキーパーは、実際には Alternate Gatekeeper または HSRP ベースの冗長性を持つように設定された複数のゲートキーパーです。

図 15-10　2 つの Cisco Unified CallManager クラスタと必要なゲートキーパー



サポートされるゲートキーパー プラットフォーム

Cisco Unified CallManager 4.1 以降を使用するエンドポイント ゲートキーパーとして機能するには、Cisco IOS Gatekeeper で Cisco IOS Release 12.3(11)T 以降を実行する必要があります。インフラストラクチャ ゲートキーパーの最小 Cisco IOS リリース要件については、P.A-1 の「推奨されるハードウェアと ソフトウェアの組み合せ」を参照してください。

次のルータ プラットフォームが Cisco IOS Gatekeeper をサポートしています。

- Cisco 2600XM シリーズおよび 2691
- Cisco 2800 シリーズ
- Cisco 3640、3640A、3660
- Cisco 3725 および 3745
- Cisco 3825 および 3845
- Cisco 7200 シリーズ、7301、および 7400 シリーズ

ルータ プラットフォームで使用する必要があるリリースと機能を判断するには、次の URL にある *Cisco Feature Navigator* を使用します（Cisco.com ログイン アカウントが必要）。

http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp

詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/vvfax_c/callc_c/h323_c/ipipgw/ipftgde.htm

この資料には、Cisco IOS Release 12.3(11)T が統合音声およびビデオ サービスを提供すると記載されています。そのため、これが推奨される最小リリースになります。

エンドポイント ゲートキーパー

次の条件の両方が該当する場合は、エンドポイント ゲートキーパーが必要です。

- クラスタに H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ（集合的に H.323 エンドポイントと呼ぶ）が含まれている。これらのタイプのエンドポイントが存在しない場合（たとえば、すべてのクライアントが SCCP エンドポイントで、MCU も H.320 ゲートウェイもない場合）、エンドポイント ゲートキーパーは不要です。
- 次の条件のいずれかに当てはまる。
  - E.164 アドレスへのコール発信のために、H.323 エンドポイントで RAS プロシージャを必要とする。すでに述べたように、ピアツーピア コール シグナリングに対応するデバイスが増えています。これらのデバイスは、ゲートキーパーに登録する必要はありません。
  - H.323 エンドポイントが静的 IP アドレスを使用しない。

エンドポイント ゲートキーパーの役割は、これらの H.323 エンドポイントを登録する場所を提供し、エンドポイントとの通信の RAS 部分を処理するだけです。エンドポイント ゲートキーパーは、これらのエンドポイントが宛先または発信元となるコール、またはこれらのエンドポイント間のすべてのコール要求に対応して、Cisco Unified CallManager がすべてのコール ルーティング機能および帯域幅制御機能を実行できるように、コールを適切な Cisco Unified CallManager サーバに転送します。このコール ルーティング制御および帯域幅制御を実現するには、H.323 トランクをゲートキーパーに登録するように Cisco Unified CallManager を設定し、ゾーンへのコール、ゾーンからのコール、またはゾーン内のコールをすべてこれらのトランクにルーティングするようにゲートキーパーを設定します。

Cisco Unified CallManager Release 4.1 では、RASAggregator トランクという新しいタイプの H.323 トランクが導入されました。このタイプのトランクは、すべての H.323 クライアント、H.323 MCU、または H.320 ゲートウェイ ゾーンに使用されます。一方、以前の Cisco Unified CallManager リリー

スからのゲートキーパー制御クラスタ間トランクおよびゲートキーパー制御 H.225 トランクは、インフラストラクチャ ゲートキーパーとの統合に使用されます。『*IP Video Telephony SRND for Cisco Unified CallManager 4.0*』に記載された推奨事項に基づいて H.323 ビデオ エンドポイントを配置した場合は、新しい RASAggregator トランクを使用してその柔軟性を利用できるように設定を修正する必要があります。この設定変更は慎重に計画し、管理者の都合の良いときに実行することで、既存の H.323 ビデオ エンドポイントの中断を最小限にする必要があります。Cisco Unified CallManager 4.0 配置からの移行手順については、P.15-47 の「Cisco Unified CallManager 4.0 からの移行」を参照してください。

H.323 クライアントのプロビジョニング

H.323 クライアントは、他の電話機とほぼ同じ方法でプロビジョニングされます。新しい電話機（モデル タイプ = H.323 Client）を作成し、ディレクトリ番号を割り当て、コーリング サーチ スペース、デバイス プールなどを割り当てます。Cisco Unified CallManager で H.323 クライアントは、次のいずれかの方法で設定します。使用する方法は、クライアントが静的 IP アドレスを使用するかどうか、クライアントで E.164 アドレスをダイヤルする RAS プロシージャが必要かどうかによって異なります。

- ゲートキーパー制御

  このタイプの設定は、静的 IP アドレスが割り当てられていないクライアント（DHCP 割り当てアドレスを使用するクライアント）で、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。これらのクライアントとの通信には、RASAggregator トランクを使用します（図 15-11 および図 15-12 を参照）。

- 非ゲートキーパー制御、非同期

  このタイプの設定は、静的 IP アドレスが割り当てられているクライアントで、E.164 アドレスをダイヤルする RAS プロシージャが必要な場合に使用します。Cisco Unified CallManager はゲートキーパーを必要せずに直接シグナルを送信して IP アドレスを解決できますが、クライアントは Cisco Unified CallManager に直接シグナルを送信できず、ダイヤルしようとしている E.164 アドレスを解決するためにゲートキーパーに照会する必要があります（非同期通信）。このタイプのクライアントをサポートするには、実際にはすべてのクライアントが静的 IP アドレスを使用していても、ゲートキーパーのゾーンごとに 1 つ以上のゲートキーパー制御クライアントを Cisco Unified CallManager で定義する必要があります。この場合、非ゲートキーパー制御クライアントは、実際には存在しない「ダミー」クライアントになります。定義する目的は、ゲートキーパーがクライアントから Cisco Unified CallManager へのコールをルーティングできるように、RASAggregator トランクを作成することだけです（図 15-13 および図 15-14 を参照）。

- 非ゲートキーパー制御、同期

  このタイプの設定は、クライアントが静的 IP アドレスを持ち、ピアツーピア シグナリングに対応している（E.164 番号をダイヤルする RAS プロシージャが必要ない）場合に使用します。Cisco Unified CallManager は直接シグナルを送信でき、クライアントは Cisco Unified CallManager に直接シグナルを送信できます（同期通信）。このタイプのクライアントには、ゲートキーパーまたは RASAggregator トランクが不要です（図 15-15 および図 15-16 を参照）。

図 15-11 から図 15-16 は、これら 3 つのシナリオで使用されるシグナリング フローを示しています。

図 15-11　Cisco Unified CallManager からゲートキーパー制御クライアントへのコール

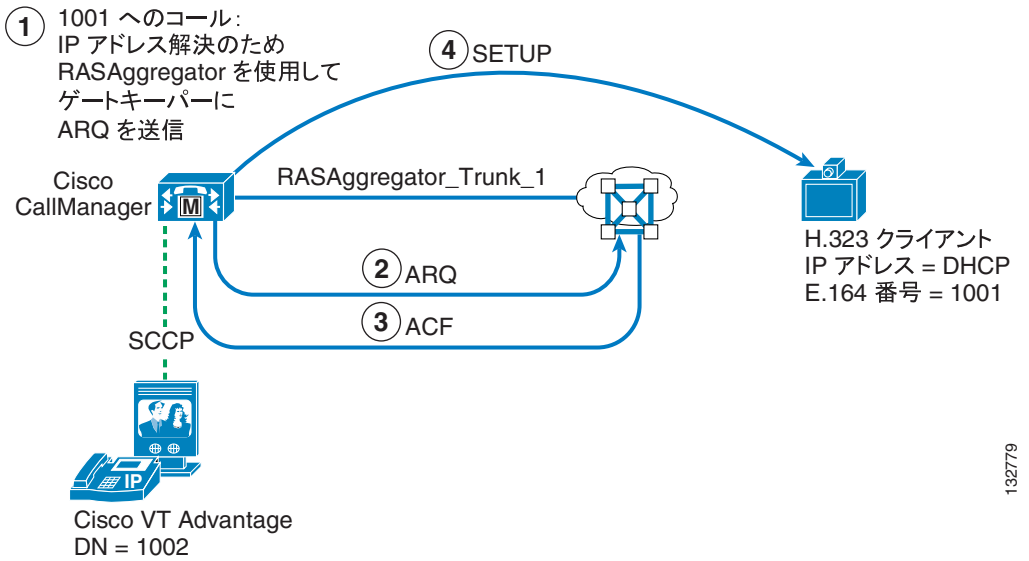


図 15-12　ゲートキーパー制御クライアントから Cisco Unified CallManager へのコール

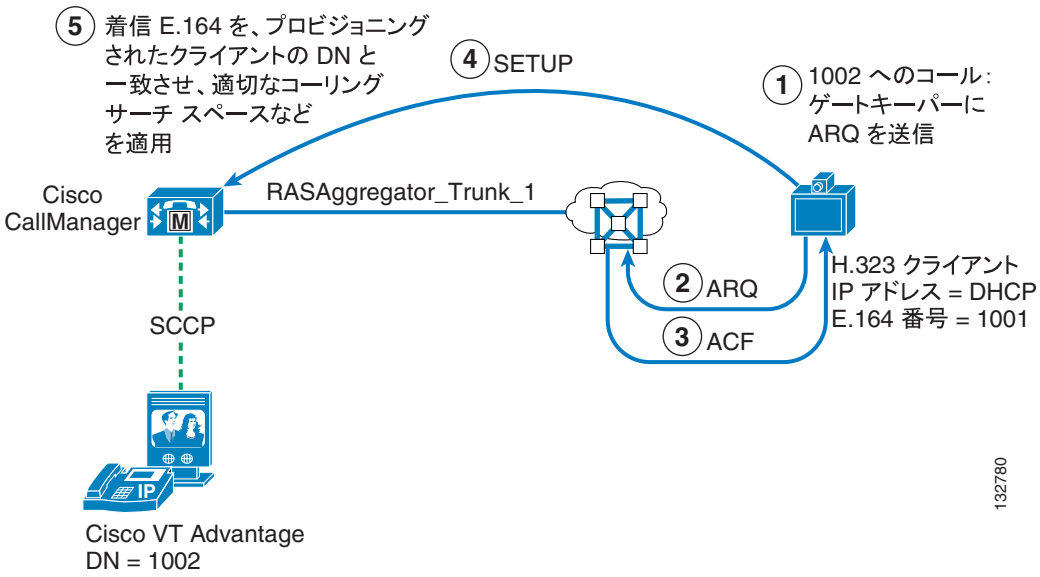


図 15-13　Cisco Unified CallManager から非ゲートキーパー制御クライアントへのコール（非同期）

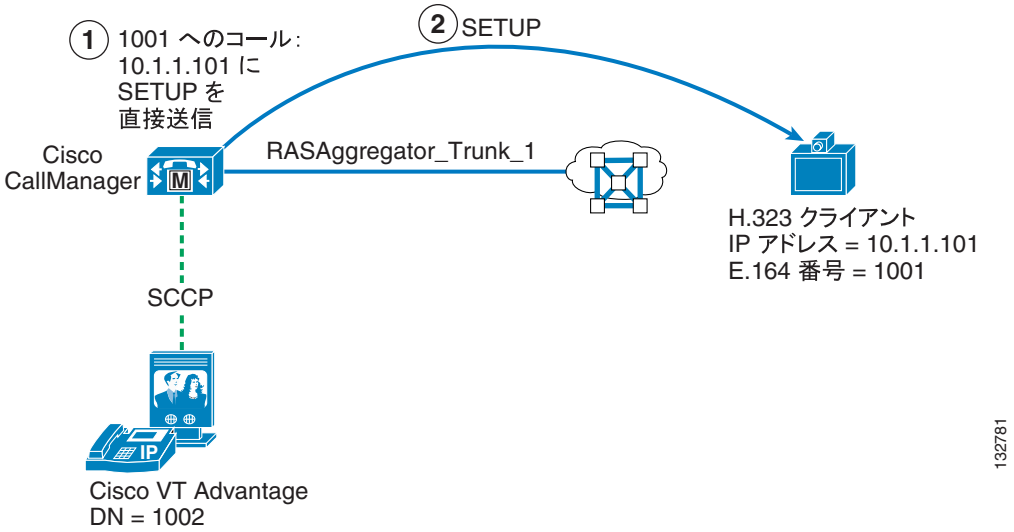


図 15-14　非ゲートキーパー制御クライアントから Cisco Unified CallManager へのコール（非同期）

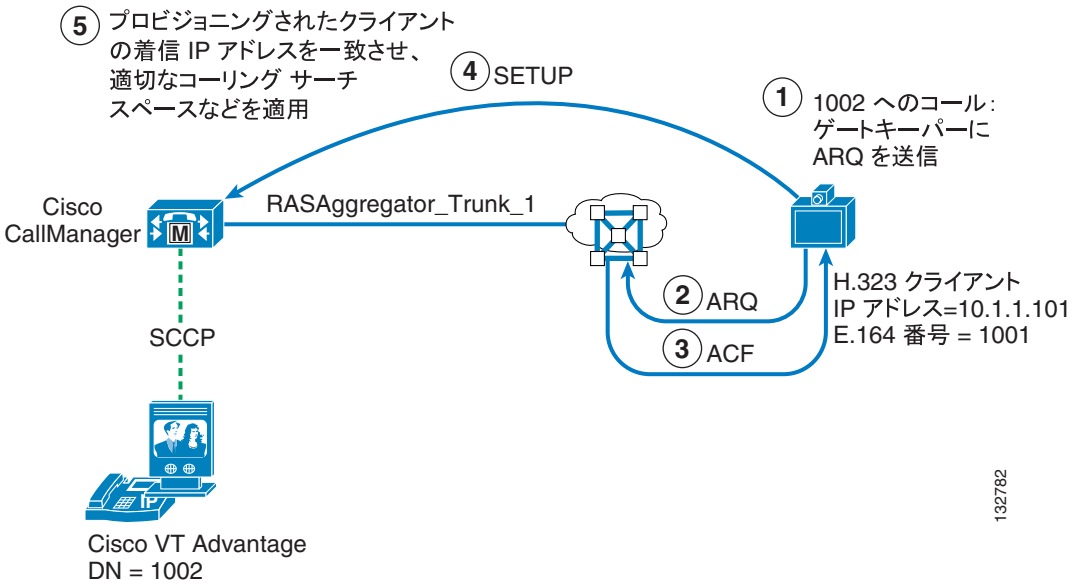


図 15-15　Cisco Unified CallManager から非ゲートキーパー制御クライアントへのコール（同期）

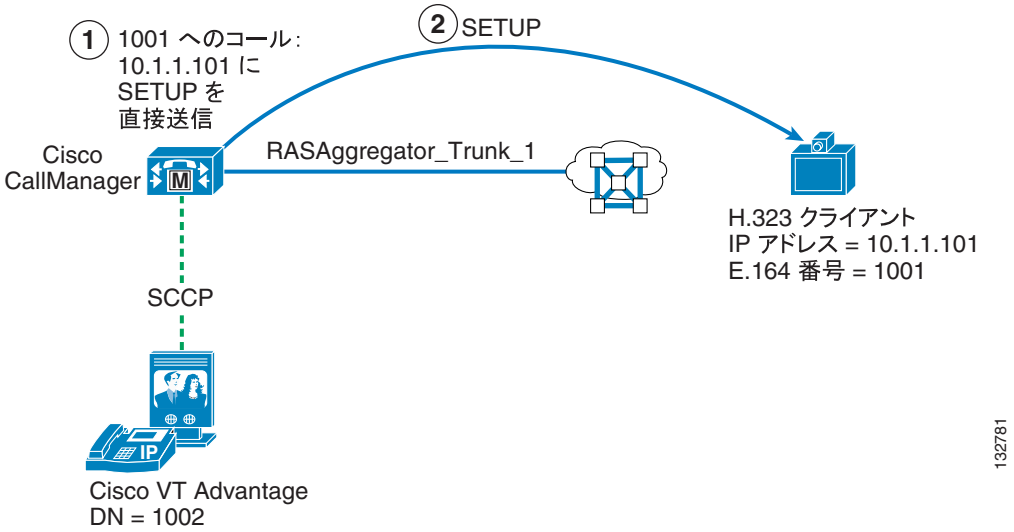
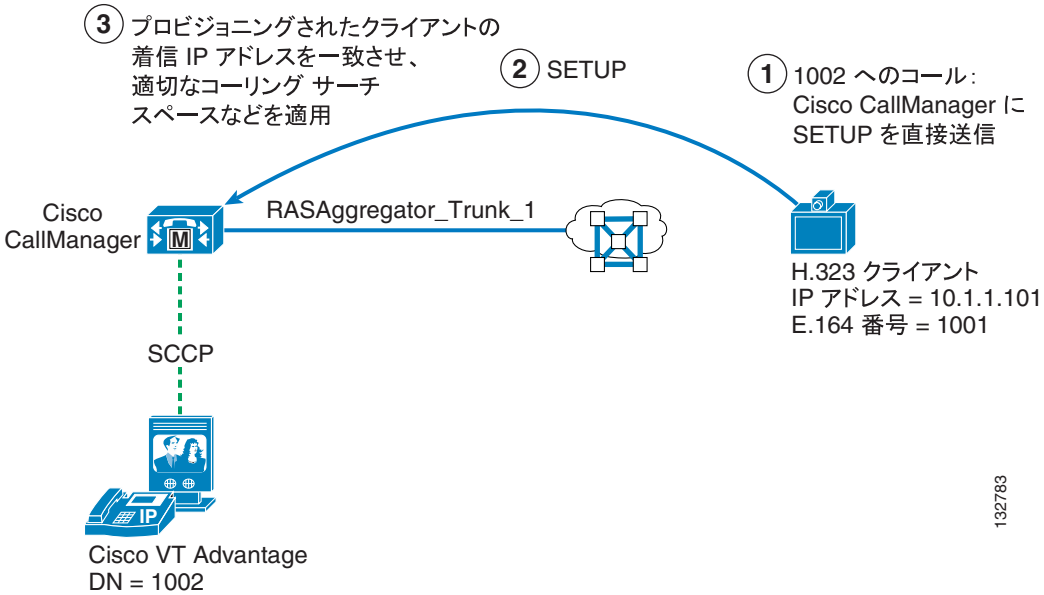


図 15-16　非ゲートキーパー制御クライアントから Cisco Unified CallManager へのコール（同期）



ゲートキーパー制御クライアント

H.323 クライアントをゲートキーパー制御として設定するときは、任意の英数字文字列（わかりやすい名前など）を Device Name フィールドに入力し、**Gatekeeper-controlled** ボックスをオンにして、次のフィールドに入力します。

- Device Pool

  クライアントで使用するデバイス プール。同じゾーンに登録されているすべての H.323 クライアント（ゲートキーパー制御と非ゲートキーパー制御の両方）が、同じデバイス プールを使用する必要があります。間違ってエンドポイントの間で異なるデバイスプールが割り当てられた場合、Cisco Unified CallManager は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Cisco Unified CallManager で拒否されます。

- Gatekeeper

  ゲートキーパー IP アドレスのドロップダウン リスト。ゲートキーパー制御 H.323 クライアントを設定する前に、Cisco Unified CallManager でゲートキーパーを定義する必要があります。

- Technology Prefix

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じテクノロジー プレフィックスを使用する必要があります。間違ってエンドポイントの間で異なるテクノロジー プレフィックスが割り当てられた場合、Cisco Unified CallManager は複数の RASAggregator トランクをゾーン内で登録し、着信コールが間違った RASAggregator トランクに転送されても、Cisco Unified CallManager で拒否されます。このプレフィックスには **1#** を使用することをお勧めします。

- Zone Name

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。同じゾーンに登録されているすべてのゲートキーパー制御 H.323 クライアントが、同じゾーン名を使用する必要があります。間違ってエンドポイントの間で異なるゾーン名（このフィールドは大文字と小文字が区別されます)が割り当てられた場合、Cisco Unified CallManager は複数の RASAggregator トランクをゲートキーパーに登録しようとし（ただし、ゾーン名が不正なトランクは登録に失敗します）、着信コールが間違った RASAggregator トランクに転送されても、Cisco Unified CallManager で拒否されます。

また、Cisco CallManager サービス パラメータの **Send Product ID and Version ID** を **True** に設定する必要があります。このパラメータによって、ゲートキーパーがクライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できるように、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。

非ゲートキーパー制御クライアント

H.323 クライアントを非ゲートキーパー制御としてプロビジョニングする場合は、クライアントの静的 IP アドレスを Device Name フィールドに入力し、Gatekeeper-controlled セクションの下のその他のすべての設定をブランク（オフ）のままにします。コールがこのディレクトリ番号にルーティングされると、Cisco Unified CallManager は静的 IP アドレスを使用してクライアントに転送します。

クライアントがピアツーピア モードを使用するように設定されている場合、これ以上の設定は不要です。クライアントで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- Device Name

  クライアント ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  非ゲートキーパー制御 H.323 クライアントを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、実際のクライアントに割り当てられたデバイス プールと異なる場合、実際のクライアントからの着信コールが Cisco Unified CallManager で拒否されることがあります。

- Gatekeeper

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Cisco Unified CallManager でゲートキーパーを定義する必要があります。

- Technology Prefix

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのクライアント ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- Zone Name

  ゲートキーパーで設定されているクライアント ゾーンの名前（大文字と小文字が区別されます）。

また、Cisco CallManager サービス パラメータの **Send Product ID and Version ID** を **True** に設定する必要があります。このパラメータによって、ゲートキーパーがクライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できるように、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。

H.323 MCU のプロビジョニング

H.323 MCU は、Cisco Unified CallManager で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、MCU の静的 IP アドレスおよび TCP シグナリング ポートを Device Name フィールドに入力する必要があります。コールが MCU に関連付けられたルート パターンと一致すると、Cisco Unified CallManager は静的 IP アドレスと TCP ポートを使用して、MCU に到達します。

（注） Cisco Unified Videoconferencing 3500 シリーズ MCU は、デフォルトでは TCP ポート 1720 を監視しません（IP/VC 3500 シリーズ MCU は、デフォルトでポート 2720 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Cisco Unified CallManager でプロビジョニングする必要があります。

MCU がピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です（Cisco Unified Videoconferencing MCU は、現在、ピアツーピア モードをサポートしていませんが、一部のサードパーティ製 MCU がサポートしています）。MCU で E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- Device Name

  MCU ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  MCU を表す H.323 ゲートウェイを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、MCU を表す H.323 ゲートウェイに割り当てられたデバイス プールと異なる場合、MCU からの着信コールが Cisco Unified CallManager で拒否されることがあります。

- Gatekeeper

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Cisco Unified CallManager でゲートキーパーを定義する必要があります。

- Technology Prefix

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーの MCU ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- Zone Name

  ゲートキーパーで設定されている MCU ゾーンの名前（大文字と小文字が区別されます）。

また、Cisco CallManager サービス パラメータの **Send Product ID and Version ID** を **True** に設定する必要があります。このパラメータによって、ゲートキーパーがクライアント ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、MCU ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できるように、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。

MCU サービス プレフィックス

H.323 MCU は、実行中の予約なしまたはスケジュール済みの H.323 会議に到達するダイヤルイン番号として、E.164 アドレスまたはテクノロジー プレフィックス（MCU ではサービス プレフィックスとも呼ばれる）を使用できます。MCU 管理画面で MCU Mode を **Gateway** ではなく **MCU** に設定して、E.164 アドレスを使用するように MCU を設定することをお勧めします。使用している MCU のモデルで **MCU** 設定を使用できない場合は、次の特別な設定を使用して、他の H.323 エンドポイントから MCU に発信されたコールを適切にルーティングします。

MCU が **Gateway** モードに設定されている場合、または、別のベンダーの MCU で、（何らかの理由で）会議 ID を E.164 アドレスではなくテクノロジー プレフィックスとして登録する必要がある場合は、MCU のサービス プレフィックスの先頭を **#** 文字にする必要があります。たとえば、MCU サービス プレフィックスが 8005551212 の場合、MCU でサービス プレフィックスを #8005551212 としてプロビジョニングする必要があります。その結果、他の H.323 エンドポイントが 8005551212 とダイヤルすると、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、コールを発信したエンドポイントのゾーンでデフォルト テクノロジー プレフィックスと共に登録された RASAggregator トランクにコールをルーティングします。Cisco Unified CallManager は、コールを MCU にルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。この文字は、MCU を表す H.323 ゲートウェイに関連付けられたルート パターンに付加されます。そのため、SCCP クライアントから MCU へのコールでも、着信番号にこの # 文字が付加されます。

MCU が **MCU** モードで設定されている場合、または E.164 アドレスを会議 ID に使用する別のベンダーの MCU である場合、# 文字を付加する必要はありません。MCU がピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合もこの条件は当てはまらず、# 文字を付加する必要はありません。

H.320 ゲートウェイのプロビジョニング

H.323 MCU と同様に、H.320 ゲートウェイも、Cisco Unified CallManager で H.323 ゲートウェイとしてプロビジョニングされてから、これらのデバイスにコールをルーティングするルート パターンが設定されます。H.323 ゲートウェイをプロビジョニングするときは、H.320 ゲートウェイの静的 IP アドレスおよび TCP シグナリング ポートを Device Name フィールドに入力する必要があります。コールがゲートウェイに関連付けられたルート パターンと一致すると、Cisco Unified CallManager は静的 IP アドレスと TCP ポートを使用して、ゲートウェイに到達します。

(注) Cisco Unified Videoconferencing 3500 シリーズ ゲートウェイは、デフォルトでは TCP ポート 1720 を監視しません（IP/VC 3500 シリーズ ゲートウェイは、デフォルトでポート 1820 を監視します）。監視している TCP ポートを確認し、1720 に変更するか、正しいポートを Cisco Unified CallManager でプロビジョニングする必要があります。

ゲートウェイがピアツーピア モードを使用するように設定されている場合は、これ以上の設定は不要です。ゲートウェイで E.164 アドレスにコールを発信する RAS プロシージャが必要な場合は、RASAggregator トランクを作成するために、次のフィールドに入力して、ダミーのゲートキーパー制御 H.323 クライアントも設定する必要があります。

- Device Name

  ゲートウェイ ゾーンの RASAggregator トランクの作成を目的とするダミー クライアントとして、クライアントを識別するためのわかりやすい名前。

- Device Pool

  H.320 ゲートウェイを表す H.323 ゲートウェイを設定するときに選択したデバイス プール。ダミー クライアントに割り当てられたデバイス プールが、ゲートウェイに割り当てられたデバイス プールと異なる場合、ゲートウェイからの着信コールが Cisco Unified CallManager で拒否されることがあります。

- Gatekeeper

  ゲートキーパー IP アドレスのドロップダウン リスト。ダミーのゲートキーパー制御 H.323 クライアントを設定する前に、Cisco Unified CallManager でゲートキーパーを定義する必要があります。

- E.164

  このフィールドの入力は必須です。Cisco Unified CallManager で「ダイヤルできない」値にしてください。

- Technology Prefix

  テクノロジー プレフィックスは RASAggregator トランクで使用され、ゲートキーパーのゲートウェイ ゾーンに登録されます。このテクノロジー プレフィックスは、ゲートキーパーでデフォルト テクノロジー プレフィックスとして設定された値と一致している必要があります。このプレフィックスには **1#** を使用することをお勧めします。

- Zone Name

  ゲートキーパーで設定されているゲートウェイ ゾーンの名前（大文字と小文字が区別されます）。

また、Cisco CallManager サービス パラメータの **Send Product ID and Version ID** を **True** に設定する必要があります。このパラメータによって、ゲートキーパーがゲートウェイ ゾーンへの H.323 コール、クライアント ゾーンからの H.323 コール、クライアント ゾーン内の H.323 コールのすべてを RASAggregator トランクに転送できるように、RASAggregator トランクをゲートキーパーに H323-GW として登録できます。

ゲートウェイ サービス プレフィックス

H.320 ゲートウェイは、ユーザが ISDN の宛先に到達するためにダイヤルするプレフィックスとして、テクノロジー プレフィックス（ゲートウェイではサービス プレフィックスとも呼ばれる）を使用します。コールを正しくルーティングするには、ゲートウェイのサービス プレフィックスを # 文字で始まるように設定する必要があります。たとえば、ISDN 番号に到達するためにクライアントがダイヤルするゲートウェイのサービス プレフィックスが 9 の場合、#9 としてゲートウェイでサービス プレフィックスをプロビジョニングする必要があります。この場合、H.323 クライアントが 9 と公衆網番号をダイヤルした場合（918005551212 など）、ゲートキーパーは登録済みの一致するテクノロジー プレフィックスを検索するのではなく、デフォルト テクノロジー プレフィックスと共に登録された Cisco Unified CallManager トランクにコールをルーティングします。Cisco Unified CallManager は、コールをゲートウェイにルーティングする前に、着信番号の先頭に # 文字を付加する必要があります。ゲートウェイがピアツーピア モードを使用しているため、テクノロジー プレフィックスをゲートキーパーに登録する必要がない場合は、この条件は当てはまらず、# 文字を付加する必要がありません。

ゲートキーパー ゾーンの設定

前の項では、Cisco Unified CallManager Administration でエンドポイントをプロビジョニングする方法について説明しました。適切なゾーン定義でエンドポイント ゲートキーパーを設定する必要もあります。Cisco Unified CallManager で、エンドポイントの各タイプ（クライアント、MCU、またはゲートウェイ）にゾーンを設定する必要があり、オプションとして、これらのエンドポイントに関連付けられている各デバイス プールにゾーンを設定します。

各ゾーンは、ゾーンを宛先または発信元とするコール、ゾーン内で発信されるコールのすべてを、ゾーンに登録されている RASAggregator トランクにルーティングするように設定されます。エンドポイント ゲートキーパーでゾーンを設定するには、次のコマンド構文を使用します。

```
zone local <zone_name> <domain_name> <ip_address> invia <zone_name>
outvia <zone_name> enable-intrazone
```

コマンド引数 **invia** は他のゾーンからこのゾーンに発信されたコールに適用され、**outvia** はこのゾーンから他のゾーンに発信するコールに適用されます。**enable-intrazone** は、ゾーン内で発信したコールに適用されます。次の項で、これらのコマンドの使用方法を示します。

クライアント ゾーン

各エンドポイント ゲートキーパー内で設定の必要なクライアント ゾーンの数は、次の要素で決まります。

- H.323 クライアントの関連付け先となるデバイス プール

  デバイス プールは、各 H.323 クライアントの 1 次、2 次、および 3 次 Cisco Unified CallManager サーバを決定します。すべての H.323 クライアントを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるクライアント ゾーンは 1 つだけです。つまり、H.323 クライアントで使用するデバイス プールごとに、ゲートキーパーで個別のクライアント ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Cisco Unified CallManager クラスタにサービスを提供するのか、複数の Cisco Unified CallManager クラスタにサービスを提供するのか

  各クライアント ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Cisco Unified CallManager クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のクライアント ゾーンを定義する必要があります。

説明のために、3 つの例でクライアント ゾーンの設定方法を示します。例 15-1 は、すべての H.323 クライアントが同じデバイス プールに関連付けられた単一の Cisco Unified CallManager クラスタに定義される、単一のクライアント ゾーンを示しています。例 15-2 は、H.323 クライアントが 2 つの異なるデバイス プールに分割された単一の Cisco Unified CallManager クラスタを示しています。例 15-3 は、H.323 クライアントがクラスタごとに 2 つの異なるデバイス プールに分割された 2 つの Cisco Unified CallManager クラスタを示しています。

(注)　以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 15-1　単一の Cisco Unified CallManager クラスタと単一のデバイス プールのクライアント ゾーン

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy clients default inbound-to terminal
no use-proxy clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-2　単一の Cisco Unified CallManager クラスタと 2 つのデバイス プールのクライアント ゾーン

```
gatekeeper
zone local dp1-clients domain.com invia dp1-clients outvia dp1-clients
enable-intrazone
zone local dp2-clients domain.com invia dp2-clients outvia dp2-clients
enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy dp1-clients default inbound-to terminal
no use-proxy dp1-clients default outbound-from terminal
no use-proxy dp2-clients default inbound-to terminal
no use-proxy dp2-clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-3　クラスタあたり 2 つのデバイス プールのある 2 つの Cisco Unified CallManager クラスタのクライアント ゾーン

```
gatekeeper
zone local clstr1-dp1-clients domain.com invia clstr1-dp1-clients outvia
clstr1-dp1-clients enable-intrazone
zone local clstr1-dp2-clients domain.com invia clstr1-dp2-clients outvia
clstr1-dp2-clients enable-intrazone
zone local clstr2-dp1-clients domain.com invia clstr2-dp1-clients outvia
clstr2-dp1-clients enable-intrazone
zone local clstr2-dp2-clients domain.com invia clstr2-dp2-clients outvia
clstr2-dp2-clients enable-intrazone
gw-type-prefix 1# default-technology
no use-proxy clstr1-dp1-clients default inbound-to terminal
no use-proxy clstr1-dp1-clients default outbound-from terminal
no use-proxy clstr1-dp2-clients default inbound-to terminal
no use-proxy clstr1-dp2-clients default outbound-from terminal
no use-proxy clstr2-dp1-clients default inbound-to terminal
no use-proxy clstr2-dp1-clients default outbound-from terminal
no use-proxy clstr2-dp2-clients default inbound-to terminal
no use-proxy clstr2-dp2-clients default outbound-from terminal
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

以前は Cisco Multimedia Conference Manager（MCM）と呼ばれていた Cisco IOS Gatekeeper は、H.323 プロキシ機能を提供していましたが、廃止される予定です。この機能は Cisco Unified CallManager と互換性がありませんが、端末（クライアント）との間のすべてのコールにプロキシを使用するゲートキーパーのコマンドは、まだデフォルトで有効になっています。この機能はクライアント ゾーンごとに、次のコマンド構文で無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] terminals
```

Cisco MCM プロキシは、Cisco IOS Multiservice IP-to-IP Gateway と、それに関連付けられた中継ゾーン対応 Cisco IOS Gatekeeper という新しいソリューションに置き換えられました。このマニュアルでは IP-to-IP ゲートウェイについては説明していませんが、Cisco Unified CallManager Release 4.1 以降は、RASAggregator トランクをゲートキーパーに登録することで中継ゾーンと IP-to-IP ゲートウェイの構成を活用し、効果的に IP-to-IP ゲートウェイを模倣し、ゲートキーパーが IP-to-IP ゲートウェイであるかのように、すべての invia、outvia、および enable-intrazone コールを RASAggregator トランクにルーティングしています。

クライアント ゾーン プレフィックス

H.323 クライアント ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU ゾーン

各エンドポイント ゲートキーパー内で設定の必要な MCU ゾーンの数は、次の要素で決まります。

- MCU の関連付け先となるデバイス プール

  デバイス プールは、各 MCU の 1 次、2 次、および 3 次 Cisco Unified CallManager サーバを決定します。すべての MCU を同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要がある MCU ゾーンは 1 つだけです。つまり、MCU クライアントで使用するデバイス プールごとに、ゲートキーパーで個別の MCU ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Cisco Unified CallManager クラスタにサービスを提供するのか、複数の Cisco Unified CallManager クラスタにサービスを提供するのか

  各 MCU ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Cisco Unified CallManager クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別の MCU ゾーンを定義する必要があります。

説明のために、3 つの例で MCU ゾーンの設定方法を示します。例 15-4 は、すべての MCU が同じデバイス プールに関連付けられた単一の Cisco Unified CallManager クラスタに定義される単一の MCU ゾーンを示しています。例 15-5 は、MCU が 2 つの異なるデバイス プールに分割された単一の Cisco Unified CallManager クラスタを示しています。例 15-6 は、MCU がクラスタごとに 2 つの異なるデバイス プールに分割された 2 つの Cisco Unified CallManager クラスタを示しています。

（注） 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 15-4　単一の Cisco Unified CallManager クラスタと単一のデバイス プールの MCU ゾーン

```
gatekeeper
zone local MCUs domain.com invia MCUs outvia MCUs enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy MCUs default inbound-to [MCU | gateway]
! no use-proxy MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-5　単一の Cisco Unified CallManager クラスタと 2 つのデバイス プールの MCU ゾーン

```
gatekeeper
zone local dp1-MCUs domain.com invia dp1-MCUs outvia dp1-MCUs enable-intrazone
zone local dp2-MCUs domain.com invia dp2-MCUs outvia dp2-MCUs enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy dp2-MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-6　クラスタあたり 2 つのデバイス プールのある 2 つの Cisco Unified CallManager クラスタの MCU ゾーン

```
gatekeeper
zone local clstr1-dp1-MCUs domain.com invia clstr1-dp1-MCUs outvia clstr1-dp1-MCUs
enable-intrazone
zone local clstr1-dp2-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr1-dp2-MCUs
enable-intrazone
zone local clstr2-dp1-MCUs domain.com invia clstr2-dp1-MCUs outvia clstr2-dp1-MCUs
enable-intrazone
zone local clstr2-dp2-MCUs domain.com invia clstr2-dp2-MCUs outvia clstr2-dp2-MCUs
enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy clstr1-dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr1-dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs default outbound-from [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs default inbound-to [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs default outbound-from [MCU | gateway]
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper は MCU またはゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 MCU ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] [MCU | gateway]
```

MCU を MCU として登録する場合は、**no use-proxy** コマンドの最後で **MCU** 引数を使用します。MCU をゲートウェイとして登録する場合は、**gateway** 引数を使用します。

MCU ゾーン プレフィックス

H.323 MCU ゾーンには、デフォルト テクノロジー プレフィックス以外のゾーン プレフィックスまたはテクノロジー プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

MCU が E.164 アドレスではなくテクノロジー プレフィックスとしてサービス プレフィックスを登録する場合は、すでに説明したように、# 文字を MCU のサービス プレフィックスに付加する特殊な設定を使用します（P.15-34 の「MCU サービス プレフィックス」を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントが MCU のサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プレフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

H.320 ゲートウェイ ゾーン

各エンドポイント ゲートキーパー内で設定の必要な H.320 ゲートウェイ ゾーンの数は、次の要素で決まります。

- H.320 ゲートウェイの関連付け先となるデバイス プール

  デバイス プールは、各 H.320 ゲートウェイの 1 次、2 次、および 3 次 Cisco Unified CallManager サーバを決定します。すべてのゲートウェイを同じデバイス プールに割り当てた場合、エンドポイント ゲートキーパーで定義する必要があるゲートウェイ ゾーンは 1 つだけです。つまり、H.320 ゲートウェイで使用するデバイス プールごとに、ゲートキーパーで個別のゲートウェイ ゾーンを設定する必要があります。

- エンドポイント ゲートキーパーが単一の Cisco Unified CallManager クラスタにサービスを提供するのか、複数の Cisco Unified CallManager クラスタにサービスを提供するのか

  各ゲートウェイ ゾーンは、特定の RASAggregator トランクにコールをルーティングするように設定されます。そのため、1 つのエンドポイント ゲートキーパーを使用して複数の Cisco Unified CallManager クラスタにサービスを提供する場合は、ゲートキーパーがサービスを提供するクラスタごとに、個別のゲートウェイ ゾーンを定義する必要があります。

説明のために、3 つの例でゲートウェイ ゾーンの設定方法を示します。例 15-7 は、すべての H.320 ゲートウェイが同じデバイス プールに関連付けられた単一の Cisco Unified CallManager クラスタに定義される単一のゲートウェイ ゾーンを示しています。例 15-8 は、ゲートウェイが 2 つの異なるデバイス プールに分割された単一の Cisco Unified CallManager クラスタを示しています。例 15-9 は、ゲートウェイがクラスタごとに 2 つの異なるデバイス プールに分割された 2 つの Cisco Unified CallManager クラスタを示しています。

(注)　以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 15-7　単一の Cisco Unified CallManager クラスタと単一のデバイス プールのゲートウェイ ゾーン

```
gatekeeper
zone local gateways domain.com invia gateways outvia gateways enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy gateways default inbound-to gateway
! no use-proxy gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-8　単一の Cisco Unified CallManager クラスタと 2 つのデバイス プールのゲートウェイ ゾーン

```
gatekeeper
zone local dp1-gateways domain.com invia dp1-gateways outvia dp1-gateways
enable-intrazone
zone local dp2-gateways domain.com invia dp2-gateways outvia dp2-gateways
enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy dp1-gateways default inbound-to gateway
! no use-proxy dp1-gateways default outbound-from gateway
! no use-proxy dp2-gateways default inbound-to gateway
! no use-proxy dp2-gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-9　クラスタあたり 2 つのデバイス プールのある 2 つの Cisco Unified CallManager クラスタのゲートウェイ ゾーン

```
gatekeeper
zone local clstr1-dp1-gateways domain.com invia clstr1-dp1-gateways outvia
clstr1-dp1-gateways enable-intrazone
zone local clstr1-dp2-gateways domain.com invia clstr1-dp2-gateways outvia
clstr1-dp2-gateways enable-intrazone
zone local clstr2-dp1-gateways domain.com invia clstr2-dp1-gateways outvia
clstr2-dp1-gateways enable-intrazone
zone local clstr2-dp2-gateways domain.com invia clstr2-dp2-gateways outvia
clstr2-dp2-gateways enable-intrazone
gw-type-prefix 1# default-technology
! no use-proxy clstr1-dp1-gateways default inbound-to gateway
! no use-proxy clstr1-dp1-gateways default outbound-from gateway
! no use-proxy clstr1-dp2-gateways default inbound-to gateway
! no use-proxy clstr1-dp2-gateways default outbound-from gateway
! no use-proxy clstr2-dp1-gateways default inbound-to gateway
! no use-proxy clstr2-dp1-gateways default outbound-from gateway
! no use-proxy clstr2-dp2-gateways default inbound-to gateway
! no use-proxy clstr2-dp2-gateways default outbound-from gateway
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

プロキシ使用の無効化

デフォルトでは、Cisco IOS Gatekeeper はゲートウェイとの間のコールにプロキシを使用しないように設定されています。ただし、これらのタイプのエンドポイントでプロキシの使用を有効にした場合は、次のコマンド構文を使用して、各 H.320 ゲートウェイ ゾーンで無効にする必要があります。

```
gatekeeper
no use-proxy <zone_name> default [inbound-to | outbound-from] gateway
```

ゲートウェイ ゾーン プレフィックス

H.320 ゲートウェイ ゾーンには、ゾーン プレフィックスを設定する必要がありません。代わりに、**invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** コマンドによって、発信されたすべてのコールが、コールを発信したゾーンに関連付けられた RASAggregator トランクにルーティングされます。

また、すでに説明したように、ゲートウェイのサービス プレフィックスに # 文字を付加する特殊な設定を使用する必要があります（P.15-36 の「ゲートウェイ サービス プレフィックス」を参照）。Cisco IOS Gatekeeper がテクノロジー プレフィックスへのコールの中継ゾーンを選択する方法が原因となり、エンドポイントがゲートウェイのサービス プレフィックスをダイヤルしたときに、ゲートキーパーが登録済みの一致するテクノロジー プレフィックスを見つけると、コールは失敗します。ゲートキーパーが一致するテクノロジー プレフィックスを見つけずに、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングするように、クライアントが # 文字をダイヤルしないようにする必要があります。

ゾーン サブネット

すでに説明したように、H.323 仕様では、単一のゲートキーパーで複数のゾーンを管理できます。ただし、ゲートキーパーには、デバイスから Registration Request（RRQ）を受信したときに、そのエンドポイントをどのゾーンに配置するかを判断する手段が必要です。RRQ メッセージには、エンドポイントがどのゾーンへの登録を希望するかを示す Gatekeeper Identifier フィールドが含まれています。ただし、多くの H.323 ビデオ エンドポイントはこのフィールドを設定せず、ゲートキーパーに複数のゾーンが定義されている場合、ゲートキーパーはエンドポイントを配置するゾーンを認識できません。そのため、**zone subnet** コマンドを使用して、エンドポイントと関連付けられたゾーン

をゲートキーパーに示す必要があります。このコマンドは、各ゾーンへの登録が許可される IP アドレスまたは IP の範囲を定義します。コマンド構文には、ネットワーク マスクの入力が必要です。そのため、32 ビット（/32）のネットワーク マスクを入力して特定のホスト アドレスを指定するか、それよりも小さなネットワーク マスクを指定してアドレスの範囲を指定します。

MCU、H.320 ゲートウェイ、および Cisco Unified CallManager サーバは通常、固定 IP アドレスを使用しますが、H.323 クライアントは DHCP アドレスを使用できます。そのため、**zone subnet** コマンドは MCU ゾーンおよびゲートウェイ ゾーンにのみ定義し、クライアント ゾーンは任意の IP アドレスを許可できるようにオープンのままにすることをお勧めします。例 15-10 で示すように、Cisco Unified CallManager サーバが MCU ゾーンおよびゲートウェイ ゾーンに登録することも許可する必要があることに注意してください。

（注） 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 15-10　ゾーン サブネットの定義

```
gatekeeper
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
```

例 15-10 の設定では、MCU ゾーンの MCU および RASAggregator を MCU ゾーンに登録することを明示的に許可しています。また、ゲートウェイ ゾーンのゲートウェイおよび RASAggregator をゲートウェイ ゾーンに登録することを明示的に許可しています。また、MCU およびゲートウェイをクライアント ゾーンに登録できないように明示的に拒否しています。その他のすべての IP アドレス（クライアント ゾーンの RASAggregator を含む）は、クライアント ゾーンに登録することが暗黙的に許可されています。

エンドポイントの存続可能時間

エンドポイントは、簡易な Registration Request（RRQ）をゲートキーパーに定期的に送信し、登録状態を維持します。これらの RRQ を送信する間隔は、Time to Live（TTL; 存続可能時間）値とも呼ばれます。エンドポイントは、使用する TTL を RRQ の本体で指定できます。ゲートキーパーは、エンドポイントが要求した TTL 値を受け入れて Registration Confirm（RCF）応答でエコーするか、異なる TTL 値を RCF で指定してエンドポイントの要求を上書きします。

TTL 値が RRQ で指定されていない場合は、ゲートキーパーが RCF 応答で指定する必要があります。この場合、エンドポイントはゲートキーパーが指定した TTL に従います。Cisco IOS Gatekeeper は、エンドポイントが指定したすべての TTL 値に従います。ただし、多くの H.323 ビデオ エンドポイントは、RRQ で TTL 値を指定しません。この場合、Cisco IOS Gatekeeper は、デフォルト値として 1800 秒（30 分）の TTL 値を指定します。Cisco IOS Gatekeeper は、エンドポイントからメッセージを受信せずに TTL 間隔の 3 倍の時間（3 * 30 分 = 90 分）が経過すると、そのエンドポイントの登録をフラッシュします。

TTL 値を大きくすると、静的 IP アドレスを使用しない H.323 クライアントで問題が発生することがあります。たとえば、デフォルト TTL 値の 1800 秒を使用した場合、クライアントをネットワークから切断し、別のロケーションに移動して異なる DHCP アドレスを受け取った場合、TTL 間隔の 3 倍が経過して、ゲートキーパーがそのエンドポイントの元の登録をフラッシュするまで、ゲートキーパーへの登録に失敗します（Registration Reject（RRJ）の理由値「duplicate alias」）。

したがって、ネットワークに悪影響が生じない範囲で、TTL 値はできるだけ小さくするようにしてください。Cisco IOS Gatekeeper では、60 秒から 3600 秒の任意の値に TTL 値を設定できます。ほとんどの場合、60 秒でうまく動作するはずです。ただし、すでにゲートキーパーの使用率が高い場合は、TTL をデフォルトの 1800 秒から 60 秒に調整すると、負荷が過大になることがあります。

TTL 値を設定するには、次のコマンド構文を使用します。

```
gatekeeper
endpoint ttl <seconds>
```

エンドポイント ゲートキーパーの要約

この項では、エンドポイント ゲートキーパーに関する重要なポイントを要約し、前の例で使用したテクニックを組み合せたいくつかの設定例を示します。

- エンドポイントのタイプ（クライアント、MCU、および H.320 ゲートウェイ）ごとに、エンドポイント ゲートキーパーに個別のゾーンを設定します。エンドポイントが複数のデバイス プールに関連付けられている場合は、エンドポイントのタイプごとに複数のゾーンを設定します。
- 各ゾーンに登録する RASAggregator トランクを設定します。このトランクは、Cisco Unified CallManager Administration でゲートキーパー制御 H.323 クライアントを設定したときに、自動的に作成されます。ただし、非ゲートキーパー制御 H.323 クライアント、H.323 MCU、および H.320 ゲートウェイに対しては、ゾーンの RASAggregator トランクを作成するために、ダミーのゲートキーパー制御 H.323 クライアントを設定する必要があります。
- RASAggregator トランクを IP-to-IP ゲートウェイとしてゲートキーパーに登録するには、デバイス パラメータ **Send Product ID and Version ID** を **True** に設定します。このように設定すると、ゲートキーパーは各ローカル ゾーン定義に適用される **invia**、**outvia**、**enable-intrazone**、および **gw-type-prefix** *<1#>* **default-technology** の各コマンドを使用することによって、ゾーンを宛先または発信元とするコール、またはゾーン内で発信されるコールのすべてについて、RASAggregator を選択できます。
- エンドポイント ゾーンにゾーン プレフィックスを関連付ける必要はありません。エンドポイントが何をダイヤルしても、ゲートキーパーは一致するゾーン プレフィックスまたはテクノロジー プレフィックスを見つけることなく、コールを発信したゾーンに関連付けられている RASAggregator トランクにコールをルーティングする必要があります。ゲートキーパーで、ダイヤルされた番号と MCU またはゲートウェイのテクノロジー プレフィックスが間違って一致することを防ぐために、すべての MCU およびゲートウェイ サービス プレフィックスを # 文字でマスクし、MCU またはゲートウェイに関連付けられているルート パターンに # 文字を付加します。
- Gatekeeper Identifier（ゾーン名）の指定機能をサポートしていない H.323 エンドポイントがある場合は、登録するゾーン サブネットを設定します。
- すべてのゾーンで、古い MCM プロキシの使用を無効にします。
- ゲートキーパーの負荷が過大にならない範囲で、できるだけ低い値でエンドポイント登録の存続可能時間（TTL）を設定します。ゲートキーパーが数百のエンドポイント登録を処理するような極端なケースでは、TTL を 60 秒に設定すると、管理できない量の RAS トラフィックが発生することがあります。小規模な環境では、60 秒でうまく動作するはずです。

例 15-11 は、単一の Cisco Unified CallManager クラスタにサービスを提供するエンドポイント ゲートキーパーの設定を示しています。このクラスタは、単一のデバイス プールを使用して、すべての H.323 ビデオ エンドポイント タイプにサービスを提供します。

(注) 以下の例で示すいくつかのコマンドは、Cisco IOS Gatekeeper で適用されるデフォルト値です。そのため、明示的に設定する必要はなく、実際の設定にも現れません。ここでは完全なものにするために含めていますが、コマンドラインの先頭に ! のマークを付けてあります。

例 15-11　単一のクラスタと単一のデバイス プールのエンドポイント ゲートキーパー設定

```
gatekeeper
zone local clients domain.com invia clients outvia clients enable-intrazone
zone local MCUs domain.com invia MCUs outvia MCUs enable-intrazone
zone local gateways domain.com invia gateways outvia gateways enable-intrazone
! zone subnet clients default enable
no zone subnet clients [MCUs_IP_addr]/32 enable
no zone subnet clients [gateways_IP_addr]/32 enable
no zone subnet MCUs default enable
zone subnet MCUs [MCUs_IP_addr]/32 enable
zone subnet MCUs [RASAggregators_IP_addr]/32 enable
no zone subnet gateways default enable
zone subnet gateways [gateways_IP_addr]/32 enable
zone subnet gateways [RASAggregators_IP_addr]/32 enable
no use-proxy clients inbound-to terminals
no use-proxy clients outbound-from terminals
! no use-proxy MCUs inbound-to [MCU | gateway]
! no use-proxy MCUs outbound-from [MCU | gateway]
! no use-proxy gateways inbound-to gateway
! no use-proxy gateways outbound-from gateway
gw-type-prefix 1# default-technology
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

例 15-12 は、2 つの Cisco Unified CallManager クラスタにサービスを提供するエンドポイント ゲートキーパーの設定を示しています。各クラスタには、H.323 ビデオ エンドポイント用に 2 つの異なるデバイス プールがあります。

例 15-12　2 つのクラスタと 2 つのデバイス プールのエンドポイント ゲートキーパー設定

```
gatekeeper
zone local clstr1-dp1-clients domain.com invia clstr1-dp1-clients outvia
clstr1-dp1-clients enable-intrazone
zone local clstr1-dp1-MCUs domain.com invia clstr1-dp1-MCUs outvia clstr1-dp1-MCUs
enable-intrazone
zone local clstr1-dp1-gateways domain.com invia clstr1-dp1-gateways outvia
clstr1-dp1-gateways enable-intrazone
zone local clstr1-dp2-clients domain.com invia clstr1-dp2-clients outvia
clstr1-dp2-clients enable-intrazone
zone local clstr1-dp2-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr1-dp2-MCUs
enable-intrazone
zone local clstr1-dp2-gateways domain.com invia clstr1-dp2-gateways outvia
clstr1-dp2-gateways enable-intrazone
zone local clstr2-dp1-clients domain.com invia clstr2-dp1-clients outvia
clstr2-dp1-clients enable-intrazone
zone local clstr2-dp1-MCUs domain.com invia clstr1-dp2-MCUs outvia clstr2-dp1-MCUs
enable-intrazone
zone local clstr2-dp1-gateways domain.com invia clstr2-dp1-gateways outvia
clstr2-dp1-gateways enable-intrazone
zone local clstr2-dp2-clients domain.com invia clstr2-dp2-clients outvia
clstr2-dp2-clients enable-intrazone
zone local clstr2-dp2-MCUs domain.com invia clstr2-dp2-MCUs outvia clstr2-dp2-MCUs
enable-intrazone
zone local clstr2-dp2-gateways domain.com invia clstr2-dp2-gateways outvia
clstr2-dp2-gateways enable-intrazone
! zone subnet clstr1-dp1-clients default enable
```

```
no zone subnet clstr1-dp1-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-clients [clstr2-dp2 gateways_IP_addr]/32 enable
! zone subnet clstr1-dp2-clients default enable
no zone subnet clstr1-dp2-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp2-clients [clstr2-dp2 gateways_IP_addr]/32 enable
! zone subnet clstr2-dp1-clients default enable
no zone subnet clstr2-dp1-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp1-clients [clstr2-dp2 gateways_IP_addr]/32 enable
zone subnet clstr2-dp2-clients default enable
no zone subnet clstr2-dp2-clients [clstr1-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp1 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp2 MCUs_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr1-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp1 gateways_IP_addr]/32 enable
no zone subnet clstr2-dp2-clients [clstr2-dp2 gateways_IP_addr]/32 enable
no zone subnet clstr1-dp1-MCUs default enable
zone subnet clstr1-dp1-MCUs [clstr1-dp1 MCUs_IP_addr]/32 enable
zone subnet clstr1-dp1-MCUs [clstr1-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp2-MCUs default enable
zone subnet clstr1-dp2-MCUs [clstr1-dp2 MCUs_IP_addr]/32 enable
zone subnet clstr1-dp2-MCUs [clstr1-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp1-MCUs default enable
zone subnet clstr2-dp1-MCUs [clstr2-dp1 MCUs_IP_addr]/32 enable
zone subnet clstr2-dp1-MCUs [clstr2-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp2-MCUs default enable
zone subnet clstr2-dp2-MCUs [clstr2-dp2 MCUs_IP_addr]/32 enable
zone subnet clstr2-dp2-MCUs [clstr2-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp1-gateways default enable
zone subnet clstr1-dp1-gateways [clstr1-dp1 gateways_IP_addr]/32 enable
zone subnet clstr1-dp1-gateways [clstr1-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr1-dp2-gateways default enable
zone subnet clstr1-dp2-gateways [clstr1-dp2 gateways_IP_addr]/32 enable
zone subnet clstr1-dp2-gateways [clstr1-dp2 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp1-gateways default enable
zone subnet clstr2-dp1-gateways [clstr2-dp1 gateways_IP_addr]/32 enable
zone subnet clstr2-dp1-gateways [clstr2-dp1 RASAggregators_IP_addr]/32 enable
no zone subnet clstr2-dp2-gateways default enable
zone subnet clstr2-dp2-gateways [clstr2-dp2 gateways_IP_addr]/32 enable
zone subnet clstr2-dp2-gateways [clstr2-dp2 RASAggregators_IP_addr]/32 enable
no use-proxy clstr1-dp1-clients inbound-to terminals
no use-proxy clstr1-dp1-clients outbound-from terminals
no use-proxy clstr1-dp2-clients inbound-to terminals
no use-proxy clstr1-dp2-clients outbound-from terminals
no use-proxy clstr2-dp1-clients inbound-to terminals
no use-proxy clstr2-dp1-clients outbound-from terminals
no use-proxy clstr2-dp2-clients inbound-to terminals
no use-proxy clstr2-dp2-clients outbound-from terminals
! no use-proxy clstr1-dp1-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr1-dp1-MCUs outbound-from [MCU | gateway]
```

```
! no use-proxy clstr1-dp2-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr1-dp2-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr2-dp1-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs inbound-to [MCU | gateway]
! no use-proxy clstr2-dp2-MCUs outbound-from [MCU | gateway]
! no use-proxy clstr1-dp1-gateways inbound-to gateway
! no use-proxy clstr1-dp1-gateways outbound-from gateway
! no use-proxy clstr1-dp2-gateways inbound-to gateway
! no use-proxy clstr1-dp2-gateways outbound-from gateway
! no use-proxy clstr2-dp1-gateways inbound-to gateway
! no use-proxy clstr2-dp1-gateways outbound-from gateway
! no use-proxy clstr2-dp2-gateways inbound-to gateway
! no use-proxy clstr2-dp2-gateways outbound-from gateway
gw-type-prefix 1# default-technology
! no arq reject-unknown-prefix
endpoint ttl 60
no shutdown
```

Cisco Unified CallManager 4.0 からの移行

『*Cisco IP Video Telephony SRND for Cisco Unified CallManager 4.0*』に記載されている設計方法から、この章で示した設計方法への移行プロセスは、次の基本手順で構成されます。

1. 新しいゲートキーパー制御 H.323 クライアント機能を利用するように、H.323 クライアントを Cisco Unified CallManager Administration で再設定する。
2. H.323 クライアント、MCU、および H.320 ゲートウェイ ゾーンに使用していた H.225 ゲートキーパー制御トランクを削除し、ダミーのゲートキーパー制御 H.323 クライアントを作成して RASAggregator トランクと置き換える。
3. 新しい中継ゾーン定義構成を使用するようにエンドポイント ゲートキーパーを再設定し、H.323 クライアント、MCU、およびゲートウェイ ゾーンに適用されていたすべてのゾーン プレフィックスを削除する。
4. 必要に応じて、プレフィックスの先頭に # 文字を含めるように、すべての MCU および H.320 ゲートウェイ サービス プレフィックスを修正する。

これらの各手順を実行すると、既存の H.323 ビデオ エンドポイントのサービスが中断されることがあります。そのため、これらの設定変更は慎重に計画し、管理者が既存の H.323 ビデオ エンドポイントの中断を最小限に抑えられるときに実行する必要があります。

アプリケーション

Cisco Unified Communications には、Cisco Unified CallManager の機能を拡張し、高度な機能と他の通信メディアとの統合を提供する幅広いアプリケーションのポートフォリオが用意されています。これらの多くのアプリケーションは、特にビデオをサポートしていなくても、IP ビデオ テレフォニー デバイスと組み合せて使用できます。たとえば、Cisco Unified CallManager Release 4.1 は、TAPI/JTAPI プロトコルを使用する CTI アプリケーションのビデオ チャネルのネゴシエーションをサポートしていませんが、CTI アプリケーションをビデオ コールと組み合せて使用する妨げにはなりません。この項では、シスコおよびサードパーティ製のアプリケーションのいくつかについて検討し、ビデオ コールに対して高度なコール処理を提供できるかどうかについて説明します。

CTI アプリケーション

次のアプリケーションは、コンピュータ / テレフォニー インテグレーション（CTI）インターフェイスに基づいています。

Cisco Emergency Responder

Cisco Emergency Responder（ER）は、緊急コール（911）を適切な Public Safety Answering Point（PSAP）にルーティングします。また、PSAP が事故のあった物理的な正しい場所に応答し、コールが切断された場合はコールバックできるように、発信元デバイスの正しい発信元回線 ID を PSAP に提供します。Cisco ER は、JTAPI を使用して Cisco Unified CallManager に統合されています。緊急コールは CTI ルート ポイント経由で Cisco ER にルーティングされ、Cisco ER は、コールの転送先 PSAP および表示する発信元回線 ID を判断します。Cisco ER は、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）と Cisco Discovery Protocol（CDP; シスコ検出プロトコル）を使用して、エンドポイントが接続されている物理ポートと特定の Cisco Catalyst Ethernet スイッチを検出することによって、ネットワークの各エンドポイントを追跡し、物理的な場所を判断します。CDP を使用できない場合は、代わりに IP サブネットを使用してエンドポイントを探すように Cisco ER を設定できます。Cisco ER は、この情報をスイッチの物理的な場所に関連付け、データベースに情報を格納します。

Cisco Unified Video Advantage と Cisco IP Video Phone 7985 はどちらも、Cisco ER 検出の目的で CDP をサポートしています。Cisco Unified Video Advantage は、スイッチに CDP メッセージを直接送信しませんが、このサポート用として、関連付けられた Cisco Unified IP Phone を利用します。その結果、Video Telephony ユーザが 911 をダイヤルすると、Cisco ER は正しい PSAP にコールをルーティングできます。

Sony 社製および Tandberg 社製の SCCP エンドポイントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。

H.323 ビデオ会議クライアントは CDP をサポートしないため、Cisco ER は、IP サブネットでこれらのエンドポイントを追跡する必要があります。これにより、Cisco ER はコールを正しい PSAP にルーティングできます。ただし、H.323 デバイスのコールを Cisco ER でルーティングするには、H.323 デバイスが Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、Cisco ER が処理する 911 へのコールは失敗します。

Cisco Unified CallManager Assistant

Cisco Unified CallManager Assistant を使用すると、アシスタントが、関連するマネージャに対応できます。Unified CM Assistant は、JTAPI を使用して Cisco Unified CallManager に統合されています。Unified CM Assistant は特にビデオ対応というわけではありませんが、ビデオ対応の電話機でも Unified CM Assistant は問題なく使用できます。Unified CM Assistant がコールを処理し、コールが最終的な宛先デバイスに転送されると、コールの 2 つのデバイスが互いに直接通信し、この時点でビデオ チャネルを確立できます。たとえば、ビデオ対応エンドポイントがマネージャのディレクトリ番号をダイヤルし、アシスタントが Unified CM Assistant アプリケーションを使用してコールをカバーした場合、コールの最初の処理ではビデオは確立されていないことがあります。しかし、アシスタントが発信者をマネージャに転送すると、Cisco Unified CallManager がビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Unified CM Assistant と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、Unified CM Assistant が代行受信したコールは、アシスタントがマネージャにコールを転送しようとしたときに失敗します。

Cisco IP 音声自動応答装置と Cisco IP Contact Center

Cisco IP 音声自動応答装置（IP IVR）および Cisco IP Contact Center（IPCC）は、JTAPI を使用して Cisco Unified CallManager に統合されています。ビデオ対応デバイスが IVR アプリケーション（ヘルプ デスクなど）にコールを発信した場合、発信者がアプリケーション サーバに接続している間（発信者が IVR メニューをブラウズしている間、またはヘルプデスクのメンバーがコールを受け付けるまでキューで待機している間）、通信は音声のみになります。ただし、IVR アプリケーションがコールを最終的な宛先に転送すると、その時点でビデオ チャネルをネゴシエートできるようになります。H.323 デバイスを Cisco Unified IP-IVR および IPCC と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、Cisco Unified IP-IVR または IPCC が代行受信したコールは、アプリケーションが最終的な宛先に発信者を転送しようとしたときに失敗します。

IVR アプリケーションは、多くの場合、DTMF トーンを使用して IVR メニューのオプションを選択します。別の方法としては音声認識があり、電話機のキーを押す代わりに、発信者が IVR サーバに向かってコマンドを発音します。Cisco Unified IP-IVR と IPCC はどちらも、JTAPI を使用して Cisco Unified CallManager に統合されているため、アウトオブバンド シグナリング メッセージで DTMF トーンを渡します。現在、市販されている多くの H.323 デバイスは、インバンド DTMF トーンを使用しています。このような H.323 クライアントでは、DTMF を使用して IP IVR または IPCC メニューをナビゲートすることはできません。ただし、これらの H.323 クライアントは、IVR サーバが対応していれば、音声認識を使用できます。Cisco Unified Video Advantage などのビデオ対応デバイス、Sony 社製または Tandberg 社製の SCCP デバイス、および DTMF に H.245 英数字アウトオブバンド シグナリングを使用する H.323 エンドポイントは、DTMF トーンを使用して IVR メニューをナビゲートできます。

Cisco Attendant Console

Cisco Attendant Console は、JTAPI を使用して Cisco Unified CallManager に統合されています。Attendant Console は、着信コールを処理する管理用デバイスとして使用されます。Attendant Console は、特にビデオをサポートしているわけではありませんが、コールが最終的な宛先に転送されると、ビデオ チャネルをネゴシエートできるようになります。ただし、H.323 デバイスを Attendant Console と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、Attendant Console が代行受信したコールは、コンソール担当者が最終的な宛先に発信者を転送しようとしたときに失敗します。

Cisco Personal Assistant

Cisco Personal Assistant（PA）には、主に次の 2 つの機能があります。

- DTMF トーンまたは音声コマンドによるダイヤル サポート
- 時刻、発信者 ID 情報などの要素に基づいてユーザがプログラムするコール ルーティングのプリファレンス

どちらの機能でも、コールが PA サーバに接続されている間は、ビデオは確立されていません。しかし、PA がコールを最終的な宛先に転送すると、ビデオ チャネルをネゴシエートできるようになります。H.323 デバイスを PA と相互運用するには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。H.323 エンドポイントが Cisco Unified CallManager からの ECS の受信をサポートしていない場合、PA が代行受信したコールは、アプリケーションが最終的な宛先に発信者を転送しようとしたときに失敗します。

Cisco IP SoftPhone および Cisco IP Communicator

Cisco IP SoftPhone は、TAPI を使用して Cisco Unified CallManager と統合されており、スタンドアロン ソフトフォンまたは関連付けられている SCCP ハードウェア電話機を制御するソフトウェア インターフェイスとして設定できます。Cisco IP SoftPhone は、特にビデオをサポートしているわけではありませんが、Cisco Unified Video Advantage クライアントが関連付けられている IP Phone と組み合せて使用できます。Cisco IP SoftPhone は、Sony 社製または Tandberg 社製の SCCP デバイスの制御には使用できません。

Cisco IP Communicator は、SCCP クライアントなので Cisco 7970 シリーズ IP Phone のように動作するという点で、IP SoftPhone と異なります。

コラボレーション ソリューション

エンドポイント間のビデオ通信を提供するために、次のテクノロジーが使用されることがあります。

T.120 アプリケーション共有

T.120 プロトコルを使用して、ドキュメント、ホワイトボード、およびテキストを会議の参加者で共有するビデオ会議エンドポイントがあります。Cisco Unified CallManager は、T.120 チャネルのネゴシエートをサポートしません。T.120 の代わりに、Cisco MeetingPlace やサードパーティのコラボレーション ソリューション（Placeware、Web-Ex、IBM E-Collaborate など）のような Web ベースのコラボレーション ソリューションを使用することをお勧めします。

Cisco Unified MeetingPlace

Cisco Unified MeetingPlace は、ハイエンドな音声およびビデオ会議ソリューションと、会議のスケジューリングおよび参加に使用する Web ベースのフロントエンドを結合します。詳細については、P.14-1 の「Cisco Unified MeetingPlace の統合」の章を参照してください。

無線ネットワーキング ソリューション

ビデオは帯域幅に大きな影響を与えるため、802.11b などの共有無線メディアをビデオ エンドポイントに使用することはお勧めしません。

Cisco Aironet 802.11b ネットワーキング ソリューション

Tandberg 社製 T-1000 モデル エンドポイントには、Cisco Aironet PCMCIA 802.11b Wireless Adapter を取り付け可能な PCMCIA インターフェイスが用意されています。ただし、ビデオ エンドポイントが、実稼働中の IP Phone と無線帯域幅を共有しないように注意する必要があります。ビデオは帯域幅の大半を消費するため、ビデオ、音声、およびデータを同じ無線メディアでサポートすることは困難です。

Cisco Unified Video Advantage は、関連付けられた IP Phone への物理イーサネット接続に依存します。通常、ユーザが物理イーサネット インターフェイスと、同じ PC にインストールされた Aironet 802.11b Wireless Adapter の両方を使用することはありません。このような設定は、無線インターフェイスがネットワークへの優先パスになった場合に、Cisco Unified Video Advantage がこのインターフェイス経由では関連付けられないため、Cisco Unified Video Advantage で問題が発生する原因になります。常に、物理イーサネット インターフェイスを優先パスにすることをお勧めします。また、ユーザが IP Phone の背面の PC ポートに接続するときは、間違って優先されないように Aironet Adapter を無効にするように指示してください。

Cisco Unified Wireless IP Phone 7920

Cisco Unified Wireless IP Phone 7920 は、ビデオをサポートしません。ビデオ エンドポイントからも Cisco Unified Wireless IP Phone 7920 にコールを発信できますが、音声のみのコールとしてネゴシエートされます。無線 IP Phone ユーザは、コールの保留、転送、または会議への参加ができます。発信者が H.323 ビデオ エンドポイントの場合、これらの補足サービスを機能させるには、Empty Capabilities Set（ECS）プロシージャをサポートしている必要があります。

XML サービス

現在、特に Cisco Unified Video Advantage クライアント ソリューション、Cisco IP Video Phone 7985、または Sony 社製や Tandberg 社製の SCCP エンドポイント用に作成された XML アプリケーションはありません。ただし、これらのエンドポイントのうち、Cisco IP Video Phone 7985 および Sony 社製エンドポイント以外は、XML アプリケーションをサポートします。Cisco VT Advantage は Cisco Unified IP Phone を使用するため、これらの電話機モデルでサポートされる XML アプリケーションは VT Advantage でも動作します。

Tandberg 社製 SCCP エンドポイントは XML をサポートしますが、現在、すべての XML アプリケーションが Tandberg 社製エンドポイントで動作するわけではありません。たとえば、Cisco エクステンション モビリティおよび Berbee InformaCast 製品は、現在、Sony 社製または Tandberg 社製の SCCP エンドポイントで動作しない代表的な 2 つの XML アプリケーションです。これらのアプリケーションをサポートするには、エンドポイントのファームウェア アップグレードと、場合によっては Cisco Unified CallManager Administration の変更が必要になります。

CHAPTER 16

LDAP ディレクトリ統合

ディレクトリ（電話帳）は、多数の読み取りや検索、および随時の書き込みや更新用に最適化される特殊なデータベースです。ディレクトリには、一般に、社員の情報、企業ネットワークでのユーザ特権など、頻繁に変更されないデータが保存されます。

ディレクトリのもう 1 つの面は、拡張可能であることです。つまり、ディレクトリに保存される情報のタイプを変更し、拡大することが可能です。ディレクトリ スキーマという語は、保存されている情報のタイプ、および情報の規則を指します。

Lightweight Directory Access Protocol（LDAP）は、ディレクトリに保存されている情報にアクセスし、変更するための標準方式をアプリケーションに提供します。この機能により、企業は、すべてのユーザ情報を、複数のアプリケーションで利用できる単一リポジトリに集中化させることができます。追加、移動、および変更が簡単なので、保守コストも大幅に削減されます。

この章では、Cisco Unified CallManager 5.0 に基づく Cisco Unified Communications システムを社内 LDAP ディレクトリと統合する場合の、設計上の主な原則について説明しています。この章の構成は、次のとおりです。

- ディレクトリ統合とは（P.16-2）

  ここでは、一般的な企業の IT 部門における社内 LDAP ディレクトリとの統合に関して、さまざまな要件を分析します。

- IP テレフォニー エンドポイントのディレクトリ アクセス（P.16-4）

  ここでは、Cisco Unified Communications エンドポイントのディレクトリ アクセスを有効にする技術的なソリューションについて説明し、そのソリューションに基づく設計上のベスト プラクティスを示します。

- Cisco Unified CallManager 5.0 でのディレクトリ統合（P.16-6）

  ここでは、Cisco Unified CallManager 5.0 でのディレクトリ統合に関して、技術的なソリューションについて説明し、設計上のベスト プラクティスを示します。LDAP 同期機能や LDAP 認証機能などを扱います。

この章で説明する考慮事項は、Cisco Unified CallManager 5.0 とそれにバンドルされているアプリケーション（エクステンション モビリティ、Cisco Unified CallManager Assistant、WebDialer、Bulk Administration Tool、および Real-Time Monitoring Tool）に適用されます。

これより前の Cisco Unified CallManager リリースについては、『*Cisco Unified Communications SRND for Cisco Unified CallManager 4.0 and 4.1*』を参照してください。その他すべてのシスコ音声アプリケーションについては、次の Web サイトで入手可能なそれぞれの製品マニュアルを参照してください。

http://www.cisco.com

特に、Cisco IP Contact Center については、次の Web サイトで入手可能な『*Cisco Cisco Unified Contact Center Enterprise Edition SRND*』および『*Cisco Cisco Unified Contact Center Express SRND*』を参照してください。

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

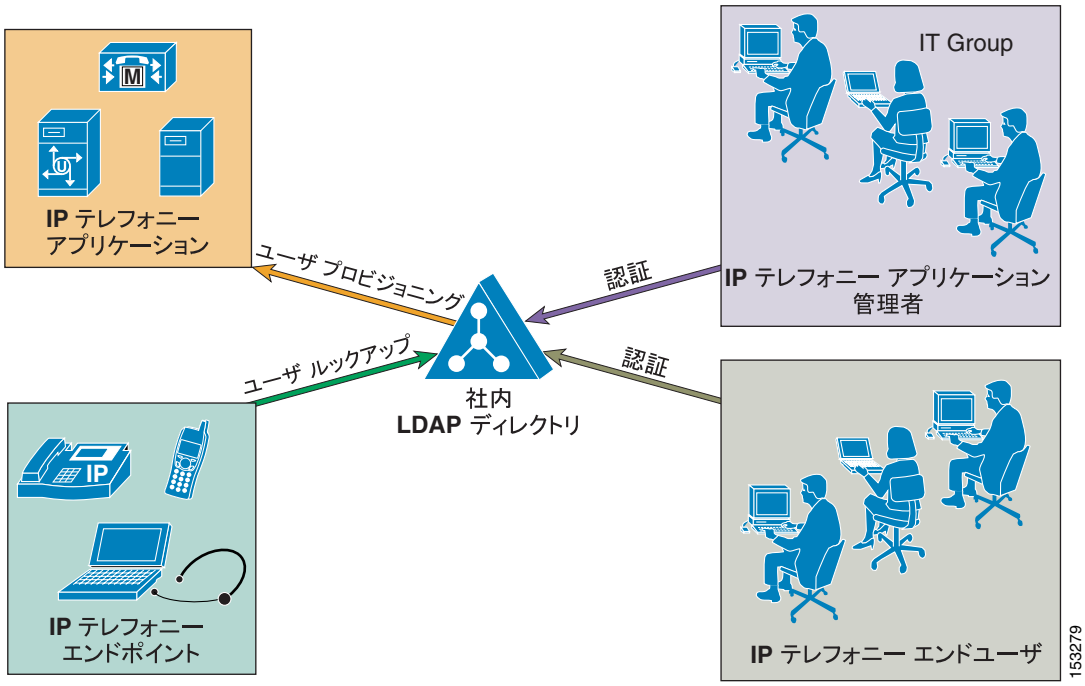
Cisco Unity については、次の Web サイトで入手可能な『*Cisco Unity Design Guide*』、および『*Cisco Unity Data and the Directory*』、『*Active Directory Capacity Planning*』、『*Cisco Unity Data Architecture and How Cisco Unity Works*』の各 White Paper を参照してください。

http://www.cisco.com

ディレクトリ統合とは

音声アプリケーションと社内 LDAP ディレクトリ間の統合は、多くの企業の IT 部門にとって一般的な作業です。ただし、統合の正確な範囲は企業によって異なるため、図 16-1 に示すように、1 つ以上の具体的かつ独立した要件として表すことができます。

図 16-1　ディレクトリ統合のさまざまな要件



たとえば、1 つの一般的な要件は、IP Phone またはその他の音声エンドポイントやビデオ エンドポイントからユーザ ルックアップ（「個人別電話帳」サービスと呼ばれることもあります）を有効にし、ユーザがディレクトリで番号を検索した後に、連絡先に直接ダイヤルできるようにすることです。

もう 1 つの要件は、社内ディレクトリから音声アプリケーションやビデオ アプリケーションのユーザ データベースを、ユーザに自動的に提供することです。この方法により、社内ディレクトリの変更のたびにコア ユーザ情報を手動で追加、削除、または修正する必要がなくなります。

多くの場合、社内ディレクトリ クレデンシャルを使用して、音声アプリケーションやビデオ アプリケーションのエンドユーザと管理者を認証することも必要です。この方法を使用すると、IT 部門がシングル ログオン機能を提供でき、さまざまな社内アプリケーション間で各ユーザが維持する必要があるパスワードの数が減ります。

表 16-1 にまとめているように、使用する Cisco Unified CallManager のバージョンに応じて異なるメカニズムを使用して、これらの要件のそれぞれを Cisco Unified Communications システムで満たすことができます。

表 16-1　ディレクトリの要件とシスコのソリューション

要件	シスコのソリューション	Cisco Unified CallManager 4.*x* の機能	Cisco Unified CallManager 5.0 の機能
エンドポイントのユーザ ルックアップ	ディレクトリ アクセス	Cisco Unified IP Phone Services SDK	Cisco Unified IP Phone Services SDK
ユーザ プロビジョニング	ディレクトリ統合	Cisco Customer Directory Configuration Plugin	LDAP 同期
IP テレフォニー エンド ユーザの認証	ディレクトリ統合	Cisco Customer Directory Configuration Plugin	LDAP 認証
IP テレフォニー アプリケーション管理者の認証	ディレクトリ統合	Cisco Customer Directory Configuration Plugin + Cisco Multilevel Administration	LDAP 認証

表 16-1 に示すように、Cisco Unified Communications システムに関係する場合、「ディレクトリ アクセス」という用語は、IP テレフォニー エンドポイントのユーザ ルックアップの要件を満たすメカニズムおよびソリューションを意味します。また、「ディレクトリ統合」という用語は、ユーザ プロビジョニングおよび（エンド ユーザと管理者の両方の）認証の要件を満たすメカニズムおよびソリューションを意味します。

この章では、これ以降、Cisco Unified CallManager Release 5.0 に基づく Cisco Unified Communications システムで、これらの要件にどのように対処するかについて説明します。これより前の Cisco Unified CallManager リリースでのディレクトリ統合ソリューションの詳細については、次の Web サイトで入手可能な『*Cisco Unified Communications SRND for Cisco Unified CallManager 4.0 and 4.1*』を参照してください。

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

（注） 「ディレクトリ統合」という用語については、管理ポリシーおよびセキュリティ ポリシーを集中化するために、Microsoft Active Directory ドメインにアプリケーション サーバを追加する機能といった解釈もあります。Cisco Unified CallManager 5.0 は、カスタマイズした組み込みオペレーティング システムで実行するアプライアンスであり、現在のところ、Microsoft Active Directory ドメインに追加できません。Cisco Unified CallManager のサーバ管理は、Cisco Real-Time Monitoring Tool（RTMT）によって行われます。アプリケーションに合せた強力なセキュリティ ポリシーが組み込みオペレーティング システム内にすでに実装されており、カスタマイズしたバージョンの Cisco Security Agent をどのサーバにもインストールできます。CiscoWorks Management Center for Cisco Security Agents により、セキュリティ ポリシーを集中管理することもできます。

IP テレフォニー エンドポイントのディレクトリ アクセス

この項では、Cisco Unified Communications エンドポイント（Cisco Unified IP Phone など）からユーザ ルックアップを実行するように、LDAP 準拠のディレクトリ サーバへの社内ディレクトリ アクセスを設定する方法について説明します。Cisco Unified CallManager やその他の IP テレフォニー アプリケーションがユーザ プロビジョニングおよび認証のために社内ディレクトリに統合されているかどうかに関係なく、この項で説明しているガイドラインが適用されます。

ディスプレイ画面を持つ Cisco Unified IP Phone では、ユーザが電話機の Directories ボタンを押すと、ユーザ ディレクトリを検索できます。IP Phone は、Hyper-Text Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）を使用して、要求を Web サーバに送信します。Web サーバからの応答には、電話機が解釈して表示できる特定の Extensible Markup Language（XML）オブジェクトが含まれている必要があります。

デフォルトでは、Cisco Unified IP Phone は、Cisco Unified CallManager の組み込みデータベースに対してユーザ ルックアップを実行するように設定されます。ただし、社内 LDAP ディレクトリでルックアップを実行するように、この設定を変更できます。変更した場合、電話機は HTTP 要求を外部 Web サーバに送信します。このサーバはプロキシとして動作し、要求を社内ディレクトリに対する LDAP 照会に変換します。次に、LDAP 応答は適切な XML オブジェクトにカプセル化され、HTTP 経由で電話機に返送されます。

図 16-2 では、Cisco Unified CallManager が社内ディレクトリに統合されていない配置において、このメカニズムを示しています。このシナリオでは、Cisco Unified CallManager はユーザ ルックアップに関連するメッセージ交換にかかわっていないことに注意してください。

図 16-2　Cisco Unified IP Phone Services SDK を使用する Cisco Unified IP Phone のディレクトリ アクセス

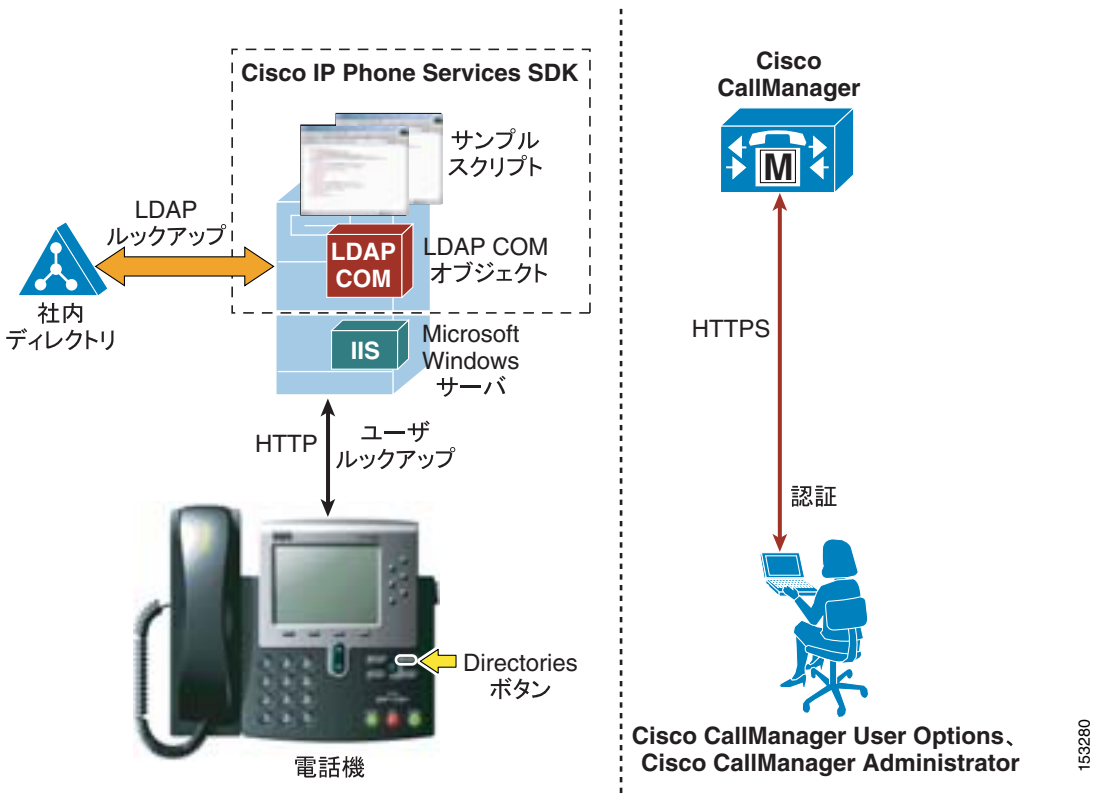


図 16-2 に示す例では、Web サーバのプロキシ機能は、Cisco Unified IP Phone Services Software Development Kit（SDK; ソフトウェア開発キット）バージョン 3.3(4) 以降に組み込まれている Cisco LDAP Search Component Object Model（COM; コンポーネント オブジェクト モデル）サーバによって提供されます。次の Web サイトの Cisco Developer Support Central から最新の Cisco Unified IP Phone Services SDK をダウンロードできます。

http://www.cisco.com/pcgi-bin/dev_support/access_level/product_support

IP Phone Services SDK は、IIS 4.0 以降を実行する Microsoft Windows Web サーバにはインストールできますが、Cisco Unified CallManager サーバにはインストールできません。SDK には、単純なディレクトリ ルックアップ機能を提供するサンプル スクリプトが入っています。

IP Phone Services SDK を使用する社内ディレクトリ ルックアップ サービスを設定するには、次の手順を実行します。

ステップ 1　社内 LDAP ディレクトリを指すようにサンプル スクリプトのどれかを修正するか、SDK に付属の『*LDAP Search COM Programming Guide*』を使用して独自のスクリプトを作成します。

ステップ 2　Cisco Unified CallManager で、外部 Web サーバ上のスクリプトの URL を指すように URL Directories パラメータ（**System** > **Enterprise Parameters**）を設定します。

ステップ 3　変更を有効にするために電話機をリセットします。

（注）　ユーザのサブセットだけにサービスを提供する場合は、Enterprise Parameters ページではなく、Phone Configuration ページ内で URL Directories パラメータを直接設定します。

まとめると、Cisco Unified IP Phone Services SDK によるディレクトリ アクセスには、次の設計上の考慮事項が適用されます。

- ユーザ ルックアップは、LDAP 準拠の社内ディレクトリに対してサポートされる。
- Microsoft Active Directory に照会する場合、スクリプトがグローバル カタログ サーバを指すようにし、スクリプト設定でポート 3268 を指定することにより、グローバル カタログに対してルックアップを実行できる。この方法では、通常はルックアップが高速化します。
- この機能に関して Cisco Unified CallManager に影響はなく、LDAP ディレクトリ サーバに最小限の影響しか及ばない。
- SDK に付属のサンプル スクリプトでは、最小限のカスタマイズのみが可能である（たとえば、返送されたすべての番号の前に番号ストリングを付けられる）。もっと高度な操作のためには、カスタム スクリプトを開発する必要があり、スクリプトの作成に役立つプログラミング ガイドが SDK に付属しています。
- この機能は、社内ディレクトリに対する Cisco Unified CallManager ユーザのプロビジョニングまたは認証を必要としない。

Cisco Unified CallManager 5.0 でのディレクトリ統合

この項では、社内 LDAP ディレクトリに対するユーザ プロビジョニングと認証を考慮した、Cisco Unified CallManager 5.0 でのディレクトリ統合のメカニズムおよびベスト プラクティスについて説明します。この項では、次のトピックを扱います。

- Cisco Unified CallManager 4.x の方法との比較（P.16-6）

  ディレクトリ統合の方法は、Cisco Unified CallManager Release 4.*x* から 5.0 で大幅に変更されており、この項では、古い方法と比較しながら新しい方法を紹介します。
- Cisco Unified CallManager 5.0 のディレクトリ アーキテクチャ（P.16-8）

  ここでは、Cisco Unified CallManager 5.0 のユーザ関連アーキテクチャの概要を示します。
- LDAP 同期（P.16-11）

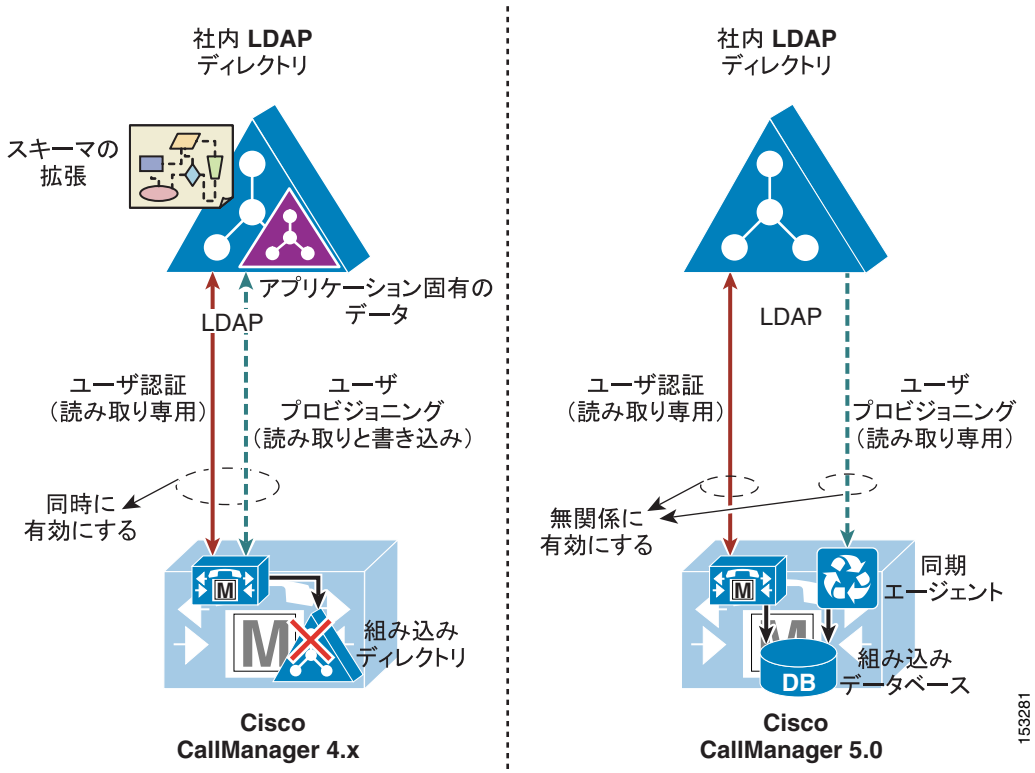
  ここでは、LDAP 同期の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。
- LDAP 認証（P.16-19）

  ここでは、LDAP 認証の機能について説明し、この機能の配置に関する設計上のガイドラインを Microsoft Active Directory に関する追加の考慮事項と共に示します。

Cisco Unified CallManager 4.x の方法との比較

図 16-3 は、*Cisco Unified CallManager 4.x* および 5.0 において、ユーザ プロビジョニングおよび認証のためのディレクトリ統合方法の高レベル機能図を示しています。

図 16-3　Cisco Unified CallManager 4.x および 5.0 におけるディレクトリ統合方法



Cisco Unified CallManager Release 4.*x* では、ユーザ関連情報の保存に組み込み LDAP ディレクトリを使用していました。社内ディレクトリ スキーマを拡張し、組み込みディレクトリをシャットダウンし、ユーザに関連するアプリケーション固有のデータの保存に社内ディレクトリを使用することで、ティレクトリ統合を有効にしていました。社内ディレクトリが実質的にユーザ情報のバックエンド保存リポジトリとして使用されていたため、この方法は、ユーザ プロビジョニングとユーザ認証の両方の要件を満たしています。社内ディレクトリのユーザ データに変更が加えられた場合、Cisco Unified CallManager は同じデータ ストアにアクセスするので、すぐにその変更が認識されていました。

ただし、この方法では、スキーマの拡張と追加データに関して社内ディレクトリに影響があり、Unified Communications システムのリアルタイム機能とディレクトリの可用性の間にも依存関係が発生します。接続が失われるかディレクトリが使用不可になると、Cisco Unified CallManager はすべてのユーザ関連設定にアクセスできなくなり、エクステンション モビリティ、Attendant Console、IP Contact Center Express などのアプリケーションに影響があります。この方法では、ユーザ プロビジョニング機能とユーザ認証機能が同じ統合プロセスに基づいているため、同時に有効にする必要がありました。さらに、社内ディレクトリをアプリケーション固有のデータの保存リポジトリとして使用することで、社内ディレクトリ自体の日常の保守操作が制限を受けることにもなっていました。

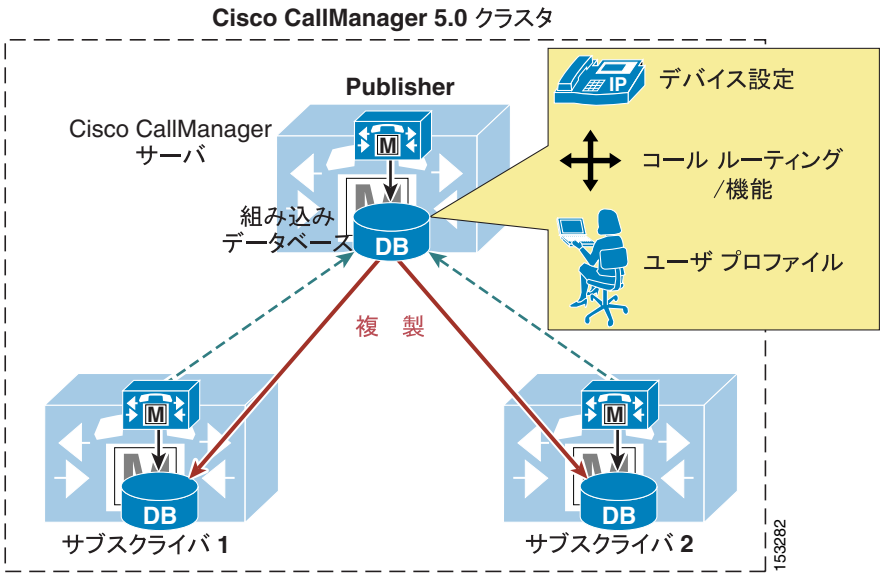
これとは逆に、Cisco Unified CallManager Release 5.0 で採用されたディレクトリ統合方法は、2 つの独立したコンポーネントに基づいてユーザ プロビジョニングとユーザ認証の要件を別々に満たします。ユーザ プロビジョニングは、社内ディレクトリから Cisco Unified CallManager の組み込みデータベースへのユーザ データの一方向同期により実行します。同期では標準 LDAPv3 を使用します。変更を Cisco Unified Communications システムに確実に反映するために、同期を手動で起動することも、定期的に実行するようにスケジューリングすることもできます。このソリューションでは、社内ディレクトリへの書き込みの必要がなくなり、スキーマの拡張も必要ありません。

ユーザ認証は、ユーザ プロビジョニングとは無関係に有効になり、社内ディレクトリ クレデンシャルに対してエンドユーザ パスワードの認証を実現します。この方法では、社内ディレクトリが使用不能または到達不能の場合でも、Cisco Unified Communications システムはすべてのリアルタイム機能を維持します。

Cisco Unified CallManager 5.0 のディレクトリ アーキテクチャ

図 16-4 は、Cisco Unified CallManager 5.0 クラスタの基本アーキテクチャを示しています。組み込みデータベースには、デバイス関連データ、コール ルーティング、その他の機能やユーザ プロファイルなど、すべての設定情報が保存されます。データベースは Cisco Unified CallManager クラスタ内のすべてのサーバ上に存在し、パブリッシャ サーバからすべてのサブスクライバ サーバに自動的に複製されます。

図 16-4　Cisco Unified CallManager 5.0 のアーキテクチャ



デフォルトでは、Cisco Unified CallManager Administration インターフェイスを介してすべてのユーザを手動でデータベースにプロビジョニングします。Cisco Unified CallManager 5.0 では、データベースのユーザを次の 2 つのカテゴリに分類することで、重要な新しい概念を導入しています。

- エンド ユーザ：現実の人および対話形式のログインに関連付けられているすべてのユーザ。このカテゴリには、すべての IP テレフォニー ユーザのほか、User Groups and Roles 設定（以前のバージョンの Cisco Unified CallManager にある Cisco Multilevel Administration 機能に相当）を使用する場合の Cisco Unified CallManager 管理者も含まれます。
- アプリケーション ユーザ：Cisco Unified Communications の他の機能またはアプリケーション（Cisco Attendant Console、Cisco IP Contact Center Express、Cisco Unified CallManager Assistant など）に関連付けられているすべてのユーザ。これらのアプリケーションは Cisco Unified CallManager に対して認証する必要がありますが、この内部「ユーザ」は対話形式のログインを行わず、単にアプリケーション間の内部通信のみを処理します。

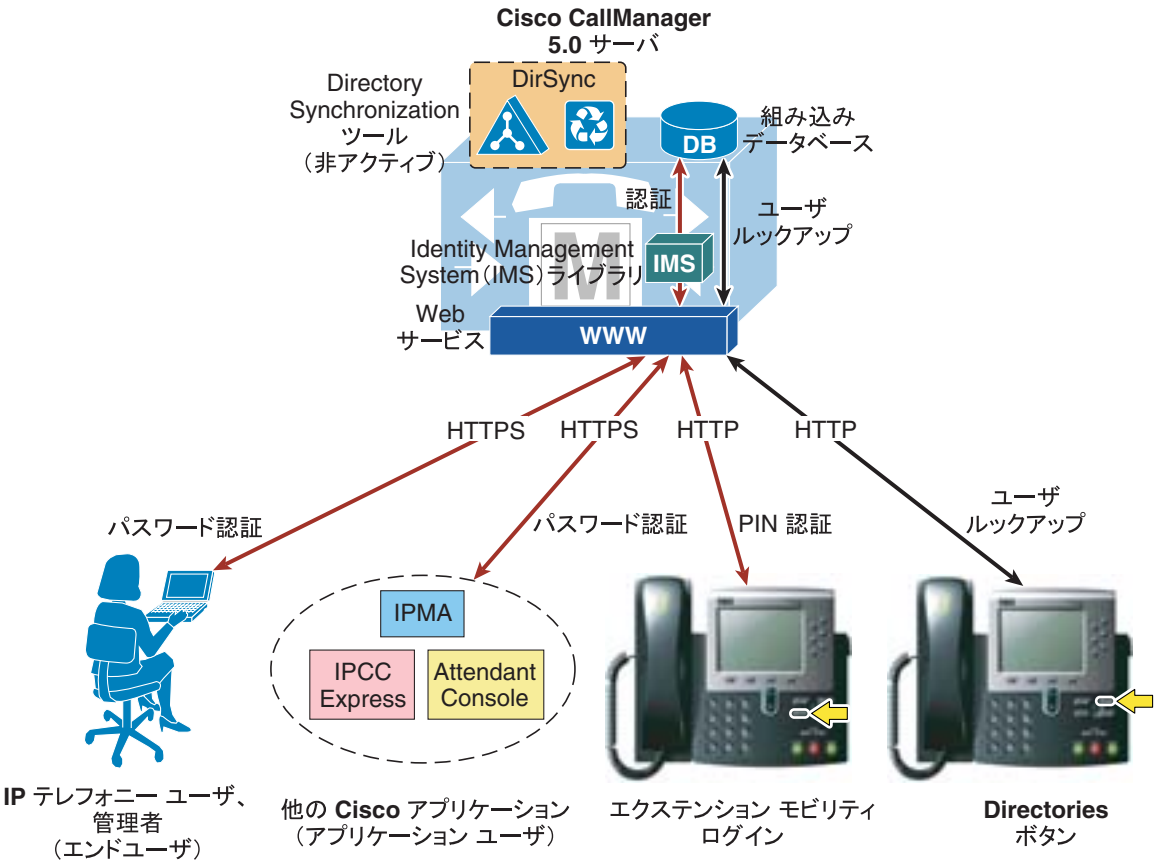
表 16-2 では、Cisco Unified CallManager データベースにデフォルトで作成されるアプリケーション ユーザのリストを、それらのユーザが使用される機能またはアプリケーションと共に示しています。Cisco Unified Communications の他のアプリケーションを統合する場合に、追加のアプリケーション ユーザを手動で作成できます（たとえば、Cisco Attendant Console の **ac** アプリケーション ユーザ、Cisco IP Contact Center Express の **jtapi** アプリケーション ユーザなど）。

表 16-2　Cisco Unified CallManager 5.0 のデフォルトのアプリケーション ユーザ

アプリケーション ユーザ	使用される機能またはアプリケーション
CCMAdministrator	Cisco Unified CallManager Administration（デフォルトは「スーパー ユーザ」）
CCMQRTSecureSysUser	Cisco Quality Reporting Tool
CCMQRTSysUser	
CCMSysUser	Cisco エクステンション モビリティ
IPMASecureSysUser	Cisco Unified CallManager Assistant
IPMASysUser	
WDSecureSysUser	Cisco WebDialer
WDSysUser	

これらの考慮事項に基づいて、図 16-5 は、ルックアップ、プロビジョニング、認証などのユーザ関連操作に対する Cisco Unified CallManager 5.0 でのデフォルト動作を示しています。

図 16-5　Cisco Unified CallManager 5.0 のユーザ関連操作に対するデフォルト動作



エンド ユーザは、HTTPS 経由で Cisco Unified CallManager User Options ページにアクセスし、ユーザ名およびパスワードで認証します。User Groups and Roles によって管理者として設定されている場合、エンド ユーザは同じクレデンシャルで Cisco Unified CallManager Administration ページにもアクセスします。

同様に、シスコの他の機能とアプリケーションは、それぞれのアプリケーション ユーザに関連付けられたユーザ名およびパスワードで、HTTPS 経由で Cisco Unified CallManager に対して認証します。

HTTPS メッセージによって伝送される認証確認は、Cisco Unified CallManager の Web サービスにより、Identity Management System（IMS）という内部ライブラリにリレーされます。デフォルト設定では、IMS ライブラリは、組み込みデータベースに対してエンド ユーザとアプリケーション ユーザの両方を認証します。このように、IP Communications システムにおける「現実の」ユーザと内部アプリケーション アカウントの両方が、Cisco Unified CallManager に設定されたクレデンシャルを使用して認証されます。

エンド ユーザは、IP Phone からエクステンション モビリティ サービスにログインするときに、ユーザ名と数値パスワード（PIN）で認証することもできます。この場合、認証確認は HTTP 経由で Cisco Unified CallManager に伝送されますが、やはり Web サービスにより IMS ライブラリにリレーされ、IMS ライブラリは組み込みデータベースに対してクレデンシャルを認証します。

さらに、Directories ボタンを介して IP テレフォニー エンドポイントによって実行されるユーザ ルックアップでは、HTTP 経由で Cisco Unified CallManager の Web サービスと通信し、組み込みデータベースのデータにアクセスします。

エンド ユーザとアプリケーション ユーザの区別の重要性は、社内ディレクトリとの統合が必要な場合に明らかになります。前の項で説明したように、この統合は次の 2 つの独立したプロセスによって実現されます。

- LDAP 同期

  このプロセスでは、Cisco Unified CallManager の Cisco Directory Synchronization（DirSync）という内部ツールを使用して、社内 LDAP ディレクトリから多数のユーザ属性を（手動または定期的に）同期します。この機能を有効にすると、ユーザは社内ディレクトリから自動的にプロビジョニングされます。この機能はエンド ユーザだけに適用され、アプリケーション ユーザは独立したままで、引き続き Cisco Unified CallManager Administration インターフェイスを介してプロビジョニングされます。要約すると、エンド ユーザは社内ディレクトリで定義され、Cisco Unified CallManager データベースに同期されますが、アプリケーション ユーザは Cisco Unified CallManager データベースに保存されるだけで、社内ディレクトリで定義する必要はありません。
- LDAP 認証

  このプロセスでは、IMS ライブラリにより、社内 LDAP ディレクトリに対してユーザ クレデンシャルを認証できます。この機能を有効にすると、エンド ユーザ パスワードは社内ディレクトリに対して認証されますが、アプリケーション ユーザ パスワードは引き続きローカルで Cisco Unified CallManager データベースに対して認証されます。Cisco エクステンション モビリティの PIN も引き続きローカルで認証されます。

Cisco Unified CallManager データベースに対して内部でアプリケーション ユーザを維持および認証すると、社内 LDAP ディレクトリの可用性とは無関係に、これらのアカウントを使用して Cisco Unified CallManager と通信するすべてのアプリケーションと機能に対して復元性が提供されます。

Cisco エクステンション モビリティの PIN も Cisco Unified CallManager データベース内で維持されます。これらの PIN はリアルタイム アプリケーションの必須部分であり、リアルタイム アプリケーションは社内ディレクトリの応答性に依存しないようにする必要があるためです。

次の 2 つの項では、LDAP 同期と LDAP 認証についてさらに詳しく説明し、両方の機能に関して設計上のベスト プラクティスを示します。

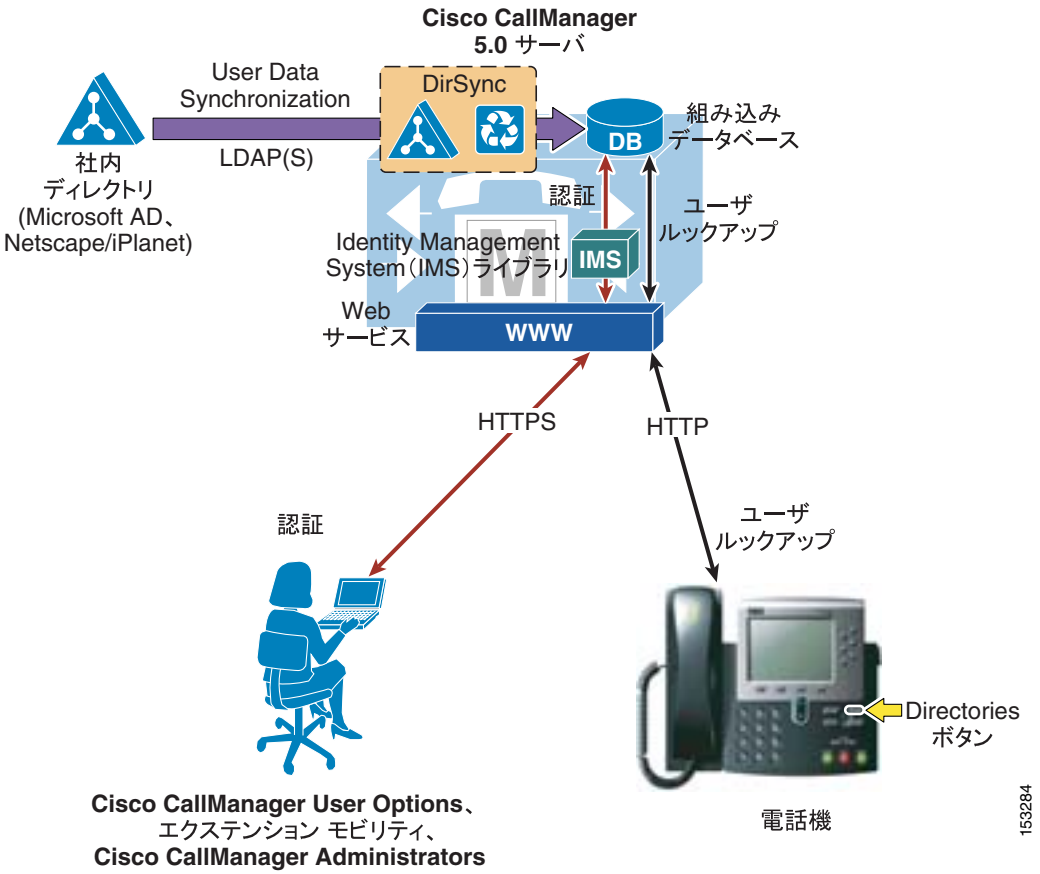
（注） P.16-4 の「IP テレフォニー エンドポイントのディレクトリ アクセス」の項で説明したように、外部 Web サーバで Cisco Unified IP Phone Services SDK を設定することにより、エンドポイントからのユーザ ルックアップを社内ディレクトリに対して実行することもできます。

LDAP 同期

Cisco Unified CallManager を社内 LDAP ディレクトリに同期すると、LDAP ディレクトリに保存されたユーザ データを再利用でき、社内 LDAP ディレクトリをその情報の中央リポジトリとして使用できます。Cisco Unified CallManager 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 データをそのデータベースで作成して維持するための Web インターフェイスを、Cisco Unified CallManager Administration 内に備えています。同期を有効にすると、ローカル データベースは引き続き使用されますが、ユーザ アカウントを作成する Cisco Unified CallManager ファシリティが無効になります。その後、ユーザ アカウントの管理は、LDAP ディレクトリのインターフェイスを介して実施されます（図 16-6 を参照）。

ユーザ アカウント情報は、LDAP ディレクトリから Cisco Unified CallManager パブリッシャ サーバにあるデータベースにインポートされます。LDAP ディレクトリからインポートされた情報は、Cisco Unified CallManager から変更できません。Cisco Unified CallManager 実装に固有の追加のユーザ情報は、Cisco Unified CallManager によって管理され、そのローカル データベース内だけに保存されます。たとえば、デバイスとユーザのアソシエーション、短縮ダイヤル、ユーザ PIN は Cisco Unified CallManager が管理するデータであり、社内 LDAP ディレクトリには存在しません。次に、ユーザ データは組み込みデータベース同期によって、Cisco Unified CallManager パブリッシャ サーバからサブスクライバに伝達されます。

図 16-6　ユーザ データ同期の有効化



同期のために、次のディレクトリが Cisco Unified CallManager でサポートされています。

- Microsoft Active Directory（AD）2000 および 2003
- Netscape Directory Server 4.x、iPlanet Directory Server 5.1、Sun ONE Directory Server 5.2

LDAP 同期をアクティブにすると、上記の LDAP 製品グループのうち、一度にいずれか 1 つのみをクラスタ用に選択できます。また、ディレクトリ ユーザの 1 つの属性が Cisco Unified CallManager User ID フィールドにマッピングするために選択されます。Cisco Unified CallManager はデータへのアクセスに標準 LDAPv3 を使用します。

Cisco Unified CallManager がインポートするデータはすべて、標準属性のデータです。表 16-3 は使用される属性のリストを示しており、これらの属性は 2 つの LDAP 実装グループ間で異なります。Cisco Unified CallManager User ID にマッピングされるディレクトリ属性のデータは、そのクラスタのすべてのエントリ内で固有のものになっている必要があります。**sn** 属性にはデータを格納する必要があります。そうしないと、そのレコードは社内ディレクトリからインポートされません。エンド ユーザ アカウントのインポート中に使用するプライマリ属性が Cisco Unified CallManager データベースのいずれかのアプリケーション ユーザと一致する場合、そのユーザはスキップされます。

一部の Cisco Unified CallManager データベース フィールドではディレクトリ属性を選択できますが、同期アグリーメントごとに単一のマッピングだけを選択できます。

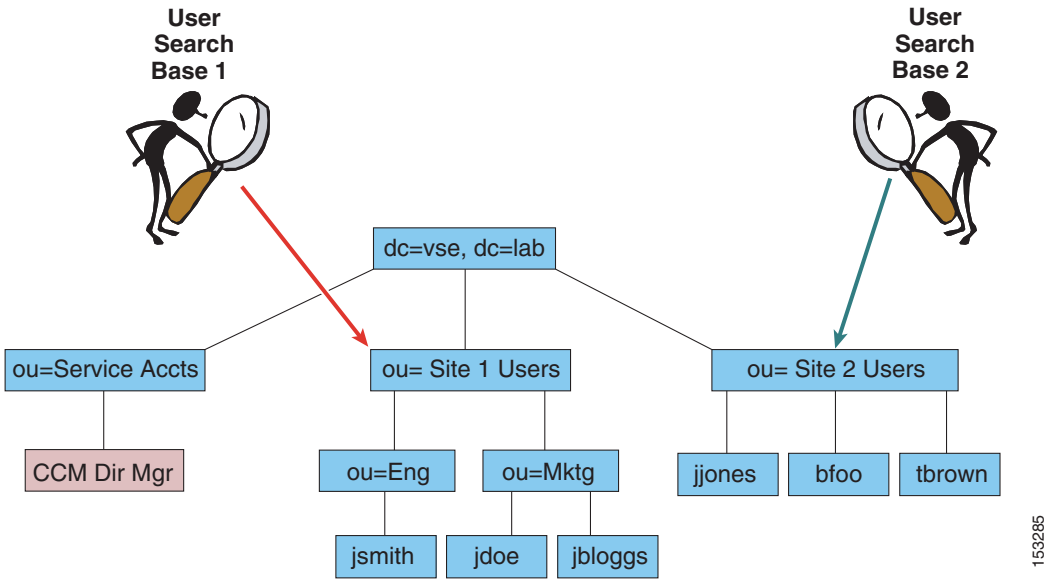
表 16-3　Cisco Unified CallManager でインポートされるデータ属性

Cisco Unified CallManager のユーザ フィールド	Microsoft Active Directory（AD）の属性	Netscape、iPlanet、または Sun ONE の属性
User ID	*次のいずれか* sAMAccountName mail employeeNumber telephoneNumber UserPrincipalName	*次のいずれか* uid mail employeeNumber telephonePhone
First Name	givenName	givenname
Middle Name	*次のいずれか* middleName initials	initials
Last Name	sn	sn
Manager ID	manager	manager
Department	department	departmentnumber
Phone Number	*次のいずれか* telephoneNumber ipPhone	telephonenumber
Mail ID	*次のいずれか* mail sAMAccountName	*次のいずれか* mail uid

同期は、Serviceability Web ページで有効にする Cisco DirSync というプロセスによって実行されます。このプロセスを有効にすると、1 つ以上の同期アグリーメントをシステムで設定できます。アグリーメントでは、LDAP ツリー内で Cisco Unified CallManager がユーザ アカウントの検索を開始する場所となる検索ベースを指定します。Cisco Unified CallManager は、特定の同期アグリーメントについて検索ベースで指定したドメインの領域に存在するユーザのみをインポートできます。

図 16-7 は、2 つの同期アグリーメントを示しています。一方の同期アグリーメントでは、User Search Base 1 を指定し、ユーザ jsmith、jdoe、jbloggs をインポートします。もう一方の同期アグリーメントでは、User Search Base 2 を指定し、ユーザ jjones、bfoo、tbrown をインポートします。CCMDirMgr アカウントは、ユーザ検索ベースで指定した場所の下位に存在しないので、インポートされません。ユーザを LDAP ディレクトリの構造に編成すると、その構造を使用して、どのユーザ グループをインポートするかを制御できます。この例では、単一の同期アグリーメントを使用してドメインのルートを指定することもできましたが、その検索ベースでは Service Accts もインポートしていたと考えられます。検索ベースではドメイン ルートを指定する必要はなく、ツリーのどの場所でも指定できます。

図 16-7　ユーザ検索ベース



データを Cisco Unified CallManager データベースにインポートするために、LDAP Manager Distinguished Name として設定で指定されたアカウントを使用して、システムが LDAP ディレクトリへのバインドを実行し、データベースの読み取りがこのアカウントで実行されます。Cisco Unified CallManager のログインのために、LDAP ディレクトリでアカウントが使用可能である必要があります。ユーザ検索ベースで指定したサブツリー内のすべてのユーザ オブジェクトの読み取り可能な権限を持つ、固有のアカウントを作成することをお勧めします。同期アグリーメントでは、そのアカウントがドメイン内のどこにでも存在できるように、アカウントの完全認定者名を指定します。図 16-7 の例では、CCMDirMgr が同期に使用するアカウントです。

アカウントのインポートは、LDAP Manager Distinguished Name アカウントの権限を使用して制御できます。この例では、ou=Eng への読み取りアクセスはできるが ou=Mktg への読み取りアクセスはできないようにこのアカウントを制限した場合、Eng の下位にあるアカウントのみがインポートされます。

同期アグリーメントには、複数のディレクトリ サーバを指定して冗長性を実現する機能があります。同期の試行時に使用するディレクトリ サーバを 3 つまで、順序付きのリストにして設定に指定できます。これらのサーバでの試行が、リストの最後まで順に行われます。どのディレクトリ サーバも応答しない場合、同期には失敗しますが、設定済みの同期スケジュールに従って再試行されます。

同期のメカニズム

同期アグリーメントでは、同期を開始する時刻を指定し、再同期の期間を時間、日、週、月のいずれかの単位（最小値は 6 時間）で指定します。同期アグリーメントは、特定の時刻に 1 回だけ実行するように設定することもできます。

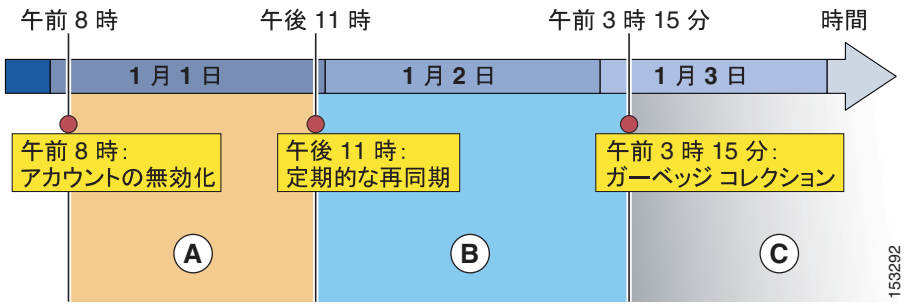
Cisco Unified CallManager パブリッシャ サーバで同期を初めて有効にすると、社内ディレクトリに存在するユーザ アカウントが Cisco Unified CallManager データベースにインポートされます。そして、その後のプロセスに従って、既存の Cisco Unified CallManager エンドユーザ アカウントがアクティブになってデータが更新されるか、新しいエンドユーザ アカウントが作成されます。

1. エンドユーザ アカウントがすでに Cisco Unified CallManager データベースに存在するときに同期アグリーメントを設定した場合、Cisco Unified CallManager ですべての既存のアカウントは非アクティブとマークされます。同期アグリーメントの設定で、Cisco Unified CallManager UserID への LDAP データベース属性のマッピングを指定します。同期中に LDAP データベースのアカウントが既存の Cisco Unified CallManager アカウントと一致すると、その Cisco Unified CallManager アカウントは再びアクティブとマークされます。
2. 同期の完了後、アクティブに設定されなかったアカウントは、ガーベッジ コレクション プロセスの実行時に Cisco Unified CallManager から永続的に削除されます。ガーベッジ コレクションは、午前 3 時 15 分の定時に自動的に実行されるプロセスで、設定はできません。Cisco Unified CallManager は同期が設定されている間はアカウントを管理できないので、LDAP ディレクトリ アカウントと一致しない Cisco Unified CallManager アカウントの削除が必要です。
3. 後で社内ディレクトリに変更を加えると、スケジューリングされた次回の同期期間に、完全な再同期として Microsoft Active Directory から同期が行われます。これに対して、Netscape、iPlanet、Sun ONE の各製品は、ディレクトリに変更が加えられると差分同期を実行します。次の項では、2 つのシナリオのそれぞれの例を示します。

Active Directory でのアカウント同期

図 16-8 は、LDAP 同期と LDAP 認証の両方を有効にした Cisco Unified CallManager 配置について、イベントのスケジュールの例を示しています。再同期は、毎日午後 11 時に設定されています。

図 16-8　Active Directory での変更の伝達



最初の同期の後、アカウントの作成、削除、または無効化は、図 16-8 に示すスケジュールに従って、次の手順で説明するように Cisco Unified CallManager に伝達されます。

1. 1 月 1 日の午前 8 時に、AD でアカウントを無効にするか削除します。これ以降、期間 A 中は、Cisco Unified CallManager が認証を AD にリダイレクトするため、このユーザのパスワード認証（たとえば、Cisco Unified CallManager User Options ページ）は失敗します。ただし、PIN は Cisco Unified CallManager データベースに保存されているため、PIN 認証（たとえば、エクステンション モビリティ ログイン）は今までどおり成功します。

2. 定期的な再同期は、1 月 1 日の午後 11 時にスケジューリングされています。このプロセス中、Cisco Unified CallManager はすべてのアカウントを検証します。AD で無効にするか削除したアカウントは、この時点で、Cisco Unified CallManager データベースでは非アクティブとしてタグ付けされます。1 月 1 日の午後 11 時より後に、アカウントが非アクティブとマークされると、Cisco Unified CallManager による PIN 認証とパスワード認証は両方とも失敗します。
3. アカウントのガーベッジ コレクションは、毎日午前 3 時 15 分の定時に実行されます。このプロセスでは、24 時間以上にわたって非アクティブとマークされていたレコードについて、ユーザ情報を Cisco Unified CallManager データベースから永続的に削除します。この例では、1 月 2 日の午前 3 時 15 分に実行するガーベッジ コレクションでは、アカウントが非アクティブになってまだ 24 時間が経過していないので、アカウントを削除しません。したがって、アカウントは 1 月 3 日の午前 3 時 15 分に削除されます。この時点で、ユーザ データは Cisco Unified CallManager から永続的に削除されます。

期間 A の開始時にアカウントを AD で作成していた場合、そのアカウントは期間 B の開始時に実行される定期的な再同期で Cisco Unified CallManager にインポートされ、Cisco Unified CallManager ですぐにアクティブになります。

(注) 上記の動作は Cisco Unified CallManager Release 5.0(3) 以降に適用されます。Release 5.0(1) および 5.0(2) では、非アクティブとマークされたユーザの PIN 認証は失敗しないので、図 16-8 で削除されたユーザでも、期間 B 中にエクステンション モビリティ サービスにログインできます。これらのリリースでは、ディレクトリ認証を有効にしない場合、ユーザが非アクティブとマークされているとき（つまり、期間 B 中）にパスワード認証も成功します。

Netscape、iPlanet、または Sun ONE でのアカウント同期

Netscape、iPlanet、Sun ONE の各製品は差分同期アグリーメントをサポートし、Active Directory とは異なる同期スケジュールを使用します。図 16-9 では、LDAP 同期と LDAP 認証の両方を有効にした Cisco Unified CallManager 配置について、この同期スケジュールの例を示しています。

図 16-9　Netscape、iPlanet、Sun ONE での変更の伝達

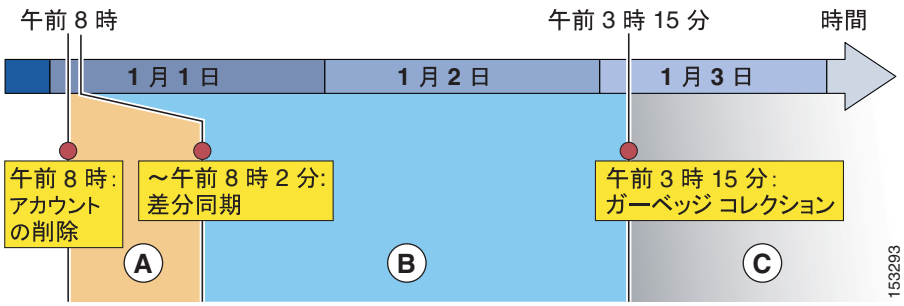


図 16-9 の例は、次の手順から構成されます。

1. 1 月 1 日の午前 8 時にアカウントが社内ディレクトリから削除され、これにより、差分更新データが LDAP サーバから Cisco Unified CallManager に送信されます。Cisco Unified CallManager は、データに対応するコピーを非アクティブに設定します。LDAP 認証が設定されているので、LDAP サーバがレコードを削除するとすぐに、ユーザはパスワードによるログインができなくなります。また、Cisco Unified CallManager レコードが非アクティブとマークされると、PIN をログインに使用できません。
2. 期間 B 中は、ユーザのレコードは非アクティブですが、まだ Cisco Unified CallManager に存在します。

3. 1 月 2 日の午前 3 時 15 分にガーベッジ コレクションが実行されるときは、レコードが非アクティブになってまだ 24 時間が経過していません。データは 1 月 3 日の期間 C の開始時まで Cisco Unified CallManager データベースに残り、ガーベッジ コレクション プロセスがこの日の午前 3 時 15 分に再び実行され、レコードが 24 時間以上にわたって非アクティブであったことを確認します。その結果、レコードはデータベースから永続的に削除されます。

ディレクトリで新規に作成したアカウントは、差分更新データによって同様に Cisco Unified CallManager に同期し、差分更新データが受信されるとすぐに使用できます。

(注) 上記の動作は Cisco Unified CallManager Release 5.0(3) 以降に適用されます。Release 5.0(1) および 5.0(2) では、Sun ONE Directory Server から削除されたユーザ アカウントは、非アクティブの段階を経ることなく、差分同期が実行されるとすぐに Cisco Unified CallManager データベースから削除されます。

セキュリティの考慮事項

アカウントのインポート中は、LDAP ディレクトリから Cisco Unified CallManager データベースに、パスワードも PIN もコピーされません。Cisco Unified CallManager で LDAP 認証を有効にしない場合、エンド ユーザのパスワードと PIN は、Cisco Unified CallManager Administration を使用して管理します。デフォルトでは、アカウントの作成時にパスワードは **ciscocisco** に設定され、PIN は **12345** に設定されます。これらの設定は、ユーザがユーザ Web ページを使用するか、管理者が管理者 Web ページを使用して変更できます。パスワードと PIN は、暗号化形式で Cisco Unified CallManager データベースに保存されます。ディレクトリ パスワードを使用してエンド ユーザを認証する場合は、P.16-19 の「LDAP 認証」の項を参照してください。

Cisco Unified CallManager および LDAP サーバで Secure LDAP（SLDAP）を有効にすることにより、Cisco Unified CallManager パブリッシャ サーバとディレクトリ サーバ間の接続を保護できます。Secure LDAP を使用すると、Secure Socket Layer（SSL）接続で LDAP 送信ができます。Cisco Unified CallManager Platform Administration 内で SSL 証明書をアップロードすることにより、Secure LDAP を有効にできます。詳細な手順については、http://www.cisco.com で入手可能な Cisco Unified CallManager の製品マニュアルを参照してください。

LDAP 同期のベスト プラクティス

Cisco Unified CallManager 5.0 で LDAP 同期を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内で特定のアカウントを使用し、Cisco Unified CallManager 同期アグリーメントがそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Cisco Unified CallManager 専用のアカウントを使用することをお勧めします（このアカウントのパスワードをディレクトリで変更した場合、変更を考慮して Cisco Unified CallManager を再設定する必要があります）。
- 所定のクラスタにあるすべての同期アグリーメントは、同じ LDAP サーバ ファミリ（Microsoft AD または Netscape、iPlanet、Sun ONE）と統合する必要がある。
- 複数のアグリーメントが同時に同じ LDAP サーバに照会することがないように、同期アグリーメントの定期性に時間差を設ける。待機期間中の同期時刻を選択します。
- ユーザ データのセキュリティが重要な場合、Cisco Unified CallManager Administration の LDAP Directory 設定ページで **Use SSL** フィールドのチェックボックスをオンにして、Secure LDAP（SLDAP）を有効にする。
- Cisco Unified CallManager UserID フィールドへのマッピングのために選択した LDAP ディレクトリ属性が、そのクラスタのすべての同期アグリーメント内で固有であることを確認する。

- UserID として選択した属性は、Cisco Unified CallManager で定義したアプリケーション ユーザのいずれかの属性と同じであってはならない。
- 同期前の Cisco Unified CallManager データベースにある既存のアカウントは、LDAP ディレクトリからインポートされたアカウントの属性に一致する場合にのみ維持される。Cisco Unified CallManager UserID に一致する属性は、同期アグリーメントによって確認されます。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- エンドユーザ アカウントは LDAP ディレクトリの管理ツールによって管理し、これらのアカウントのシスコ固有データは Cisco Unified CallManager Administration Web ページによって管理する。

Microsoft Active Directory に関する追加の考慮事項

ドメインの同期アグリーメントでは、ドメイン外のユーザや子ドメイン内のユーザは同期されません。同期プロセス中は Cisco Unified CallManager が AD 照会に従わないためです。図 16-10 の例では、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。Search Base 1 ではツリーのルートを指定しますが、子ドメインのいずれかに存在するユーザはインポートしません。範囲は VSE.LAB に限定されており、残りの 2 つのドメインに対し、そのユーザをインポートするように別々のアグリーメントが設定されています。

図 16-10　複数の Active Directory ドメインでの同期

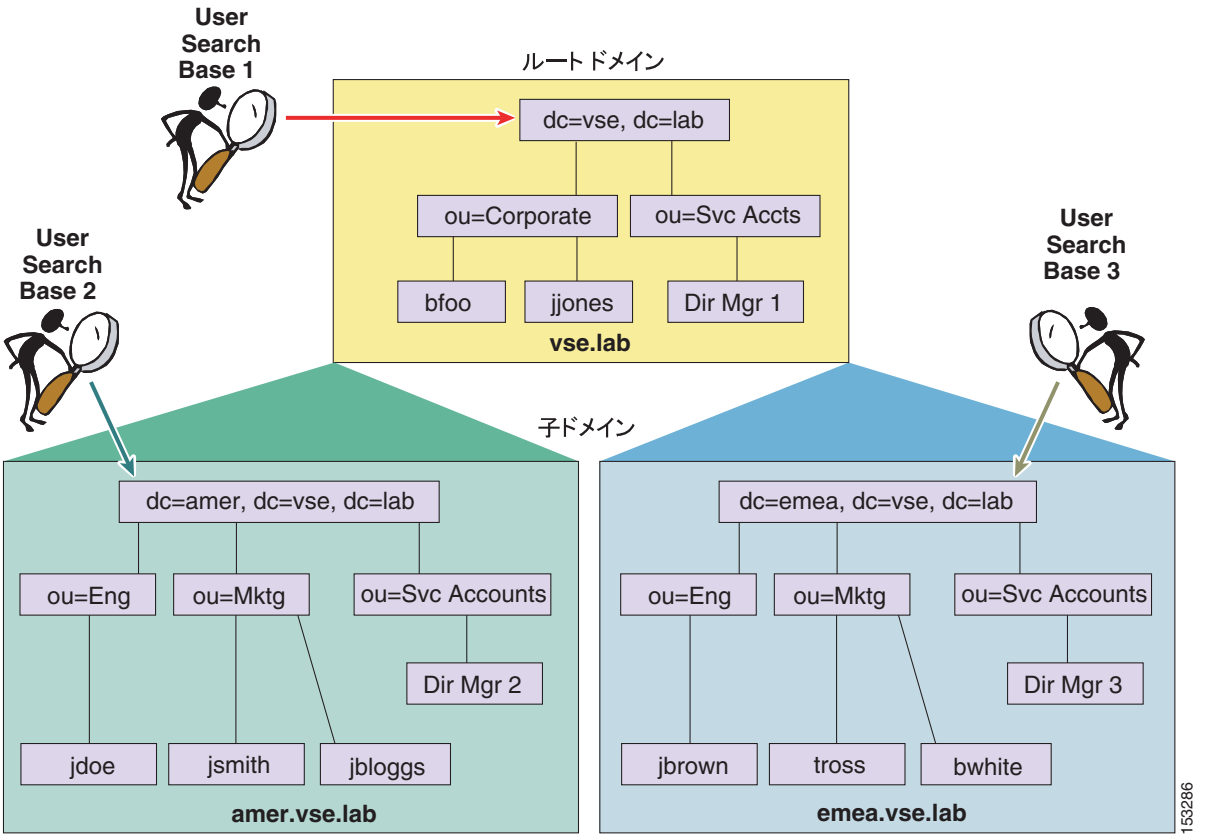
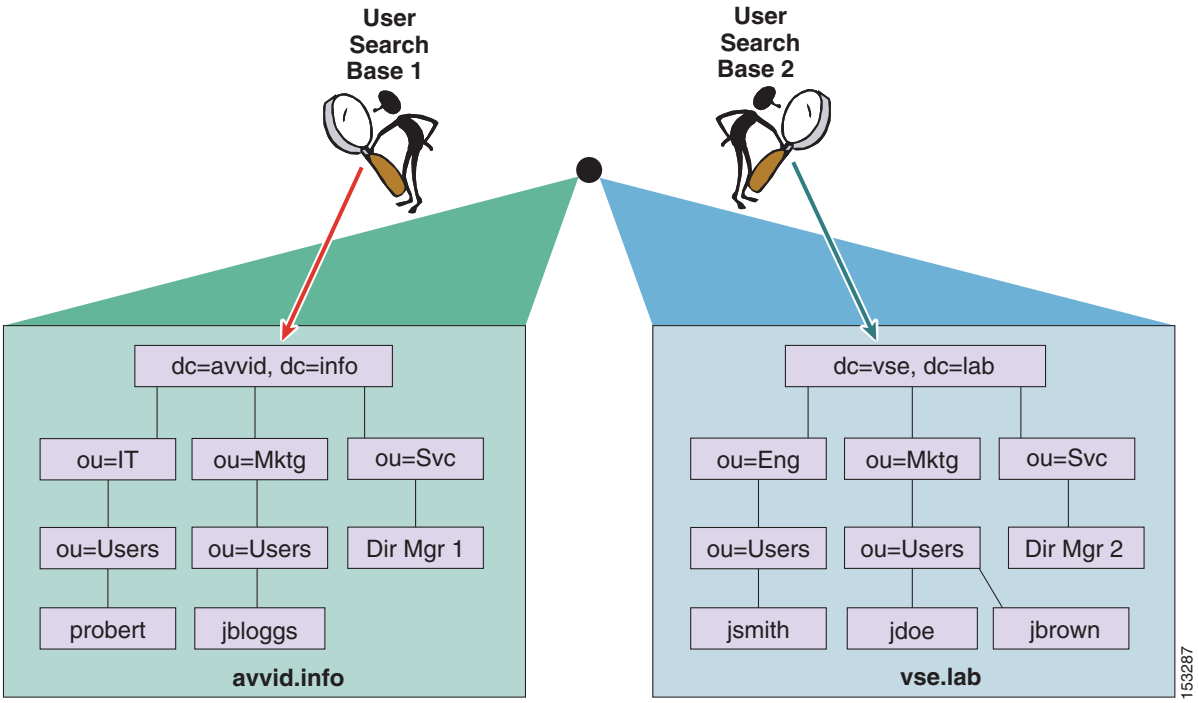


図 16-10 では、ドメインとサブドメインのそれぞれに少なくとも 1 つの Domain Controller（DC; ドメイン コントローラ）が関連付けられ、3 つの同期アグリーメントはそれぞれ適切なドメイン コントローラを指定します。DC にある情報は、その DC が存在するドメイン内のユーザの情報だけなので、すべてのユーザをインポートするために 3 つの同期アグリーメントが必要です。

図 16-11 に示すように、複数のツリーを含む AD フォレストで同期を有効にした場合も、上記と同じ理由で複数の同期アグリーメントが必要です。さらに、UserPrincipalName（UPN）属性がフォレスト全体で固有であることが Active Directory によって保証され、この属性は Cisco Unified CallManager UserID にマッピングする属性として選択する必要があります。マルチツリーの AD シナリオで UPN 属性を使用する場合の追加の考慮事項については、P.16-22 の「Microsoft Active Directory に関する追加の考慮事項」の項を参照してください。

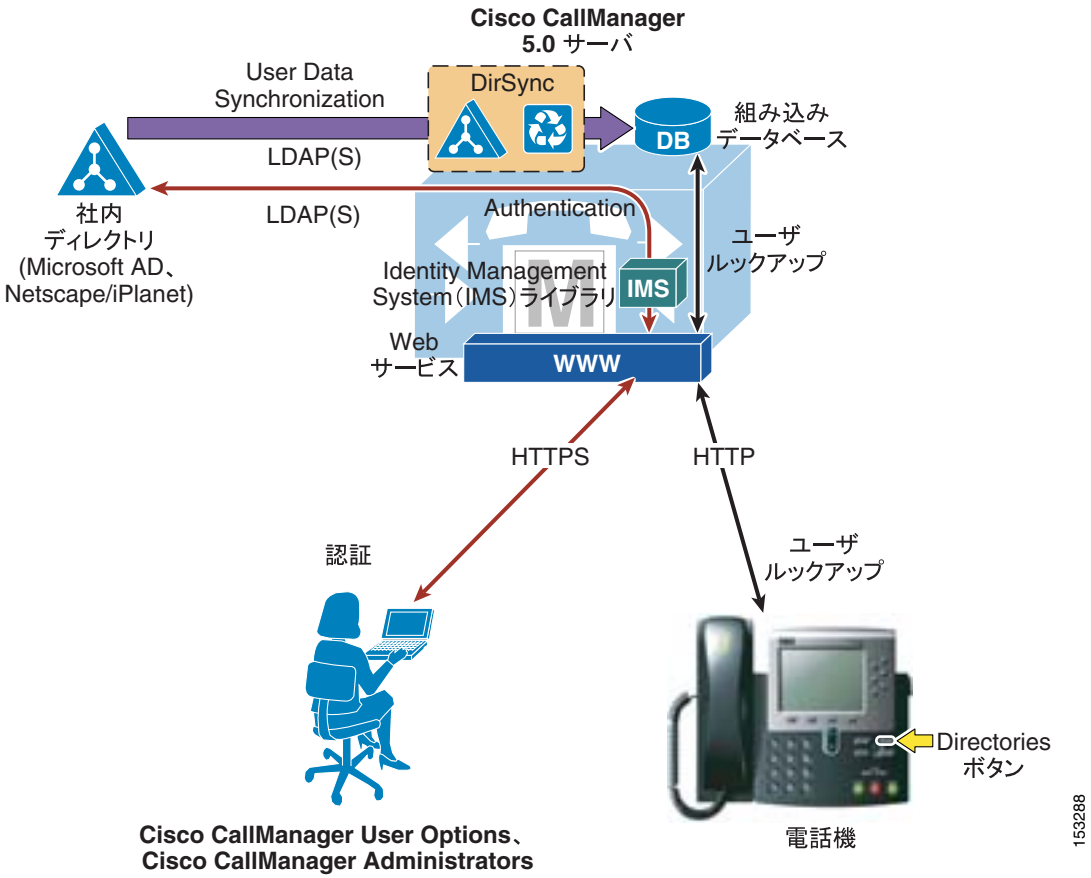
図 16-11　複数の AD ツリー（不連続なネームスペース）での同期



LDAP 認証

LDAP 認証機能を使用すると、組み込みデータベースを使用する代わりに、社内 LDAP ディレクトリに対して Cisco Unified CallManager でエンド ユーザ パスワードを認証できます。図 16-12 に示すように、Cisco Unified CallManager 内の IMS モジュールと社内ディレクトリ サーバ間で確立した LDAPv3 接続によって、この認証が実現されます。

図 16-12　LDAP 認証の有効化



LDAP 同期機能の場合と同様に、次の社内ディレクトリ製品がサポートされます。

- Microsoft Active Directory（AD）2000 および 2003
- Netscape Directory Server 4.x、iPlanet Directory Server 5.1、Sun ONE Directory Server 5.2

認証機能では、冗長性を得るためにサーバを 3 つまで設定でき、必要に応じて Secure LDAP（SLDAP）を有効にした場合、ディレクトリ サーバへの保護接続もサポートされます。認証機能は、LDAP 同期機能とは無関係に有効にできます。ただし、認証を単独で有効にする場合は、Cisco Unified CallManager のユーザ ID が社内ディレクトリで定義されているユーザ ID と一致することを確認する必要があります。

認証を有効にした場合の Cisco Unified CallManager の動作説明を、次に示します。

- エンド ユーザ パスワードは、社内ディレクトリ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、Cisco Unified CallManager データベースに対して認証される。
- エンド ユーザ PIN は、Cisco Unified CallManager データベースに対して認証される。

この動作は、リアルタイム IP Communications システムの操作を社内ディレクトリの可用性に依存しないようにしながら、シングル ログオン機能をエンド ユーザに提供するという原則に従ったものです。図 16-13 に図示します。

図 16-13　エンド ユーザ パスワード、アプリケーション ユーザ パスワード、エンド ユーザ PIN の認証

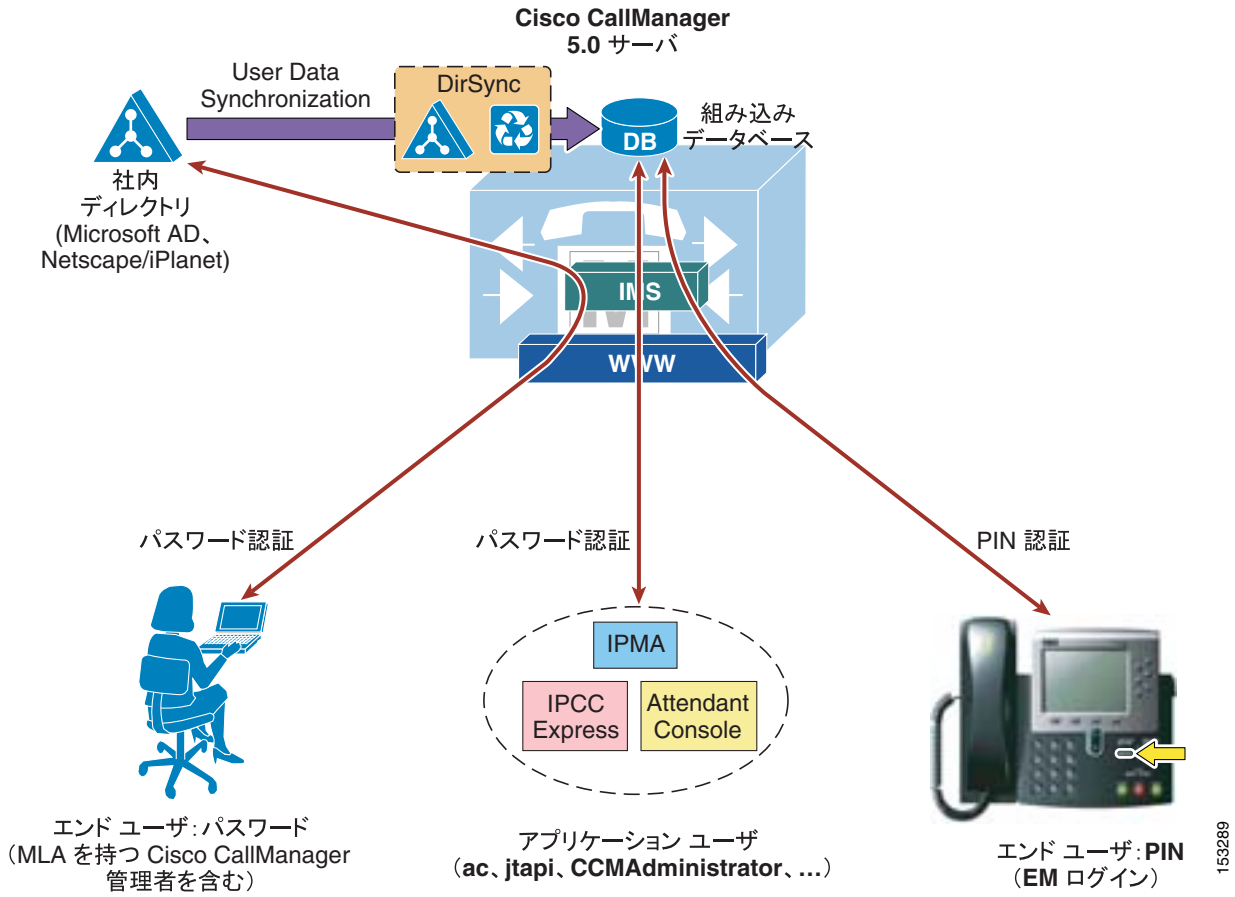
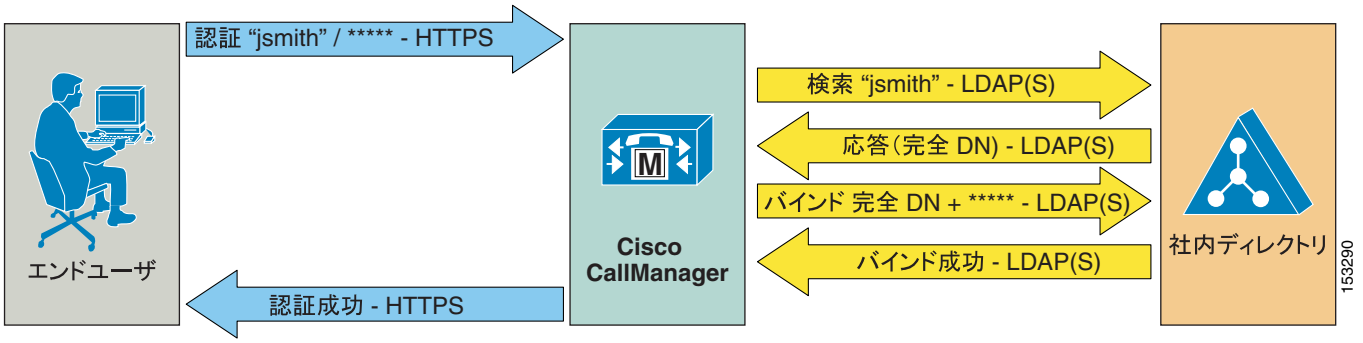


図 16-14 は、エンド ユーザを社内 LDAP ディレクトリに対して認証するために Cisco Unified CallManager で採用された、次のプロセスを示しています。

1. まず、ユーザは、HTTPS 経由で Cisco Unified CallManager User Options ページに接続し、ユーザ名とパスワードで認証を試行します。この例では、ユーザ名は jsmith です。
2. 次に、Cisco Unified CallManager はユーザ名 jsmith に関する LDAP 照会を発行し、LDAP Authentication 設定ページの LDAP Search Base で指定された値を、この照会の範囲として使用します。SLDAP を有効にした場合、この照会は SSL 接続を通じて行われます。
3. 社内ディレクトリ サーバは、LDAP 経由で、ユーザ jsmith の完全 Distinguished Name（DN; 認定者名）で応答します（たとえば、「cn=jsmith, ou=Users, dc=vse, dc=lab」）。
4. 次に、Cisco Unified CallManager は、この完全 DN とユーザが提供するパスワードを使用して、LDAP バインドを試行します。
5. LDAP バインドが成功した場合、Cisco Unified CallManager は、要求された設定ページにユーザが進むことを許可します。

図 16-14　認証プロセス



Cisco Unified CallManager 5.0 で LDAP 認証を配置する場合は、設計と実装に関する次のベスト プラクティスに従ってください。

- 社内ディレクトリ内でアカウントを作成し、Cisco Unified CallManager がそのディレクトリに対して接続および認証できるようにする。目的の検索ベース内にあるすべてのユーザ オブジェクトを「読み取る」ように最小権限を設定し、期限切れにならないようにパスワードを設定した状態で、Cisco Unified CallManager 専用のアカウントを使用することをお勧めします（このアカウントのパスワードをディレクトリで変更した場合、変更を考慮して Cisco Unified CallManager を再設定する必要があります）。LDAP 同期も有効にした場合は、同じアカウントを両方の機能に使用できます。
- LDAP Manager Distinguished Name および LDAP Password で前述のアカウントのクレデンシャルを指定し、LDAP User Search Base ですべてのユーザが存在するディレクトリ サブツリーを指定することにより、Cisco Unified CallManager で LDAP 認証を有効にする。
- 冗長性が得られるように、2 台以上の LDAP サーバを設定する。ホスト名の代わりに IP アドレスを使用すると、Domain Name System（DNS; ドメイン ネーム システム）の可用性に依存しなくなります。
- この方法では、シングル ログオン機能をすべてのエンド ユーザに提供する。エンド ユーザは、Cisco Unified CallManager User Options ページにログインすると、社内ディレクトリ クレデンシャルを使用できるようになります。
- 社内ディレクトリ インターフェイスでエンド ユーザ パスワードを管理する（認証を有効にすると、Cisco Unified CallManager Administration ページにパスワード フィールドが表示されなくなります）。
- Cisco Unified CallManager Administration または Cisco Unified CallManager User Options ページでエンド ユーザ PIN を管理する。
- Cisco Unified CallManager Administration でアプリケーション ユーザ パスワードを管理する（これらの仮想ユーザは Cisco Unified Communications の他の機能およびアプリケーションとの通信専用であり、実在の人物に関連付けられていません）。
- 対応するエンド ユーザを Cisco Unified CallManager Administration ページから Unified CM Super Users ユーザ グループに追加することにより、Cisco Unified CallManager 管理者のシングル ログオンを有効にする。カスタマイズしたユーザ グループおよびロールを作成することにより、複数レベルの管理者権利を定義できます。

Microsoft Active Directory に関する追加の考慮事項

Microsoft Active Directory で LDAP 認証を有効にする場合、応答時間の短縮のために Microsoft Active Directory グローバル カタログ サーバに照会するように Cisco Unified CallManager を設定することをお勧めします。

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 Authentication ページの LDAP Server Information を設定し、LDAP ポートを 3268 として設定するだけです。

Microsoft AD から同期するユーザが複数のドメインに属していると、認証へのグローバル カタログの使用がさらに効率的になります。Cisco Unified CallManager は、照会に従う必要がなく、すぐにユーザを認証できるためです。このような場合は、Cisco Unified CallManager がグローバル カタログ サーバを指すようにし、LDAP User Search Base をルート ドメインの最上位に設定します。

複数のツリーを含む Microsoft AD フォレストの場合には、追加の考慮事項が適用されます。単一の LDAP 検索ベースでは複数のネームスペースを扱えないので、Cisco Unified CallManager は別のメカニズムを使用して、これらの不連続なネームスペース間でユーザを認証する必要があります。

P.16-11 の「LDAP 同期」の項で説明したように、複数のツリーがある AD フォレストで同期をサポートするために、UserPrincipalName（UPN）属性を Cisco Unified CallManager 内でユーザ ID として使用する必要があります。ユーザ ID が UPN の場合、Cisco Unified CallManager Administration の LDAP Authentication 設定ページで LDAP Search Base フィールドへの入力はできませんが、その代わりに「LDAP user search base is formed using userid information.」という注意が表示されます。

実際には、図 16-15 に示すように、ユーザごとに UPN サフィックスからユーザ検索ベースが導き出されます。この例では、Microsoft Active Directory フォレストは avvid.info と vse.lab という 2 つのツリーで構成されます。同じユーザ名が両方のツリーに表示される場合があるため、同期プロセス中および認証プロセス中は UPN を使用してデータベースのユーザを固有に識別するように、Cisco Unified CallManager が設定されています。

図 16-15　複数のツリーがある Microsoft AD フォレストでの認証

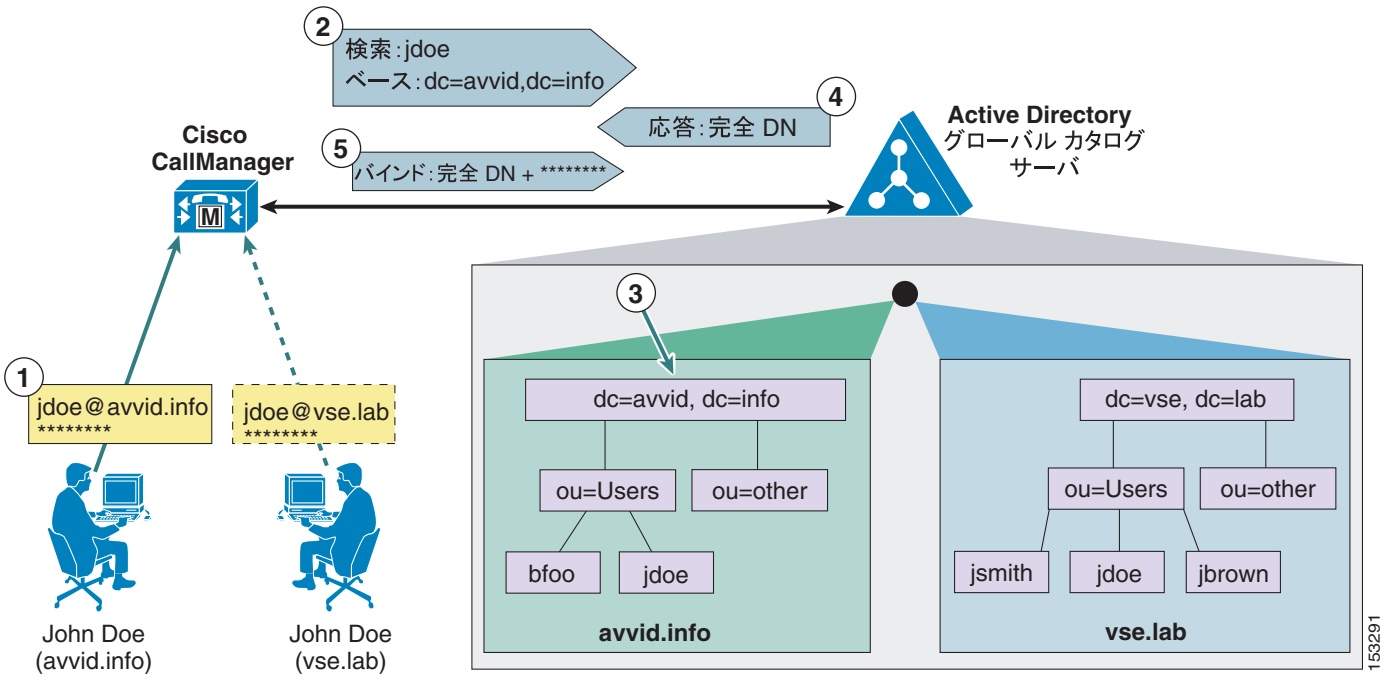


図 16-15 に示すように、John Doe という名前のユーザが avvid.info ツリーと vse.lab ツリーの両方に存在します。次の手順は、UPN が jdoe@avvid.info となる第 1 のユーザに対する認証プロセスを示しています。

1. ユーザは、ユーザ名（UPN に対応するもの）とパスワードを使用し、HTTPS 経由で Cisco Unified CallManager に対して認証します。
2. Cisco Unified CallManager は、Microsoft Active Directory グローバル カタログ サーバに対して LDAP 照会を実行し、UPN で指定したユーザ名（@ 記号より前の部分）を使用して、UPN サフィックス（@ 記号より後の部分）から LDAP 検索ベースを得ます。この場合、ユーザ名は jdoe で、LDAP 検索ベースは「dc=avvid, dc=info」です。
3. Microsoft Active Directory は、LDAP 照会で指定したツリーのユーザ名に対応する正しい認定者名を識別します。この場合は、「cn=jdoe, ou=Users, dc=avvid, dc=info」です。
4. Microsoft Active Directory は LDAP 経由で、このユーザの完全認定者名を使用して Cisco Unified CallManager に応答します。
5. Cisco Unified CallManager は、提供された認定者名とユーザが最初に入力したパスワードで LDAP バインドを試行し、その後は図 16-14 に示す標準的な場合と同様に、認証プロセスが続行されます。

（注） 複数のツリーを含む Microsoft AD フォレストでの LDAP 認証のサポートは、上記の方法だけで行われます。したがってサポートは、ユーザの UPN サフィックスが、そのユーザが存在するツリーのルート ドメインに対応する配置だけに限定されます。UPN サフィックスがツリーの実際のネームスペースから分離されている場合は、Microsoft Active Directory フォレスト全体で Cisco Unified CallManager ユーザを認証できなくなります（ただし、その場合でも、別の属性をユーザ ID として使用し、統合をフォレスト内の単一のツリーに限定することはできます）。

CHAPTER 17

IP テレフォニー移行オプション

この章では、IP テレフォニー システム（または他の電話システム）に移行するための、次の主な方法について説明します。

- 段階的な移行（P.17-2）
- パラレル カットオーバー（P.17-3）

どちら方法が正しいというわけではありません。お客様の状況や好みに応じて、どちらのオプションを使用するかを決めてください。

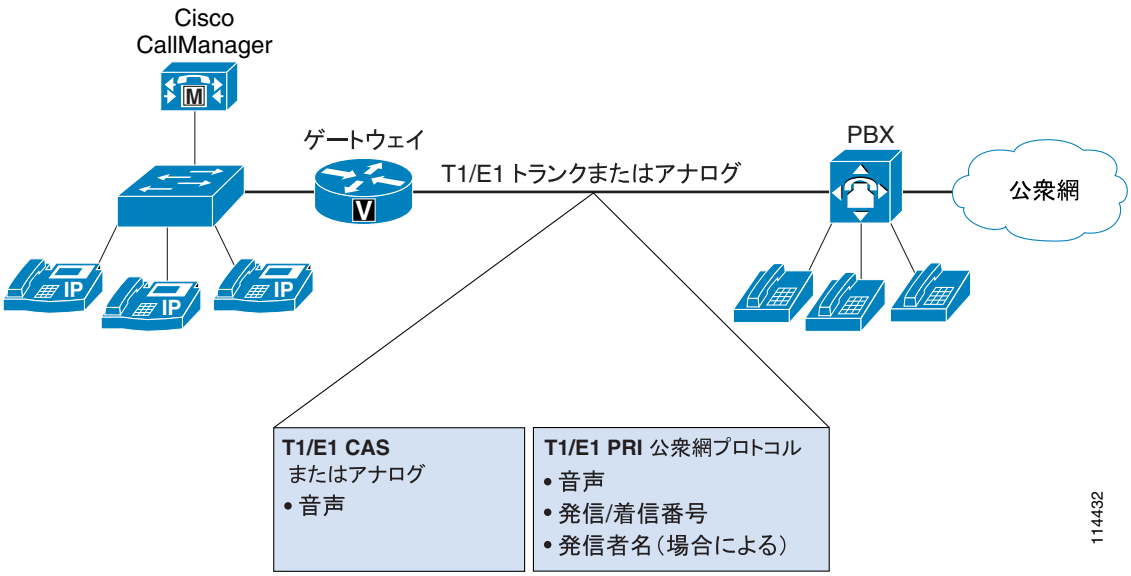
この章では、P.17-4 の「マルチサイト企業における QSIG の必要性」についても説明します。

段階的な移行

この方法では、通常、メインの社内 PBX に接続されている小規模な初期 IP テレフォニー配置が実現されます。どのシグナリング プロトコルを選択するかは、必要な機能および実装コストによって決まります。Cisco Unified CallManager は、一般的な公衆網タイプの PRI または QSIG PRI と、H.323 および SIP をサポートできます。これらのオプションのうち、T1/E1 QSIG は、2 つのシステム間で最高レベルの機能透過性を実現します。

公衆網タイプの PRI は、基本的なコール接続および Automatic Number Identification（ANI; 自動番号識別）を提供します。場合によっては、図 17-1 に示しているように、このプロトコルが発信者名情報をサポートすることもあります。

図 17-1　シグナリング プロトコルによってサポートされる機能



このレベルの接続は、すべての PBX に使用できます。つまり、Cisco Unified CallManager を接続の「ネットワーク」側として設定できるため、PRI を介してパブリック ネットワークに接続できる PBX は Cisco Unified CallManager に接続できます。

Cisco Unified CallManager Release 3.3 以降では、International Standards Organization（ISO; 国際標準化機構）バリアントの QSIG が組み込まれています。QSIG プロトコルを使用すると、公衆網タイプの PRI から得られる機能に加えて、異なるベンダーの PBX 間の機能透過性を実現できます。したがって、このプロトコルは、すでに複雑なネットワークを稼働している大規模な企業に適しています（P.17-4 の「マルチサイト企業における QSIG の必要性」を参照）。

公衆網タイプの PRI や QSIG でも、段階的な移行のプロセスはほぼ同じです。移行が完了するまで、加入者を一度に 1 グループずつ、グループ単位で PBX から Cisco Unified CallManager に移動します。

約 60 個のビルディングに約 23,000 人の加入者が収容されているシスコの San Jose キャンパスでは、開始から終了まで 1 年以上かかって、この方法で IP テレフォニーに移行しました。週末ごとに 1 つのビルディングを変換しました。選択したビルディング内のすべての加入者を識別し、金曜日の晩にその内線番号を PBX から削除しました。同時に、その内線番号をダイヤルした人が正しい PRI トランクを介してルーティングされ、Cisco Unified CallManager に転送されるように、PBX ルーティング テーブルに追加の設定を加えました。週末の間、Cisco Unified CallManager に加入者の新しい内線番号を作成し、新しい IP Phone を適切なロケーションに配置して、月曜日の朝までに使用できるよう準備しました。すべての加入者を移行するまで、このプロセスを各ビルディングに対して繰り返しました。

パラレル カットオーバー

この方法は、完全な IP テレフォニー インフラストラクチャの実装から開始されます。完全な IP テレフォニー インフラストラクチャとは、冗長で、アベイラビリティが高く、QoS 対応のインフラストラクチャであり、インライン パワーが供給されるイーサネット ポートを装備しています。インフラストラクチャの完成後、IP テレフォニー アプリケーションを配置できます。加入者が自分のデスクに 2 台の電話機（IP Phone と PBX 電話機）を同時に置くことができるように、すべての IP Phone とゲートウェイを完全に設定および配置できます。この方法を使用すると、システムをテストする機会が得られ、加入者には新しい IP Phone に慣れるための時間が与えられます。発信専用トランクを IP テレフォニー システムに接続することもできます。これにより、加入者は、新しい IP Phone で内部コールだけではなく外部コールも発信できます。

IP テレフォニー システムを完全に配置した後、着信公衆網トランクを PBX から IP テレフォニー ゲートウェイに移動して新しいシステムの完全な運用を開始するための時間枠を選択できます。IP テレフォニー システムが正常に動作することを確信するまで PBX をそのまま残し、確信した時点で PBX を撤去することもできます。

パラレル カットオーバーは、段階的な移行に比べて次のような利点があります。

- 予期せぬ事態が発生した場合のために、パラレル カットオーバーでは、着信公衆網トランクを IP テレフォニー ゲートウェイから PBX に戻すだけで PBX システムに戻ることができるバックアウト計画が提供される。
- パラレル　カットオーバーでは、システムによって実際の公衆網トラフィックが伝送される前に、IP テレフォニー データベースの設定を確認できる。このシナリオは、着信公衆網トランクを PBX から IP テレフォニー ゲートウェイに移動するカットオーバー前のどれだけの期間でも実行できるため、加入者情報、電話機、ゲートウェイ、ダイヤル プランなどすべての設定が正しいことを確認できます。
- 着信公衆網トランクのカットオーバー前の都合のよいときに、加入者が IP テレフォニー システムを調べたり使用したりできるようにして、ゆったりとしたペースでトレーニングを実施できる。
- システム管理者が「対象となるコミュニティ」に対して特別な準備をする必要がない。段階的な移行方法では、コール ピックアップ グループ、ハント グループ、シェアドラインなどの整合性を保つことを考慮する必要があります。パラレル カットオーバーでサイト全体を移行する場合は、これらのアソシエーションを簡単に保持できます。

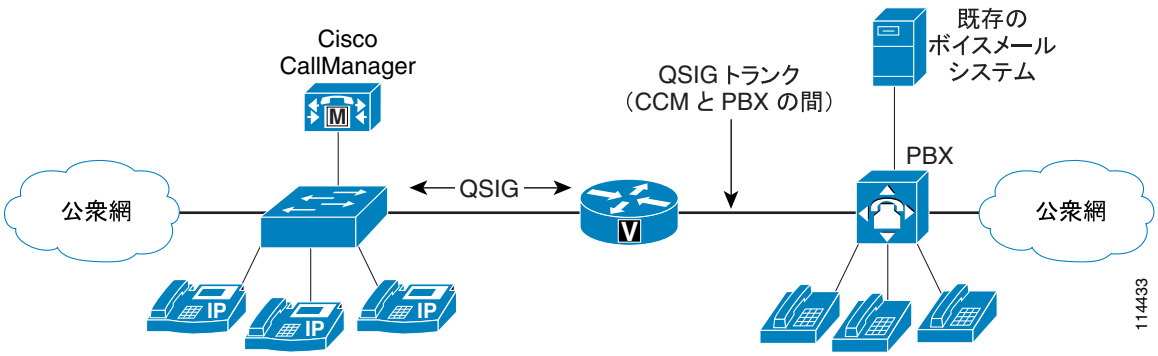
パラレル カットオーバーの 1 つの欠点は、システムの運用開始前にシステム全体を準備しておく必要があるため、最初から IP テレフォニー ソリューションに対する完全な資金供給が必要であるということです。これに対して、段階的な移行では、必要に応じてシステムの個々のコンポーネントを購入でき、完全な配置に移行する前に、小規模な試行システムから始めることができます。

マルチサイト企業における QSIG の必要性

1 つのロケーションだけで構成されている企業もありますが、多数のサイトで構成され、その一部のサイトが遠方に散在している企業もあります。マルチサイト企業の PBX ネットワークは、通常、Avaya DCS、Nortel MCDN、Siemens CorNet、NEC CCIS、Fujitsu FIPN、Alcatel ABC などの専用プロトコルを実行している T1 トランクまたは E1 PRI トランク（ロケーションに応じて異なる）を使用して接続されています。これらの専用ネットワーキング プロトコルによって、PBX は加入者間の高レベルの機能透過性を提供できます。

QSIG は異なるベンダーの PBX の相互接続を可能にするために開発されたため、同様のレベルの機能透過性を実現できます。シスコは、まず、Cisco Unified CallManager Release 3.3 に QSIG を追加して、Cisco Unified CallManager を大規模企業ネットワークに導入できるようにしました（図 17-2 を参照）。

図 17-2　Cisco Unified CallManager と PBX の間で使用される QSIG



Cisco Unified CallManager Release 5.0 で実装される QSIG は、次の機能をサポートしています。

- 基本的なコール
- Direct Inward Dialing（DID; ダイヤルイン方式）
- 発信番号
- 着信番号
- 接続名
- 転送（参加による）
- メッセージ待機表示（MWI）
- 宛先変更（転送切り替えによる）
- 発信者名の制限
- 発信番号の制限
- 宛先変更（再ルーティングによる）
- 宛先変更（「チェック制限」要求への応答）
- アラート名（呼び出し時）
- パス交換
- コールバック：Call Completion Busy Subscriber（CCBS）および Call Completion No Reply（CCNR）

Cisco Unified CallManager によって QSIG がサポートされるため、加入者間の機能透過性を保持しながら、Cisco Unified CallManager を大規模な企業ネットワークに導入できます。いつでも都合のよいときに、PBX ロケーションを IP テレフォニーに変換できます。

ただし、PBX でまだ QSIG を有効にしていない場合、または QSIG の追加機能が特に必要でない場合は、短期間で PBX を撤廃すると、PBX のアップグレードのコストが正当化されにくくなることがあります。たとえば、2、3 か月で PBX を撤廃することを計画している場合に、PBX で QSIG を有効にするために 30,000 ドルを費やす理由はありません。

要約

どちらの移行方法も正常に機能するので、どちらの方法が正しいということはありませんが、ほとんどの場合はパラレル カットオーバー方法の方がうまくいきます。さらに、大規模な企業では、QSIG を使用して Cisco Unified CallManager を企業ネットワークに導入することにより、どちらの移行方法も改良できます。

シスコには、Cisco Unified CallManager システムと PBX システム間の相互運用性をテストするための専用の実験設備があります。テスト結果はアプリケーション ノートとして入手できます。アプリケーション ノートは次の Web サイトで公開されています。

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

アプリケーション ノートは頻繁に更新され、新しい資料は常にこの Web サイトに追加されています。最新情報を入手するには、この Web サイトを頻繁に確認してください。

要約

CHAPTER 18

音声セキュリティ

この章では、IP テレフォニー ネットワークを保護するためのガイドラインと推奨事項について説明します。この章のガイドラインに従うことは、安全な環境を保証するものではなく、ネットワーク上のすべての侵入攻撃を防止するものではありません。適切なセキュリティを達成するには、適切なセキュリティ ポリシーを確立し、そのセキュリティ ポリシーを適用する必要があります。また、ハッカーおよびセキュリティ コミュニティでの最新の動向を常に把握し、信頼性の高いシステム管理プラクティスによりすべてのシステムを保守および監視する必要があります。

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

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

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

セキュリティの概要

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

セキュリティ ポリシー

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

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

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

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

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

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

要約すると、セキュリティ ポリシーを定義するには、次のプロセスに従います。

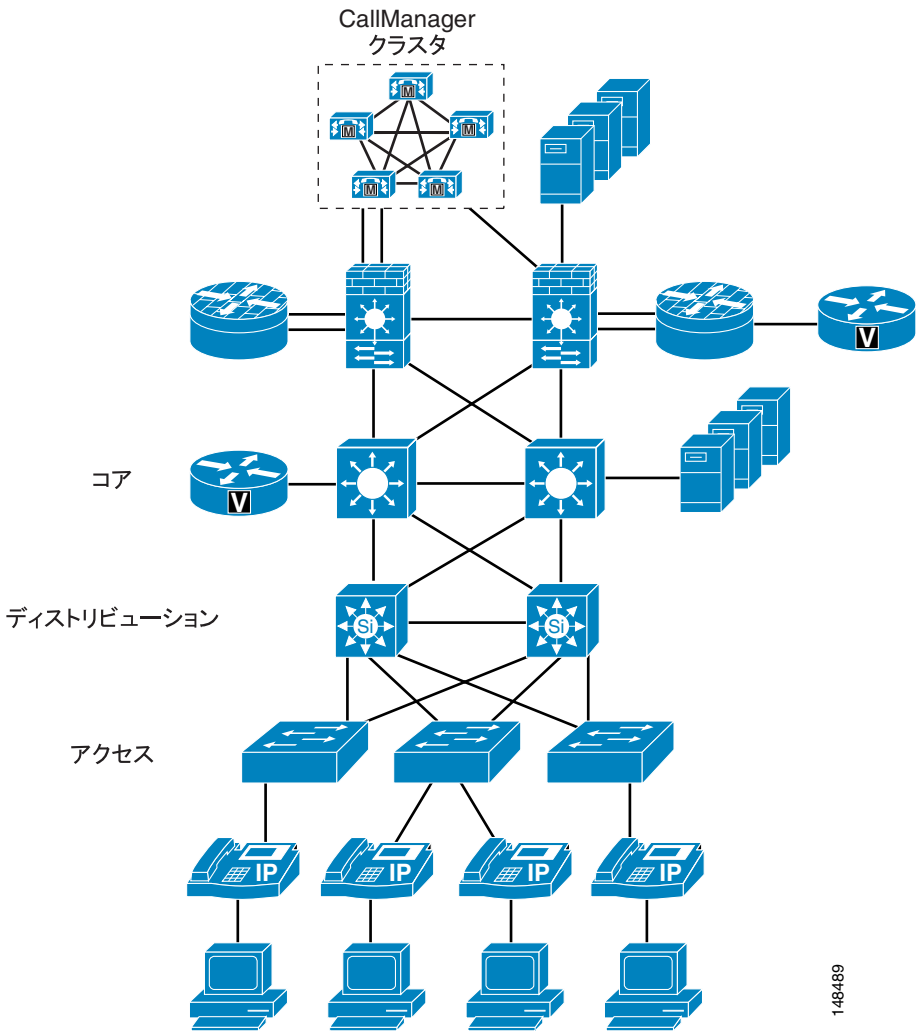
- ネットワーク上のデータを定義する。
- データの重要性を定義する。
- データの重要性に基づいてセキュリティを適用する。

レイヤ化したセキュリティ

この章では、最初にユーザが PC に接続できる電話機ポートについて説明します。また、電話機がネットワークを介して、アクセス スイッチ、ディストリビューション レイヤ、コア レイヤ、最後にデータ センターに到達する方法について説明します（図 18-1 を参照）。アクセス ポートからネットワーク自体に至るまで、セキュリティ レイヤの上にレイヤを構築します。各機能について説明するにあたり、社内セキュリティ ポリシーの観点から考慮する必要がある、それぞれの利点と欠点について説明します。

たとえば、図 18-1 は、IP テレフォニー ネットワークを使用することの利点と欠点の両方を示しています。音声製品は IP を使用してすべてのデバイスに接続するため、ネットワーク内の任意の場所に配置できます。この特性を使用すると、ネットワークの設計者は、IP テレフォニー アプリケーションを配置する上で物理的にも論理的にも簡単な場所に、デバイスを配置できます。しかし、簡単に配置できるということは、セキュリティがより複雑になることを意味します。接続性があるところであればネットワーク内のどこにでも、IP テレフォニー デバイスを配置できるからです。

図 18-1　セキュリティ レイヤ



インフラストラクチャの保護

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

ネットワーク全体のセキュリティを向上させるためにデータ ネットワークで実行できる、多くのベストプラクティスがあります。たとえば、攻撃者がパスワードをクリア テキスト形式で見ることができないように、Telnet（パスワードをクリア テキスト形式で送信します）を使用して任意のネットワーク デバイスに接続する代わりに、Secure Shell（SSH、Telnet の安全な形式）を使用できます。Cisco.com Web サイトでは、ネットワーク内のセキュリティ全般に関する多数のマニュアルを入手できます。導入済みのセキュリティ ポリシーと共にこれらのマニュアルを使用し、インフラストラクチャで必要なセキュリティを判別してください。

ビデオ インフラストラクチャ

ゲートキーパー機能を提供する Cisco IOS 機能セット（IP/H323 機能セットと EnterprisePlus/H323 MCU 機能セット）は Telnet だけをサポートし、Secure Shell（SSH）はサポートしません。Telnet ではユーザ名とパスワードがクリア テキスト形式で送信されるため、Access Control List（ACL; アクセス コントロール リスト）を使用して、Telnet によるルータへの接続をだれに許可するかを制御することをお勧めします。また、ゲートキーパーには、安全なネットワーク セグメントにあるホストから常に接続するように努めてください。

Cisco Unified Videoconferencing 3500 シリーズ MCU および H.320 ゲートウェイは Telnet、FTP、HTTP、および SNMP をサポートします。これらの IP/VC デバイスは TACACS または RADIUS の認証をサポートしません。限定数の管理アカウントのみをデバイスにローカルで設定できます。ユーザ名とパスワードは Telnet、FTP、HTTP、SNMP のすべての通信でクリア テキスト形式で送信されます。これらのデバイスには、安全なネットワーク セグメントにあるホストからアクセスすることをお勧めします。これらのデバイスを不正アクセスから保護するにはファイアウォール、アクセス コントロール リスト、Cisco Authentication Proxy、およびその他の Cisco セキュリティ ツールも使用する必要があります。

次のリンクは、Cisco.com で入手可能なセキュリティ関連マニュアルをリストしています。

- Best Practices for Cisco Switches（ログイン認証が必要）

  http://cisco.com/en/US/partner/products/hw/switches/ps663/products_tech_note09186a0080094713.shtml
- SAFE：A Security Blueprint for Enterprise Networks

  http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008009c8b6.shtml

物理的なセキュリティ

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

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

- http://www.cisco.com/go/safe/
- http://www.cisco.com/web/about/ac123/iqmagazine/archives/q2_2005/addressing_network_security.html

IP アドレッシング

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

このマニュアルの他の項で説明されているとおり（P.3-4 の「キャンパス アクセス レイヤ」を参照）、RFC 1918 に基づいた IP アドレッシングを使用する必要があります。このアドレッシング方式では、ネットワークの IP アドレッシングをやり直すことなく、IP テレフォニー システムをネットワークに配置できます。音声エンドポイントの IP アドレスは適切に定義されていて理解しやすいので、RFC 1918 を使用すると、ネットワーク内の制御をより適切に実行できます。すべての音声エンドポイントが 10.x.x.x. のネットワーク内でアドレッシングされていると、アクセス コントロール リスト（ACL）、およびこれらのデバイスが受信または送信するデータのトラックは単純になります。

利点

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

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

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

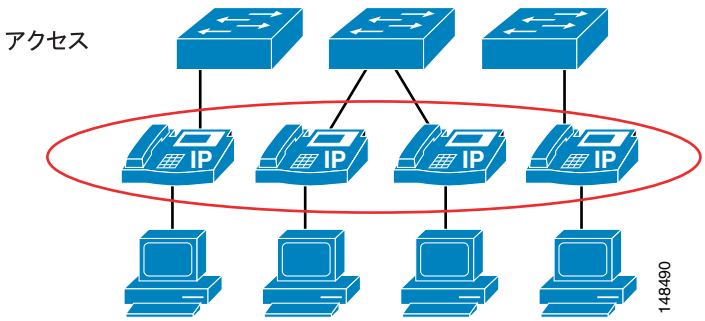
欠点

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

電話機のセキュリティ

Cisco Unified IP Phone には、IP テレフォニー ネットワーク上のセキュリティを強化するための組み込み型の機能があります。これらの機能を電話機単位で有効または無効にして、IP テレフォニー配置のセキュリティを強化できます。セキュリティ ポリシーは、電話機の配置に応じて、これらの機能を有効にする必要があるかどうか、および有効にする必要がある場所を判別するのに役立ちます（図 18-2 を参照）。

図 18-2　電話機レベルでのセキュリティ



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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/secuphne.htm

電話機の PC ポート

電話機には、通常、PC を接続するための電話機の背面のポートを、オンまたはオフにする機能があります。この機能は、そのタイプの制御が必要な場合に、ネットワークにアクセスするためのコントロール ポイントとして使用できます。

セキュリティ ポリシーおよび電話機の配置状況によっては、特定の電話機の背面にある PC ポートを無効にする必要があります。このポートを無効にすると、電話機の背面にデバイスを接続したり、電話機自体を介してネットワークにアクセスしたりできなくなります。ロビーのような一般的なエリアに設置した電話機の場合、通常はポートを無効にします。ロビーでは物理的なセキュリティが非常に弱いため、ほとんどの企業では、制御されていないポートから不特定のユーザがネットワークにアクセスするのを許可しません。セキュリティ ポリシーで、電話機の PC ポートを経由してデバイスがネットワークにアクセスするのを許可しない場合は、通常の作業エリアに設置した電話機でも、ポートを無効にすることがあります。配置された電話機のモデルによっては、Cisco Unified CallManager は、電話機の背面の PC ポートを無効にできます。この機能の有効化を試みる前に、次のリンクで入手可能なマニュアルを参照して、特定の Cisco Unified IP Phone モデルでこの機能がサポートされていることを確認してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

利点

電話機の PC ポートを無効にすると、電話機からネットワークへのアクセスを禁止する必要があるエリアに電話機を配置できます。これにより、電話機の背面の PC ポートが有効であればアクセス可能だったはずのネットワークへのアクセスが制御されます。

欠点

電話機の PC ポートが無効な場合、ネットワーク アクセスを必要としているユーザで、アクセスのための承認を得ているユーザごとに、ネットワーク アクセスを提供する個別のイーサネット ポートを追加する必要があります。ユーザは、イーサネット ジャックを電話機から切断し、別のデバイスに接続することを試行できます。

Cisco Unified Video Advantage が正しく動作するには、PC ポートとビデオ機能の両方を有効にする必要があります。その他の設定は無効にしてもかまいません。

Gratuitous ARP

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

Gratuitous ARP は、攻撃者がネットワークの音声セグメントにアクセスできた場合に、攻撃者が電話機からのシグナリングや RTP 音声ストリームを取り込むことから電話機を保護するのに役立ちます。この機能で保護されるのは電話機だけです。インフラストラクチャの残りの部分は、Gratuitous ARP 攻撃から保護されません。スイッチ ポートには電話機とネットワーク デバイスの両方を保護する機能があるので、Cisco インフラストラクチャを実行している場合、この機能はそれほど重要ではありません。これらのスイッチ ポートの機能の説明については、P.18-14 の「スイッチ ポート」を参照してください。

利点

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

欠点

別の電話機から発信されたかネットワークを経由して到達するダウンストリーム シグナリングおよび RTP 音声ストリームは、電話機のこの機能では保護されません。保護されるのは、この機能が有効になっている電話機からのデータのみです（図 18-3 を参照）。

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

図 18-3　Gratuitous ARP は導入先の電話機は保護するが他のトラフィックは保護しない

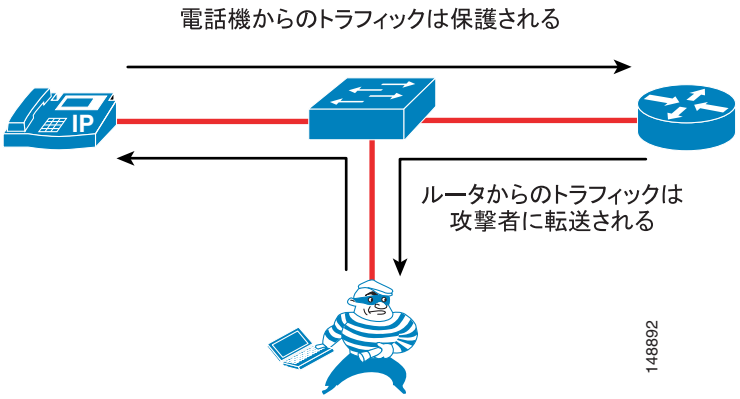


図 18-3 が示しているとおり、Gratuitous ARP 機能を持つ電話機からのトラフィックは保護されますが、エンドポイントに、データ フローを保護する機能がない可能性があるので、攻撃者が別のエンドポイントからのトラフィックを見ることができる場合があります。

PC Voice VLAN へのアクセス

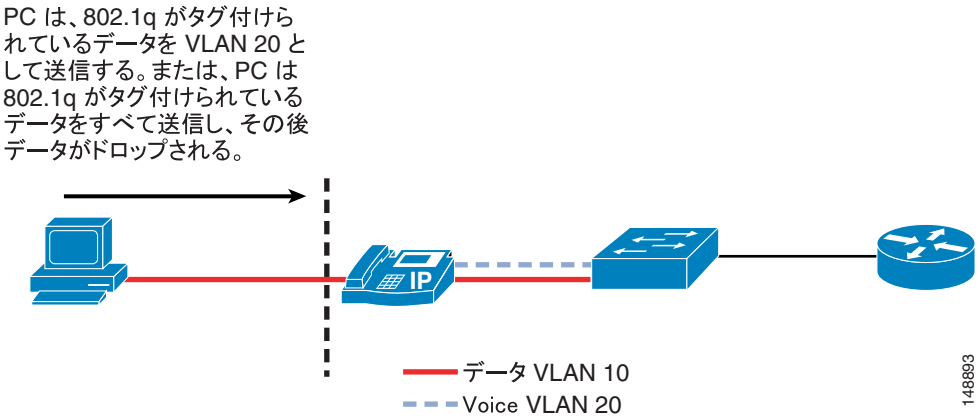
スイッチから電話機までに 2 つの VLAN が存在するので、電話機は、望まないアクセスから Voice VLAN を保護する必要があります。電話機では、電話機の背面から Voice VLAN に入り込む、望まないアクセスを防止できます。PC Voice VLAN Access 機能は、電話機の背面にある PC ポートから Voice VLAN への任意のアクセスを防止します。この機能を無効にすると、電話機の PC ポートに接続されたデバイスが、電話機の背面の PC ポートに到達する Voice VLAN を宛先とした 802.1q タグ付き情報を送信することにより、VLAN を「ジャンプ」して Voice VLAN にアクセスすることは許可されません。設定している電話機に応じて、この機能は 2 つの方法のいずれかで動作します。高機能の電話機では、電話機の背面の PC ポートに着信する Voice VLAN を宛先とした、すべてのトラフィックをブロックします。図 18-4 に示す例の場合、PC が、電話機の PC ポートに対して Voice VLAN トラフィック（このケースでは 200 の 802.1q タグ付き）の送信を試行すると、そのトラフィックはブロックされます。この機能が動作する他の方法は、電話機の PC ポートに着信する、802.1q タグ付きのすべてのトラフィック（Voice VLAN トラフィックに限らない）をブロックする方法です。

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

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

図 18-4　電話機の PC ポートから Voice VLAN へのトラフィックのブロック



利点

PC Voice VLAN Access 機能は、攻撃者が、電話機の背面にある PC ポートを経由して、制御されていないデータを Voice VLAN に送信することを防止します。

欠点

電話機に接続されているデバイスが 802.1q タグ付きパケットを送信することが、通常は許可されている場合、これらのパケットはドロップされます。ほとんどのエンド ステーションでは、アクセス レイヤでこの機能を実行することが許可されていません。この機能がネットワーク内で通常の動作と見なされる場合、この機能が動作することは許可されません。

Web アクセス

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

利点

電話機の Web アクセスを有効にすると、電話機やネットワークの問題をデバッグするときにその電話機を使用できます。電話機からの Web アクセスを無効にすると、ユーザまたは攻撃者は、IP テレフォニー ネットワークに関する情報をその電話機から入手できません。

欠点

電話機からの Web アクセスを無効にすると、ネットワークや IP テレフォニーの問題をデバッグするのがより困難になります。Web サーバがグローバルで無効だが、デバッグの参考として必要な場合、Cisco Unified CallManager の管理者は、電話機のこの機能を有効にする必要があります。この Web ページにアクセスする機能は、ネットワークの ACL で制御できます。ネットワーク オペレータは、この機能を使用して、必要なときに Web ページにアクセスできます。

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

ビデオ機能

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

利点

Cisco Unified Video Advantage が正しく機能するには、PC ポートとビデオ機能が必要です。

欠点

これらの機能を有効にすると、電話機の保護に ACL を使用していない場合に、PC から電話機への通信が許可される可能性があります。

アクセス設定

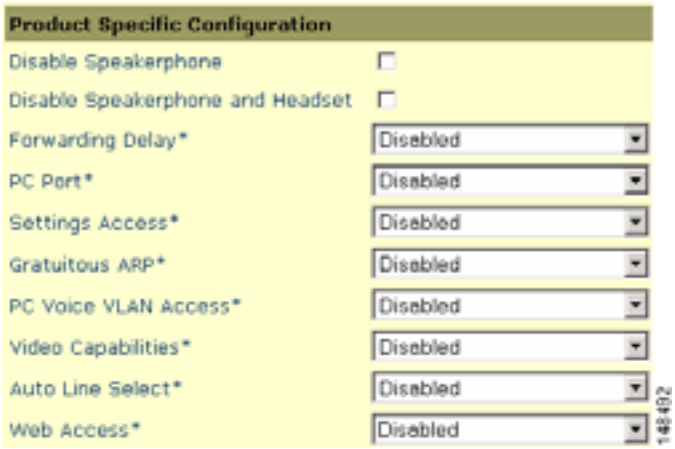
各 Cisco Unified IP Phone にはネットワーク設定ページがあり、そのページには、電話機が動作するのに必要な多くのネットワーク要素や詳細情報がリストされます。攻撃者はこの情報を使用して、電話機の Web ページに表示される情報の一部と共に、ネットワーク上で調査を開始できます。たとえば、攻撃者は設定ページを参照して、デフォルト ゲートウェイ、TFTP サーバ、および Cisco Unified CallManager の IP アドレスを判別できます。これらの断片的な情報が、音声ネットワークにアクセスしたり、音声ネットワーク内のデバイスを攻撃したりするのに使用される場合がありま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

このアクセスを電話機ごとに無効にすることにより（図 18-5 を参照）、エンド ユーザまたは攻撃者が、Cisco Unified CallManager IP アドレスや TFTP サーバ情報などの追加情報を取得するのを防止できます。

電話機設定ページの詳細については、次の Web サイトで入手可能な『*Cisco Unified IP Phone Authentication and Encryption for Cisco Unified CallManager*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/ae/index.htm

図 18-5　Cisco Unified CallManager の Phone Configuration ページ



利点

電話機設定ページへのアクセスを無効にすると、エンド ユーザおよび攻撃を仕掛けようとしている人が、ネットワークに関する詳細情報や音声システムで使用される IP テレフォニー情報を見ることはできません。この機能を無効にしたときに保護される情報には、電話機の IP アドレス、電話機の登録先の Cisco Unified CallManager などの情報が含まれます。

欠点

電話機設定ページへのアクセスを無効にすると、エンド ユーザは、スピーカー ボリューム、連絡先、呼び出しタイプなど、通常は制御可能な多くの電話機設定を変更できなくなります。電話機インターフェイスについてエンド ユーザに課される制限により、このセキュリティ機能を使用することが現実的ではない場合があります。ただし、管理者が電話機設定ページへのアクセスを無効にするのではなく制限する場合は、アクセス不可にはなりません。

電話機の認証および暗号化

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

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

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

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/sec_vir/ae/sec413/

利点

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

- 完全性：この機能が有効な場合は、電話機に対する TFTP ファイル操作を許可しませんが、トランスポート レイヤ セキュリティ（TLS）シグナリングを許可します。

- 認証：電話機のイメージは、Cisco Unified CallManager から電話機に対して認証され、デバイス（電話機）は Cisco Unified CallManager に対して認証されます。電話機と Cisco Unified CallManager の間のすべてのシグナリング メッセージは、認可されているデバイスから送信されるときに検証されます。
- 暗号化：サポートされているデバイスで、盗聴を防止するためシグナリングとメディアを暗号化できます。
- Secure Real-time Transport Protocol（SRTP）：Cisco IOS MGCP ゲートウェイでサポートされています。当然、電話機間でもサポートされています。Cisco Unity もボイスメールのための SRTP をサポートしています。

欠点

Cisco Unified CallManager は、メディア サービスが使用されていない単一クラスタにおける、2 つの Cisco Unified IP Phone の間のコールの、認証、完全性、および暗号化をサポートしています。ただし、すべてのデバイスまたは電話機の認証、完全性、または暗号化を提供しているわけではありません。ご使用のデバイスがこれらの機能をサポートしているかどうかを判別するには、次の Web サイトで入手可能なマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/

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

アクセス セキュリティ

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

Voice VLAN と Video VLAN

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

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

Sony 社製および Tandberg 社製の SCCP エンドポイントは、Cisco Discovery Protocol（CDP）または 802.1Q VLAN ID タギングをサポートしません。したがって、標準的な環境では、音声 VLAN をネイティブ VLAN として使用するようにポートを手動で設定してある場合を除き、これらのデバイスはデータ VLAN に存在します。Sony 社製および Tandberg 社製のエンドポイントは、設定のダウンロードのために TFTP サーバと通信し、SCCP シグナリングのために Cisco Unified CallManager と通信し、RTP オーディオ / ビデオ メディア チャネルのために他のエンドポイントと通信します。したがって、データ VLAN と TFTP サーバの間で TFTP プロトコルを許可し、データ VLAN と Cisco Unified CallManager サーバの間で TCP ポート 2000 を許可し、データ VLAN と音声 VLAN の間で RTP メディア用の UDP ポートを許可する必要があります。

H.323 クライアント、Multipoint Control Unit（MCU; マルチポイント コントロール ユニット）、およびゲートウェイは、H.323 プロトコルを使用して Cisco Unified CallManager と通信します。Cisco Unified CallManager H.323 トランク（H.225 やインタークラスタ トランクのほかに、RAS アグリゲーター トランク タイプなど）は、ウェルノウン TCP ポート 1720 ではなくランダムなポート範囲を使用します。したがって、これらのデバイスと Cisco Unified CallManager サーバの間で広範囲の TCP ポートを許可する必要があります。MCU とゲートウェイはインフラストラクチャ デバイスと見なされ、通常は Cisco Unified CallManager サーバに隣接するデータ センターに存在します。一方、H.323 クライアントは通常はデータ VLAN に存在します。

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

利点

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

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

欠点

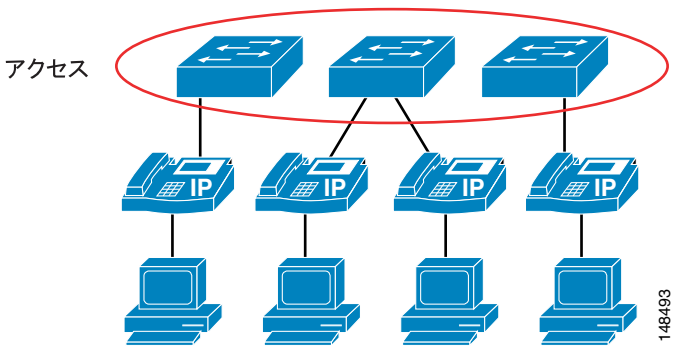
通常は電話機に送られる CDP メッセージから情報が収集され、その情報が一部のネットワークを検出するために使用される可能性があります。Cisco Callmanager で音声またはビデオ用に使用可能なすべてのデバイスが、音声 VLAN の検出に CDP を使用できるわけではありません。

スイッチ ポート

Cisco スイッチ インフラストラクチャには、データ ネットワークを保護するために使用できる多くのセキュリティ機能があります。この項では、ネットワーク内の IP テレフォニー データを保護するため、Cisco Access Switch で使用できるいくつかの機能について説明します（図 18-6 を参照）。この項では、現在のすべての Cisco スイッチで使用可能なすべてのセキュリティ機能について説明するのではなく、シスコが製造する多くのスイッチで使用されている一般的なセキュリティ機能をリストします。ネットワーク内に配置された特定の Cisco デバイスで使用可能なセキュリティ機能の追加情報については、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com

図 18-6　電話機が接続される代表的なアクセス レイヤ設計



ポートセキュリティ：MAC CAM フラッディング

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

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

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

ポート セキュリティ：ポート アクセスの防止

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

この期間は、固定タイマーまたは非活動タイマー（非持続アクセス）のいずれかで決定するか、永続的に割り当てることができます。永続的に MAC アドレスを割り当てる機能は、Cisco 6000 スイッチでは*自動設定*と呼ばれ、Cisco Catalyst 4500、2550、2750、または 2950 スイッチでは*スティッキ*と呼ばれます。どちらの場合も、スイッチのリロードまたはリブートが発生しても、取得された MAC アドレスはポートで保持されます。

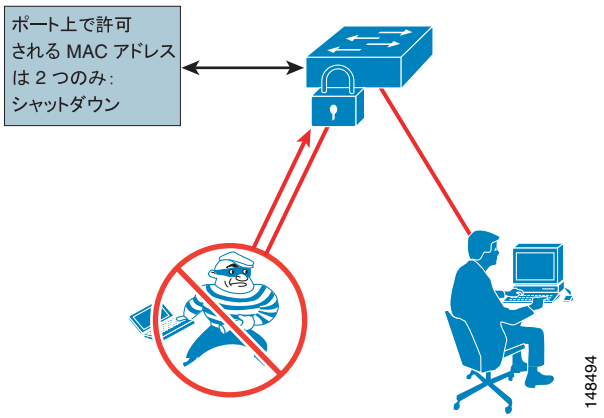
自動設定またはスティッキを使用した MAC アドレスの持続割り当ては、コマンドを使用してのみクリアできます。現在、Cisco Catalyst スイッチング プラットフォーム全体で最も一般的なデフォルト動作は、非持続動作です。この動作は、Cisco CatOS Release 7.6（1）が持続的になる前に、唯一有効だった動作です。デバイス モビリティに対し、静的ポート セキュリティまたは持続性のある動的ポート セキュリティによるプロビジョニングは行われません。最重要の要件ではありませんが、MAC フラッディング攻撃は、特定の MAC アドレスへのアクセスを制限することを目的としているポート セキュリティにより暗黙的に防止されます。

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

ポート セキュリティ：不良ネットワーク拡張の防止

ハブまたは無線アクセス ポイント（AP）を経由する不良なネットワーク拡張を防止します。ポート セキュリティは 1 つのポートでの MAC アドレスの数を制限するので、ポート セキュリティを、IT で作成されたネットワークへのユーザ拡張を抑制するためのメカニズムとして使用することもできます。たとえば、ユーザ方向のポート、または単一の MAC アドレス用にポート セキュリティが定義された電話機のデータ ポートに、ユーザが無線 AP を接続した場合、無線 AP 自体がその MAC アドレスを占有し、背後にあるデバイスはネットワークにアクセスできません。（図 18-7 を参照）。一般的に、MAC フラッディングを停止するのに適切な設定は、不良アクセスを抑制するためにも適切です。

図 18-7　MAC アドレス数の制限による不良ネットワーク拡張の防止



利点

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

欠点

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

設定例

（注） この設定例は、これらの機能をサポートするために適切なコード レベルを実行しているスイッチに基づいています。電話機へのトランク モードは実行されません。

次の例は、データ ポートにデバイスが接続されている電話機に対して、ダイナミック ポート セキュリティを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

```
switchport access vlan 10
switchport mode access
switchport voice vlan 20
switchport port-security
switchport port-security maximum 2
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
```

上記の例のコマンドは、次の機能を実行します。

- **switchport port-security** *x/x* **enable**

  このコマンドは、指定したモジュール / ポートでポート セキュリティを有効にします。

- **switchport port-security violation restrict**

  このコマンドが、推奨されている設定です。デフォルトでは、ポートを無効にします。ポートを **restrict** すると、ポートは、MAC アドレスの最大数に達するまで MAC アドレスを取得し、その後は新しい MAC アドレスの取得を停止します。ポートの設定がデフォルトの **disable** の場合、MAC アドレスの最大数に達すると、ポートはエラーを無効化し、電話機の電源を切ります。ポートを再有効化するデフォルト タイマーは、5 分です。導入済みのセキュリティ ポリシーによっては、ポートを無効にすることにより電話機をシャットダウンせずに、ポートを制限した方が適切な場合があります。

- **switchport port-security aging time 2**

  このコマンドは、MAC アドレスからのトラフィックがない状態で、その MAC アドレスをポートで保持する時間を設定します。一部のスイッチと電話機の間の CDP 通信を考慮に入れると、推奨されている最小時間は 2 分です。

- **switchport port-security aging type inactivity**

  このコマンドは、取得した MAC アドレスをタイムアウトするために、ポートで使用されるエージングのタイプを定義します。

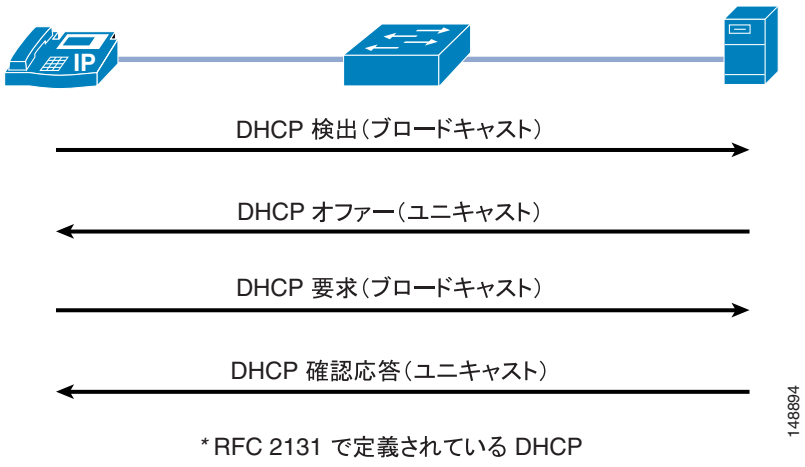
DHCP スヌーピング：不正な DHCP サーバ攻撃の防止

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

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

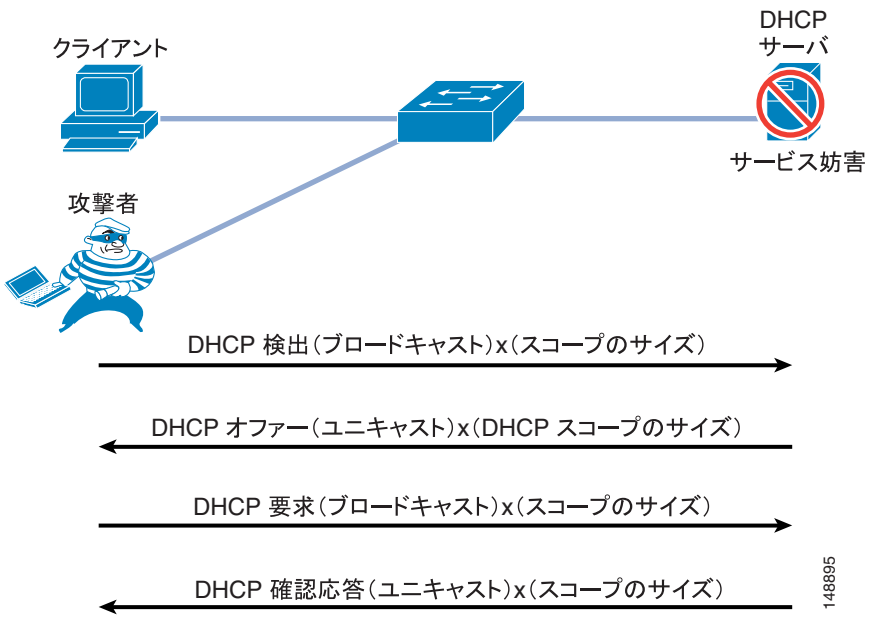
図 18-8 は、DHCP サーバに IP アドレスを要求するネットワーク接続デバイスの通常の操作を示しています。

図 18-8　DHCP 要求の通常の操作



ただし、攻撃者は、単一の IP アドレスではなく、VLAN 内で使用可能なすべての IP アドレスを要求できます（図 18-9 を参照）。これは、ネットワークへのアクセスを試みている正当なデバイスのための IP アドレスが存在しないことを意味します。IP アドレスがないと、電話機は Cisco Unified CallManager に接続できません。

図 18-9　攻撃者は VLAN で使用可能なすべての IP アドレスを取得できる



利点

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

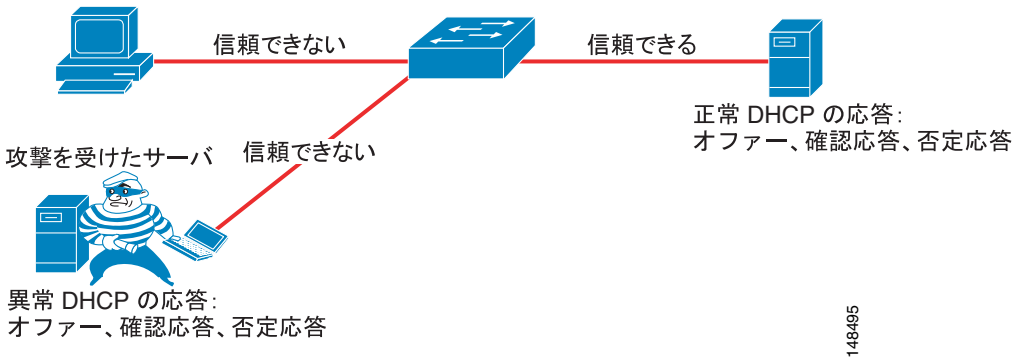
欠点

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

DHCP スヌーピング：DHCP スターベーション攻撃の防止

Gobbler などのツールを使用した DHCP アドレス スコープ スターベーション攻撃は、DHCP DoS 攻撃（サービス拒絶攻撃）を仕掛けるために使用されます。Gobbler ツールは、ランダムに生成される異なる送信元 MAC アドレスから DHCP 要求を実行するので、ポート セキュリティを使用して MAC アドレスの数を制限することにより、Gobbler ツールが DHCP アドレス スペースをスタービングするのを防止できます（図 18-10 を参照）。ただし、高度な DHCP スターベーション ツールでは、1 つの送信元 MAC アドレスから DHCP 要求を実行でき、DHCP ペイロード情報も多様です。DHCP スヌーピングを有効にすると、信頼されていないポートで、送信元 MAC アドレスと DHCP ペイロード情報が比較され、それらが一致しない場合は要求が失敗します。

図 18-10　DHCP スヌーピングを使用した DHCP スターベーション攻撃の防止



利点

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

欠点

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

設定例

次の例は、データ ポートにデバイスが接続されている電話機に対して、DHCP スヌーピングを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10, 20
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド

```
no ip dhcp snooping trust (Default)
ip dhcp snooping limit rate 10 (pps)
ip dhcp snooping trust
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip dhcp snooping vlan 10, 20**
  このコマンドは、DHCP スヌーピングが有効になっている VLAN を特定します。

- **No ip dhcp snooping information option**

  DHCP アドレスをリースするのに Option 82 情報が要求されないようにするため、このコマンドを使用する必要があります。Option 82 情報は DHCP サーバでサポートされている必要がありますが、ほとんどの企業サーバは、この機能をサポートしていません。Option 82 は Cisco IOS DHCP サーバでサポートされています。

- **ip dhcp snooping**

  このコマンドは、スイッチで、グローバル レベルでの DHCP スヌーピングを有効にします。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip dhcp snooping trust**

  このコマンドは、DHCP サーバからポートに着信する情報をすべて信頼しないようにインターフェイスを設定します。

- **ip dhcp snooping limit rate 10**

  このコマンドは、DHCP スヌーピングが最初に設定されるときにインターフェイスで設定される、デフォルトのレート制限を設定します。この値は、導入済みのセキュリティ ポリシーに合せて変更できます。

- **ip dhcp snooping trust**

  このコマンドは、DHCP サーバから DHCP 情報を送信するときに経由するポートに対して実行します。DHCP 情報の送信元のポートを信頼できない場合、いずれのデバイスも DHCP アドレスを受信しません。この情報がクライアントに到達するようにするには、DHCP サーバが接続されている最低 1 つのポート（アクセス ポートまたはトランク ポート）を設定する必要があります。このコマンドは、固定 IP アドレスが与えられていて、IP アドレスを取得するために DHCP を使用しないポートに接続されている、任意のデバイスを信頼するためにも使用できます。DHCP サーバへのアップリンク ポート、または DHCP サーバへのトランク ポートも信頼する必要があります。

DHCP スヌーピング：バインディング情報

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

次の例は、DHCP スヌーピングからのバインディング情報を示しています。

- Cisco IOS のバインディング情報の表示：

```
show ip dhcp snooping binding
MacAddress          IpAddress     Lease(sec)    Type            VLAN Interface
----------          ---------     ----------    -------------   ---- ---------
00:03:47:B5:9F:AD   10.120.4.10       193185    dhcp-snooping   10
FastEthernet3/18
```

- Cisco CatOS のバインディング情報の表示：

```
ngcs-6500-1> (enable) show dhcp-snooping bindings
MacAddress          IpAddress       Lease(sec)      VLAN      Port
------------------  --------------- ----------      ----      -----
00-10-a4-92-bf-dd   10.10.10.21          41303      10        2/5
```

DHCP スヌーピングのために各タイプのスイッチに格納できるバインディング テーブル エントリには、最大制限があります（この制限を判別するには、使用するスイッチの製品マニュアルを参照してください）。スイッチのバインディング テーブル内のエントリ数が気になる場合は、バインディング テーブルのエントリがより早くタイムアウトになるように、DHCP 範囲のリース時間を短縮できます。リースが期限切れになるまで、これらのエントリは DHCP バインディング テーブルに残されます。言い換えると、エンド ステーションがそのアドレスを持っていると DHCP サーバが判断する限り、これらのエントリは DHCP スヌーピング バインディング テーブルに残されます。ワークステーションまたは電話機を切断しても、これらのエントリはポートから除去されません。

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

Dynamic ARP Inspection の要件

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

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

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

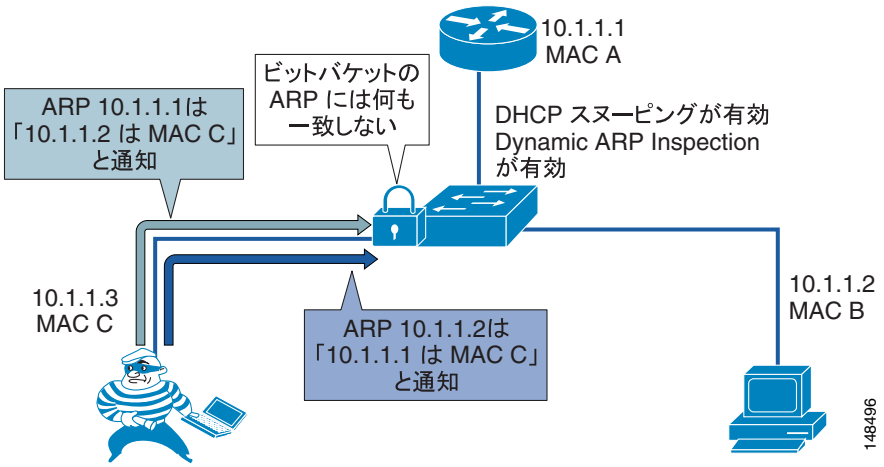
ただし、Gratuitous ARP は、別のステーションの身分を不正にかたること目的とした悪質なプログラムにより悪用される可能性もあります。悪質なステーションが、相互に通信しているその他の 2 つのステーションのトラフィックを自らにリダイレクトすると、GARP メッセージを送信したハッカーが中間者になります。ettercap などのハッカー プログラムは、このことを精密に行うため、GARP メッセージをブロードキャストするのではなく、「プライベートな」GARP メッセージを特定の MAC アドレスに発行します。これにより、攻撃の犠牲者は、自分のアドレスに対する GARP パケットを見ることが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

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

DAI の使用

Dynamic ARP Inspection（DAI）では、ARP 応答または Gratuitous ARP メッセージを正当化するために、DHCP バインディングが存在している必要があります。ホストで、アドレスを取得するための DHCP が使用されていない場合、そのホストを信頼するか、ホストの IP アドレスと MAC アドレスを対応付けるために ARP 検査用のアクセス コントロール リスト（ACL）を作成する必要があります（図 18-11 を参照）。DHCP スヌーピングと同様、DAI は VLAN ごとに有効化されます。すべてのポートは、デフォルトで、信頼できないポートとして定義されます。DAI で DHCP スヌーピングからのバインディング情報を活用するには、DAI を有効化する前に、VLAN で DHCP スヌーピングを有効化する必要があります。DAI を有効化する前に DHCP スヌーピングを有効化しないと、VLAN 内のいずれのデバイスも、ARP を使用して、デフォルト ゲートウェイを含む VLAN 内の他のデバイスに接続できません。その結果、VLAN 内のすべてにデバイスに対するサービスを、自ら拒否することになります。

図 18-11　DHCP スヌーピングおよび DAI を使用した ARP 攻撃の防止



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

利点

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

欠点

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

設定例

次の例は、DHCP スヌーピングおよび Dynamic ARP Inspection を使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- グローバル コマンド

```
ip dhcp snooping vlan 10,20 (required)
no ip dhcp snooping information option (required without option 82 dhcp server)
ip dhcp snooping (required)
ip arp inspection vlan 10,20
ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb
```

- インターフェイス コマンド

```
ip dhcp snooping trust
ip arp inspection trust
no ip arp inspection trust (default)
ip arp inspection limit rate 15 (pps)
```

上記の例のグローバル コマンドは、次の機能を実行します。

- **ip arp inspection vlan 10,20**

  このコマンドは、Dynamic ARP Inspection（DAI）が有効になっている VLAN を特定します。

- **ip arp inspection trust**

  ip dhcp snooping trust と同様、このコマンドは、ルータなどの信頼済みデバイスが ARP メッセージに応答するのを許可します。このコマンドは、使用するルータ用のポートで設定する必要があります。そのように設定しないと、ルータは DHCP スヌーピング バインディング テーブルに含まれないので、ルータはいずれの ARP 要求にも応答できません。

- **no ip arp inspection trust**

  この設定は、VLAN 上のすべてのポートのデフォルト設定です。信頼を有効にする必要があります。

- **ip arp inspection limit rate 15 (pps)**

  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数のグローバル デフォルト値を設定します。この値を超えると、インターフェイスは無効になります。この動作が問題になる場合は、制限を増加または減少させるか、**none** に設定することができます。

- **ip dhcp snooping database tftp://172.26.168.10/tftpboot/cisco/ngcs-dhcpdb**

  このコマンドは、DHCP スヌーピング バインディング テーブルのバックアップを TFTP サーバに作成します。DHCP スヌーピング バインディング テーブルは、ブートフラッシュ、FTP、RCP、スロット 0、および TFTP にバックアップできます。

上記の例のインターフェイス コマンドは、次の機能を実行します。

- **no ip arp inspection trust**

  このコマンドは、ポート上で DAI を有効にし、DHCP スヌーピング バインディング テーブルを基にすべての ARP をチェックします。

- **ip arp inspection limit rate 15 (pps)**

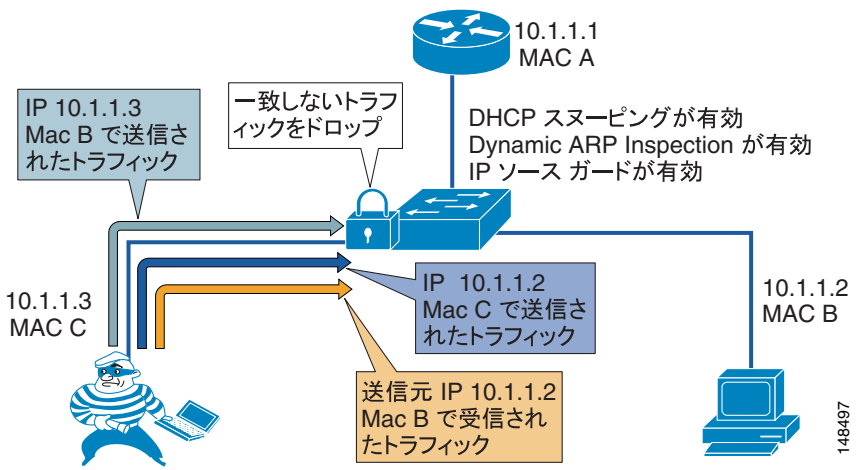
  このコマンドは、インターフェイス上の ARP メッセージで許可されている、1 秒当たりのパケット数の最大数を指定します。インターフェイスが、指定された数を超える ARP メッセージを 1 秒間に受信する場合、ポートは無効化されます。導入済みのセキュリティ ポリシーによっては、デフォルト値（15 pps）が最適な設定の場合があります。1 秒間に 15 個を超える ARP メッセージをポートが受信するときに電話機を無効化しない場合は、レート制限を **none** に設定できます。この設定では、電話機は有効なままです。

IP ソース ガード

ARP スプーフィングに加えて、攻撃者は IP アドレス スプーフィングも仕掛ける場合があります。この方法は、第二の当事者に対して DoS 攻撃を行うときに一般的に使用されます。この方法では第三の当事者を介してパケットが送信されるため、攻撃システムの ID がマスクされます。単純な例として、攻撃者は、攻撃先の第二の当事者の IP アドレスを送信元にしながら、サードパーティ システムに ping することがあります。ping の応答は、サードパーティ システムから第二の当事者に転送されます。スプーフィングされた IP アドレスを基にしたアグレッシブ SYN フラッディングは、サーバを TCP ハーフセッションで氾濫させる別の一般的なタイプの攻撃です。

IP ソース ガード（IPSG）機能を呼び出すと、DHCP スヌーピング バインディング テーブルの内容に基づいて ACL が動的に作成されます。この ACL は、トラフィックの送信元が DHCP バインディング時に発行された IP アドレスであることを保証し、スプーフィングされた他のアドレスによりトラフィックが転送されるのを防止します。DHCP スヌーピングは IP ソース ガードの前提条件ですが、DAI は前提条件ではありません。ただし、IP アドレス スプーフィングに加えて ARP ポイズニングおよび中間者攻撃を防止するため、IP ソース ガードだけでなく DAI も有効にすることをお勧めします（図 18-12 を参照）。

図 18-12　IP ソース ガードを使用したアドレス スプーフィングの防止



IP アドレス スプーフィングを使用すると、攻撃者は、アドレスを手動で変更するか、アドレス スプーフィングを行うように設計された hping2 などのプログラムを実行することにより、有効なアドレスになりすますことができます。インターネット ワームは、送信元を偽装するためスプーフィング技法を使用する場合があります。

設定例

次の例は、IP ソース ガードを使用してアクセス ポートを設定する Cisco IOS コマンドを示しています。

- IP ソース ガードを有効にする前に有効にする必要があるコマンド

```
ip dhcp snooping vlan 4,104
no ip dhcp snooping information option
ip dhcp snooping
```

- インターフェイス コマンド：このコマンドは、DHCP Option 82 を指定せずに IP ソース ガードを有効にします。

```
ip verify source vlan dhcp-snooping
```

追加情報

ネットワーク セキュリティに関する追加情報については、次の Web サイトで入手可能な Cisco マニュアルを参照してください。

- http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper0900aecd8015f0ae.shtml
- http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml

Quality of Service

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

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

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

http://cisco.com/go/srnd

利点

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

欠点

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

アクセス コントロール リスト

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

VLAN アクセス コントロール リスト

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

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

VLAN ACL の設定については、次の製品マニュアルを参照してください。

- Cisco Catalyst 3750 スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/12225sed/scg/swacl.htm
- Cisco Catalyst 4500 シリーズ スイッチ
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/12_2_25s/conf/secure.htm
- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/swcg/acl.htm
- Cisco 6500 シリーズ スイッチ（Cisco CatOS を実行）
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/acc_list.htm

次の例は、Cisco 7960 IP Phone のトラフィックだけが VLAN でブートおよび機能するのを許可する、VLAN ACL を示しています（インライン コメントは、ACL の各行の目的を示しています）。この例の VLAN ACL は、Cisco Unified CallManager Release 4.1 で使用するポート用です。この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- デフォルト ゲートウェイは 10.0.10.2 および 10.0.10.3
- DNS サーバの IP アドレスは 10.0.40.3

（注） アプリケーションがアップデートされたとき、または OS がアップデートされたとき（またはその両方）、ポートは変更されます。この注意事項は、電話機を含む、ネットワーク内のすべての IP テレフォニー デバイスに適用されます。製品で使用されるポートの最新のリストを取得するには、ネットワーク上で実行している製品のバージョンに応じて適切なマニュアルを参照してください。ポートの使用方法についてのマニュアルは、http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/udp_tcp/index.htm で入手可能です。

```
20 permit udp host 10.0.10.2 eq 1985 any
30 permit udp host 10.0.10.3 eq 1985 any
!permit HSRP from the routers
40 permit udp any any eq bootpc
50 permit udp any any eq bootps
!permit DHCP activity
60 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0 0.0.0.255 eq tftp
70 permit udp 10.0.20.0  0.0.0.255 range 1024 5000 10.0.10.0 0.0.0.255 range 49152 65535
80 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 range 1024 5000
!permit the tftp traffic from the tftp server and phone
90 permit udp 10.0.10.0 0.0.0.255 range 49152 65535 host 10.0.40.3 eq domain
100 permit udp host 172.19.244.2 eq domain 10.0.10.0 0.0.0.255 range 49152 65535
!permit DNS to and from the phone
110 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq 2000
120 permit tcp 10.0.20.0  0.0.0.255 eq 2000 10.0.10.0 0.0.0.255 range 49152 65535
!permit signaling to and from the phone.
130 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
140 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 10.0.10.0 0.0.0.255 range 16384 32767
150 permit udp 10.0.10.0 0.0.0.255 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
!permit all phones to send udp to each other
160 permit tcp 10.0.10.0 0.0.0.255 range 49152 65535 10.0.20.0  0.0.0.255 eq www
170 permit tcp 10.0.20.0  0.0.0.255 eq www 10.0.10.0 0.0.0.255 range 49152 65535
180 permit tcp 10.0.20.0  0.0.0.255 range 49152 65535 10.0.10.0 0.0.0.255 eq www
190 permit tcp 10.0.10.0 0.0.0.255 eq www 10.0.20.0  0.0.0.255 range 49152 65535
!permit web access to and from the phone
200 permit Intelligent Contact ManagementP any any
!allow all icmp - phone to phone, gateway to phone, and NMS to phone
220 permit udp 10.0.30.0 0.0.0.255 rang 16384 327676 10.0.10.0 0.0.0.255 rang 16384 32767
!permit udp to the gateways in the network for pstn access
```

この ACL の例が示しているとおり、ネットワーク内で IP アドレスが適切に定義されているほど、ACL を書き出して配置するのが簡単になります。

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

- Cisco Catalyst 3750 スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps5023/products_configuration_guide_book09186a0080464bdc.html

- Cisco Catalyst 4500 シリーズ スイッチ

  http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_book09186a008011c8a5.html

- Cisco Catalyst 6500 シリーズ スイッチ（Cisco CatOS 対応）

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_5/confg_gd/

- Cisco Catalyst 6500 シリーズ スイッチ（Cisco IOS 対応）

  http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_book09186a00801609ea.html

利点

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

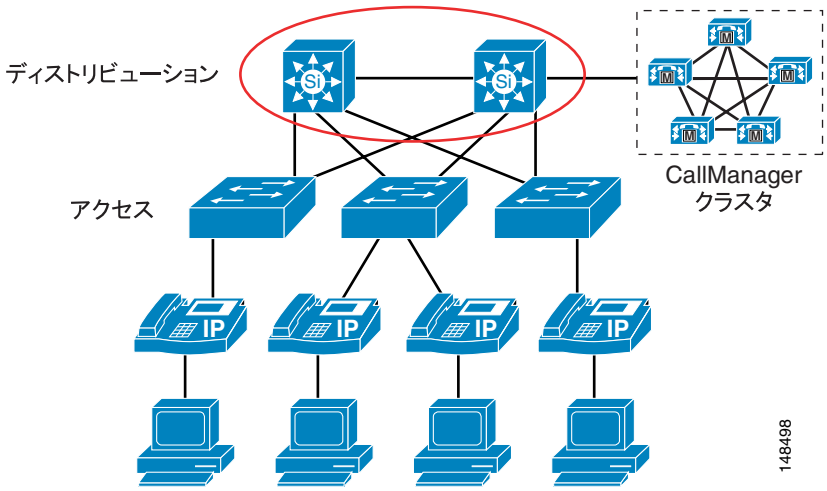
欠点

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

ルータのアクセス コントロール リスト

VLAN ACL と同様、ルータにも、ポートごとにインバウンド ACL およびアウトバウンド ACL の両方を処理する機能があります。最初のレイヤ 3 デバイスは、音声およびデータ VLAN を使用するときの音声データと別タイプのデータとの間の境界ポイントです。境界ポイントでは、2 つのタイプのデータが、相互にトラフィックを送信することが許可されます。VLAN ACL とは異なり、ルータ ACL は、ネットワーク内のすべてのアクセス デバイスには配置されません。その代わり、ネットワーク全体にルーティングするすべてのデータを準備する場所である、エッジ ルータで適用されます。これは、各 VLAN のデバイスがネットワーク内でアクセス可能なエリアを制御するために、レイヤ 3 ACL を適用するのに最適な場所です。レイヤ 3 ACL をネットワーク全体に配置することにより、トラフィックが収束する場所で、デバイスを相互に保護できます（図 18-13 を参照）。

図 18-13　レイヤ 3 のルータ ACL



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

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

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

この例では、次の IP アドレス範囲を使用します。

- 電話機の範囲は 10.0.20.*
- IP テレフォニー サーバの範囲は 10.0.10.*
- ゲートウェイの範囲は 10.0.30.*
- ネットワーク内の他のすべてのデバイスの範囲は 192.168.*.*

```
10 deny ip 192.168.0.0 0.0.255.255 10.0.10.0 0.0.0.255
!deny all non voice devices to the voip servers
20 deny 192.168.0.0 0.0.255.255 10.0.30.0 0.0.0.255
!deny all non voice devices to the voip gateways
30 deny 192.168.0.0 0.0.255.255 10.0.20.0 0.0.0.255
!deny all non voice devices to communicate with the phones ip addresses
```

利点

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

欠点

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

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

ゲートウェイおよびメディア リソース

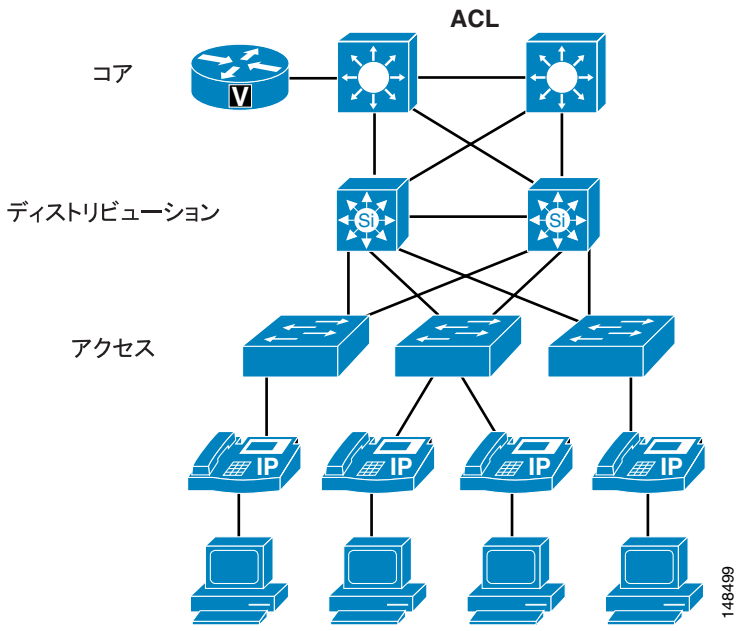
ゲートウェイおよびメディア リソースは、IP テレフォニー コールを公衆網コールに変換するデバイスです。外部コールがかけられた場合、ゲートウェイまたはメディア リソースは、IP テレフォニー ネットワークにおいてすべての音声 RTP ストリームが流れる数少ない場所の 1 つです。

IP テレフォニー ゲートウェイおよびメディア リソースは、ネットワーク内のほぼすべての場所に配置できるので、導入済みのセキュリティ ポリシーによっては、IP テレフォニー ゲートウェイまたはメディア リソースを保護することが、他のデバイスを保護することより難しいと見なされる場合があります。しかし、ネットワーク内のどこで信頼が確立されているかによりますが、ゲートウェイおよびメディア リソースを簡単に保護できる場合もあります。ゲートウェイおよびメディア リソースが Cisco Unified CallManager により制御される方法が関係していますが、シグナリングがゲートウェイまたはメディア リソースに到達するために通るパスがネットワーク内で安全と見なされている部分にある場合、単純な ACL を使用して、ゲートウェイまたはメディア リソースに送る、またはそこから戻るシグナリングを制御することができます。ゲートウェイ（またはメディア リソース）と Cisco Unified CallManager のロケーションの間のネットワークが安全と見なされない場合は（ゲートウェイがリモートの支店に置かれている場合など）、インフラストラクチャを使用してゲートウェイおよびメディア リソースへの IPSec トンネルを構築することにより、シグナリングを保護できます。ほとんどのネットワークでは、通常、2 つの方式（ACL および IPSec）の組み合せにより、これらのデバイスが保護されています。

H.323 ビデオ会議デバイスでは、ネットワークのどの H.323 クライアントからでも H.225 トランクのためにポート 1720 をブロックするように、ACL を記述できます。この方法では、ユーザが互いに H.225 セッションを直接開始するのをブロックします。Cisco デバイスでは H.225 にさまざまなポートを使用する場合があるので、どのポートが使用されるかを確認するには、使用する機器の製品マニュアルを参照してください。可能であれば、シグナリングの制御に必要な ACL が 1 つだけになるように、ポートを 1720 に変更します。

ここでは、ネットワークのエッジで QoS を使用しているので、攻撃者が Voice VLAN に侵入してゲートウェイおよびメディア リソースの場所を判別できた場合、ポートの QoS により、攻撃者がゲートウェイまたはメディア リソースに送信できるデータの量が制限されます（図 18-14 を参照）。

図 18-14　IPSec、ACL、および QoS を使用したゲートウェイおよびメディア リソースの保護



電話機で SRTP が有効な場合、一部のゲートウェイおよびメディア リソースでは、ゲートウェイに対する Secure RTP（SRTP）および電話機からのメディア リソースがサポートされます。ゲートウェイまたはメディア リソースが SRTP をサポートしているかどうかを判別するには、次の Web サイトで入手可能な適切な製品マニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_access/index.htm

IPSec トンネルの詳細については、次の Web サイトで入手可能な『*Site-to-Site IPSec VPN Solution Reference Network Design（SRND）*』を参照してください。

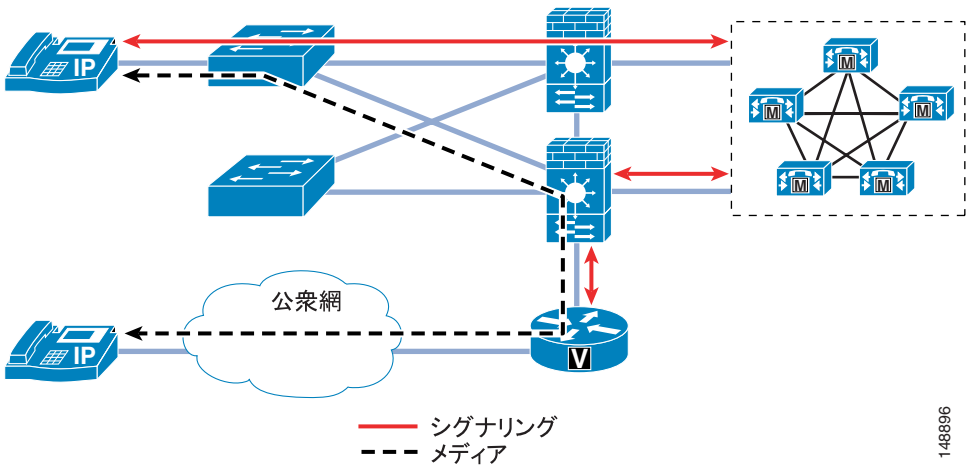
http://www.cisco.com/go/srnd

ゲートウェイの周囲へのファイアウォールの配置

コールの送信元である電話機と、公衆網ネットワークへのゲートウェイとの間にファイアウォールを配置する場合、注意が必要な問題が生じます。ステートフル ファイアウォールは、Cisco Unified CallManager、ゲートウェイ、および電話機の間のシグナリング メッセージの内容を参照し、コールの実行を許可するための RTP ストリーム用のピンホールを開けます。通常の ACL で同じことを行うには、RTP ストリームで使用されるポート範囲全体を、ゲートウェイに対して開放する必要があります。

ネットワーク内にゲートウェイを配置する方法は 2 つあります。つまり、ファイアウォールの背後に配置する方法と、ファイアウォールの前面に配置する方法です。ゲートウェイをファイアウォールの背後に配置する場合、そのゲートウェイを使用している電話機からのすべてのメディアは、ファイアウォールを通過する必要があります。また、これらのストリームがファイアウォールを通過するようにするには、追加の CPU リソースが必要です。次に、ファイアウォールでは、これらのストリームの制御が追加され、ゲートウェイが DoS 攻撃から保護されます（図 18-15 を参照）。

図 18-15　ファイアウォールの背後に配置されたゲートウェイ



ゲートウェイを配置する 2 番目の方法は、ファイアウォールの外側に配置する方法です。電話機からゲートウェイに送信される唯一のデータ タイプは RTP ストリームなので、そのゲートウェイに送信可能な RTP トラフィックの量は、アクセス スイッチの QoS 機能により制御されます。Cisco Unified CallManager からゲートウェイに送信されるのは、コールをセットアップするためのシグナリングだけです。ネットワーク内で、信頼できるエリアにゲートウェイが配置されている場合、Cisco Unified CallManager とゲートウェイの間で許可する必要がある唯一の通信は、そのシグナリングです（図 18-15 を参照）。RTP ストリームはファイアウォールを通過しないので、この配置方式では、ファイアウォールの負荷が低下します。

利点

ACL とは異なり、ほとんどのファイアウォール設定では、シグナリングがファイアウォールを経由している限り、Cisco Unified CallManager が電話機とゲートウェイに対して、それらの 2 つのデバイスの間で使用するように指示している RTP ストリーム ポートだけが開放されます。また、ファイアウォールには、DoS 攻撃用の追加機能や、対象トラフィックを参照して、攻撃者が禁止動作を行っていないかどうかを判別するための Cisco Intrusion Detection System（IDS）シグニチャがあります。

欠点

P.18-33 の「ファイアウォール」の項で説明するように、ファイアウォールが、電話機からゲートウェイへのすべてのシグナリングおよび RTP ストリームを調べる場合、キャパシティが問題になることがあります。また、音声データ以外のデータがファイアウォールを通過する場合、ファイアウォールを通過するコールがファイアウォールにより影響されないように、CPU 使用率を監視する必要があります。

アクティブまたはスタンバイ モードでは、Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）のフェールオーバー時間の最小設定は 3 秒です。Cisco Firewall Services Module（FWSM）の最小タイマー設定も、3 秒です。引き継ぐ必要があるとスタンバイ ユニットが判別した場合、ファイアウォールでは、すぐにフェールオーバーが発生します。ステートフル フェールオーバーが設定されている場合、プライマリ ファイアウォールを通過するデータの状態は、フェールオーバー ユニットに渡されます。このようにして、フェールオーバーの前に実行されていたすべてのことが保持されます。しかし、プライマリ ユニットまたはそのユニットに対する接続性に全面的な障害が発生した場合、ゲートウェイにトラフィックが渡されない時間が、ASA または PIX の場合は 3 秒以上、FWSM の場合は 3 秒間発生します。つまり、ファイアウォールでのフェールオーバーを強要する、ある種類の障害が発生した場合、RTP ストリームは最低 3 秒間停止します。

ファイアウォール

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

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

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

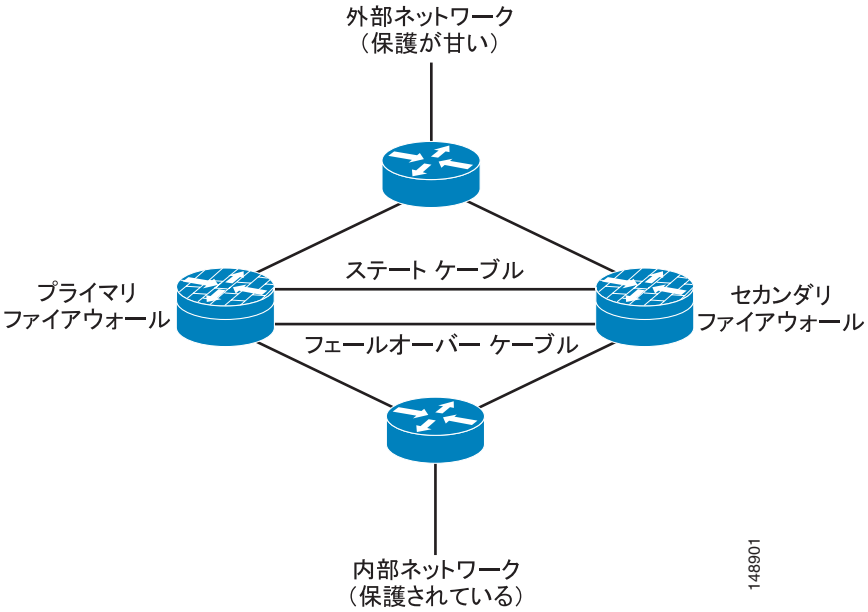
ファイアウォールを配置する方法はいくつもあります。この項では、ルーテッドおよび透過の両方のシナリオにおける、アクティブ / スタンバイ モードの ASA、PIX、および FWSM について集中的に説明します。この項で説明する各設定は、ファイアウォール設定の音声セクション内で、シングル コンテキスト モードで設定されたものです。

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

ASA または PIX と FWSM の機能性の相違点

図 18-16 は、ネットワーク内の冗長ファイアウォールを論理的に表現しています。配置方法は、ルーテッド設定と透過設定で同じです。

図 18-16　冗長ルーテッドまたは透過ファイアウォール



Cisco Adaptive Security Appliance（ASA）および Cisco Private Internet Exchange（PIX）は、Cisco Firewall Cisco Firewall Services Modules（FWSM）とは異なる方法で動作します。ASA または PIX 内では、より信頼性が高いインターフェイスに ACL がない限り、そのインターフェイスからのすべてのトラフィックは信頼され、そこから出て、より信頼性が低いインターフェイスに到達することが許可されます（図 18-17 を参照）。たとえば、ASA の内部インターフェイスまたはデータ センター インターフェイスからのすべてのトラフィックは、ASA から出て、ASA の外部インターフェイスに到達することが許可されます。ASA/PIX 上のより信頼性の高いインターフェイスに任意の ACL を適用すると、他のすべてのトラフィックは拒否（DENY）され、ファイアウォールは FWSM と同様に機能するようになります（図 18-18 を参照）。

図 18-17　Cisco ASA または PIX の機能

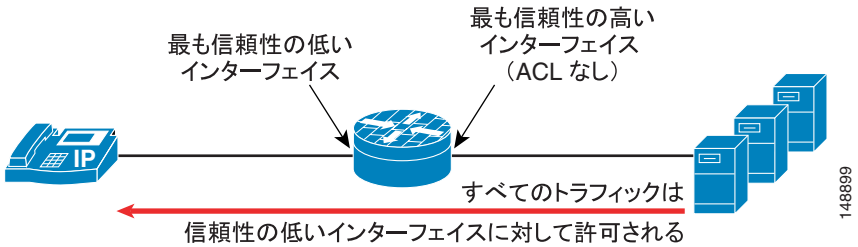
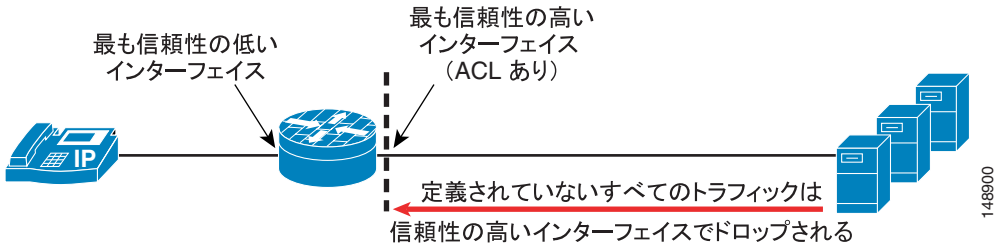


図 18-18　Cisco FWSM の機能



ファイアウォールの全般的な利点

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

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

ファイアウォールの全般的な欠点

ファイアウォールでは、すべての IP テレフォニー アプリケーション サーバまたはアプリケーションがサポートされているわけではありません。ファイアウォール、またはファイアウォール内の ALG でサポートされていない一部のアプリケーションには、Cisco Unity ボイスメール サーバ、Attendant Console、Cisco Unified Contact Center Enterprise、および Cisco Unified Contact Center Express が含まれます。トラフィックがファイアウォールを経由して流れるのを許可するため、これらのアプリケーション用の ACL を書き込むことができます。

現在出荷されているどのファイアウォールでも（ASA/PIX 7.1*x* と FWSM 3.1.*x*、およびそれ以前のバージョンを含む）、SCCP ビデオはサポートされていません。ALG を使用するファイアウォールでは、*Cisco Unified CallManager 5.x* で使用される SIP は現在サポートされていません。SIP シグナリングまたはメディアがファイアウォールを通過する必要がある場合、サポートが可能になるまで ACL を使用する必要があります。

バージョン 3.0 より前の Cisco FWSM では、SCCP フラグメンテーションがサポートされていません。電話機、Cisco Unified CallManager、またはゲートウェイから別の IP テレフォニー デバイスに送信される SCCP パケットが断片化されている場合、断片化されたパケットが FWSM を通過するのは許可されません。断片化が、バージョン 2.*x* のコードを実行する FWSM で発生した場合、シグナリング トラフィック用のファイアウォールの ALG 機能を使用せずに、ACL を使用する必要があります。この設定では、FWSM を通過するシグナリング トラフィックが許可されますが、シグナリングがファイアウォールを通過するときにパケットの検査は実行されません。

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

http://www.cisco.com/univercd/cc/td/doc/product/ipcvoice.htm

ルーテッド ASA および PIX

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

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

利点

ルーテッド ASA または PIX ファイアウォールは、QoS、NAT、およびボックスへの VPN 終端をサポートしています。これらの機能は、トランスペアレント モードではサポートされていません（P.18-36 の「トランスペアレント ASA および PIX」を参照）。

図 18-16 は、アクティブ スタンバイ モードのルーテッド設定と透過設定の両方における、ファイアウォールの論理配置を示しています。ルーテッド設定では、ASA または PIX 上の各インターフェイスに IP アドレスが与えられます。トランスペアレント モードでは、ASA または PIX をリモートで管理するための IP アドレスの他には、インターフェイス上に IP アドレスは与えられません。

欠点

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

トランスペアレント ASA および PIX

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

利点

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

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

欠点

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

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

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

http://www.cisco.com/univercd/cc/td/doc/product/multisec/asa_sw/v_70/config/index.htm

ASA および PIX の設定例

次の設定例は、ファイアウォールが ASA および PIX ソフトウェア Release 7.04 の音声に対して動作するように設定するための、ポートおよび **inspect** コマンドをリストしています。これはあくまでも例にすぎません。任意のファイアウォールを配置する前に、ネットワーク内で使用されているすべてのアプリケーションから取得したポート リストを確認する必要があります。この設定例は、音声セクションのみを示しています。

```
!
!
object-group service remote-access tcp
 description remote access
 !Windows terminal
 port-object range 3389 3389
 !VNC
 port-object range 5800 5800
 !VNC
 port-object range 5900 5900
 port-object range 8080 8080
 port-object eq ssh
 !SSH
 port-object eq ftp-data
 !FTP data transport
  port-object eq www
 !HTTP Access
 port-object eq ftp
 !FTP
 port-object eq https
 !HTTPS Access
object-group service voice-protocols-tcp tcp
 description TCP voice protocols
 CTI/QBE
 port-object range 2428 2428
 !SIP communication
 port-object eq ctiqbe
 !SCCP
 port-object range 2000 2000
 !Secure SCCP
 port-object range 2443 2443
object-group service voice-protocols-udp udp
 !TFTP
 port-object eq tftp
 !MGCP Signaling
 port-object range 2427 2427
 !DNS
 port-object eq domain
 !RAS
 port-object range 1719 1719
 !SIP

!Object Group applied for remote-access
access-list OUTSIDE extended permit tcp any any object-group remote-access
!Object Group applied for voice-protocols-tcp
access-list OUTSIDE extended permit tcp any any object-group voice-protocols-tcp
!Object Group applied for voice-protocols-udp
access-list OUTSIDE extended permit udp any any object-group voice-protocols-udp
! Object Group applied for remote-access
access-list inside_access_in extended permit tcp any any object-group remote-access
! Object Group applied for voice-protocols-tcp
access-list inside_access_in extended permit tcp any any object-group
voice-protocols-tcp
! Object Group applied for voice-protocols-udp
access-list inside_access_in extended permit udp any any object-group
voice-protocols-udp

!Failover config
ip address 172.19.245.3 255.255.255.248 standby 172.19.245.4
failover
```

```
failover lan unit primary
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
!Lowest and fastest setting for failover
failover polltime interface 3
failover link failover_state GigabitEthernet0/2
failover interface ip failover 192.168.1.1 255.255.255.0 standby 192.168.1.2
failover interface ip failover_state 192.168.0.1 255.255.255.0 standby 192.168.0.2

!
!Default inspection with inspects enabled
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map global_policy
 class inspection_default
  inspect h323 h225
  inspect h323 ras
  inspect skinny
  inspect sip
  inspect tftp
  inspect mgcp
```

FWSM ルーテッド モード

ルーテッド モードでは、FWSM がネットワークのルータ ホップと見なされます。このモードでは、接続されているネットワークの間で NAT が実行されます。また、OSPF またはパッシブ RIP（シングル コンテキスト モード）を使用できます。ルーテッド モードでは、コンテキストあたり最大 256 個のインターフェイスがサポートされています。シングル モードでは、すべてのコンテキストに分割された最大 1,000 個のインターフェイスがサポートされています。

利点

ネットワーク内のルーテッド デバイスとして、FWSM は、ルーティング機能、およびトランスペアレント モードで使用可能でない他のすべての機能をサポートしています。

欠点

トランスペアレント モードとは異なり、ルーテッド デバイスはネットワーク上で参照することができ、それが原因で攻撃ポイントになる場合があります。ネットワークにデバイスを配置するには、IP アドレッシングとルーティングの設定を変更する必要があります。

FWSM トランスペアレント モード

トランスペアレント モードでは、FWSM は「Bump In The Wire」または「ステルス ファイアウォール」として動作し、ルータ ホップではありません。FWSM はインターフェイスの内側と外側で同じネットワークに接続しますが、各インターフェイスは異なる VLAN に置かれている必要があります。ダイナミック ルーティング プロトコルまたは NAT は必要ありません。ただし、ルーテッド モードと同様、トランスペアレント モードでも、トラフィックの通過を許可する ACL が必要です。トランスペアレント モードでは、オプションで EtherType ACL を使用して、非 IP トラフィックを許可することもできます。トランスペアレント モードでは、内側インターフェイスと外側インターフェイスの 2 つのインターフェイスのみがサポートされています。

透過ファイアウォールを使用すると、ネットワーク設定を簡素化できます。トランスペアレント モードは、ファイアウォールを攻撃者から見えないようにするためにも便利です。ルーテッド モードではブロックされるトラフィックのために、透過ファイアウォールを使用することもできます。たとえば、透過ファイアウォールで、EtherType ACL を使用したマルチキャスト ストリームを許可できます。

利点

この設定には、ファイアウォールがルーティングを一切行わないため、攻撃者がファイアウォールを見つけることができないという利点があります。この設定では、ファイアウォールに合せてルーティングを変更する必要がないので、より簡単に既存のネットワークにファイアウォールを配置できます。またこの設定は、ファイアウォール内でいずれのルーティングも行わないため、ファイアウォールの管理やデバッグも簡単に実行できます。また、非 IP トラフィックと IP マルチキャストトラフィック、静的 ARP インスペクション、および MAC 移動検出と静的 MAC をブリッジできます。

欠点

トランスペアレント モードでフェールオーバーを使用するときにループを回避するには、Bridge Port Data Unit（BPDU）転送をサポートしているスイッチ ソフトウェアを使用し、BPDU を許可するように FWSM を設定する必要があります。トランスペアレント モードでは、NAT、ダイナミック ルーティング、またはユニキャストのリバース パス フォワーディング（RPF）チェックはサポートされていません。トランスペアレント モードの FWSM に NAT 0 はありません。

FWSM の設定例

次の設定例では、ファイアウォールを FWSM ソフトウェア Release 2.3.*x* の音声に対応させるために使用する、ポートと **inspect** コマンドをリストします。これは例にすぎないので、ファイアウォールを配置する前に、使用中のネットワークで使用されているすべてのアプリケーションからポートのリストを取得して確認する必要があります。この設定例は、音声セクションのみを示しています。

```
fixup protocol h323 H225 1720
!Enable fixup  h3232 h225

fixup protocol h323 ras 1718-1719
!Enable fixup h323 RAS

fixup protocol mgcp 2427
!Enable fixup  mgcp

fixup protocol skinny 2000
!Enable fixup

fixup protocol tftp 69
!Enable fixup

object-group service VoiceProtocols tcp
  description Unified CM Voice protocols
  port-object eq ctiqbe
  port-object eq 2000
  port-object eq 3224
  port-object eq 2443
  port-object eq 2428
  port-object eq h323
!Defining the ports for TCP voice

object-group service VoiceProtocolsUDP udp
  description UDP based Voice Protocols
  port-object range 2427 2427
  port-object range 1719 1719
  port-object eq tftp
!Defining the ports for UDP voice

object-group service RemoteAccess tcp
  description Remote Acces
  port-object range 3389 3389
  port-object range 5800 5809
```

```
  port-object eq ssh
  port-object range 5900 5900
  port-object eq www
  port-object eq https
!Defining remote access TCP ports

access-list inside_nat0_outbound extended permit ip any any
!

access-list phones_access_in extended permit tcp any any object-group RemoteAccess log
notifications interval 2
access-list phones_access_in extended permit tcp any any object-group VoiceProtocols
log notifications interval 2
access-list phones_access_in extended permit udp any any object-group
VoiceProtocolsUDP log notifications interval 2
access-list phones_access_in extended deny ip any any log notifications interval 2
access-list outside_access_in extended permit tcp any any object-group VoiceProtocols
log notifications interval 2
access-list outside_access_in extended permit tcp any any object-group RemoteAccess
log notifications interval 2
access-list outside_access_in extended permit udp any any object-group
VoiceProtocolsUDP log notifications interval 2
!Access lists applying the object groups defined above for inside and outside
interfaces

access-list outside_access_in extended deny ip any any log notifications interval 2
access-list inside_access_in extended deny ip any any
!Deny all other traffic

access-list phones_nat0_outbound extended permit ip any any
!

failover
failover lan unit primary
failover lan interface flan vlan 4050
failover polltime unit 1 holdtime 5
failover polltime interface 15
!Failover config - 15 seconds
failover interface-policy 50%
failover link flin vlan 4051
failover interface ip flan 1.1.1.1 255.255.255.252 standby 1.1.1.2
failover interface ip flin 1.1.1.5 255.255.255.252 standby 1.1.1.6
nat (inside) 0 access-list inside_nat0_outbound_V1
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
```

データ センター

データ センター内では、IP テレフォニー アプリケーション サーバで必要なセキュリティについて、セキュリティ ポリシーを定義する必要があります。Cisco Unified Communications サーバは IP に基づいているので、データ センター内にある、時間に敏感なほかのデータに適用するセキュリティを、これらのサーバにも適用することができます。

データ センターの間で WAN でのクラスタ化が使用されている場合、データ センター内とデータ センター間の両方に適用されている追加のセキュリティは、クラスタ内のノード間で許可されている最大往復時間に収まる必要があります。ネットワーク内のアプリケーション サーバ用に導入されている現在のセキュリティ ポリシーに、Cisco IP テレフォニー サーバが含まれている場合、そのセキュリティを使用する必要があります。また、すでに配置されている任意のインフラストラクチャ セキュリティを使用することもできます。

データ アプリケーションに適したデータ センター セキュリティを設計するには、次の Web サイトで入手可能な『*Data Center Networking: Server Farm Security SRND*』（『*Server Farm Security in the Business Ready Data Center Architecture*』）のガイドラインに従うことをお勧めします。

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

アプリケーション サーバ

Cisco Unified CallManager セキュリティ機能のリスト、および有効にする方法については、次の Web サイトで入手可能な『*Cisco Unified CallManager Security Guide*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/ipp7960/sec_vir/sec413/index.htm

任意の Cisco Unified CallManager セキュリティ機能を有効にする前に、それらの機能が、ネットワーク内のこれらのタイプのデバイスに関する企業セキュリティ ポリシーで指定されている、セキュリティ要件を満たしていることを確認してください。

Cisco Unified CallManager およびアプリケーション サーバ上の Cisco Security Agent

Cisco Security Agent は、IP テレフォニーおよび IP テレフォニー サービスを提供するのにシスコが使用するアプリケーション サーバのほとんどで使用されています。Cisco Security Agent ソフトウェアは、サーバとの間のトラフィックの動作と、サーバ上でアプリケーションが実行される方法を調べて、すべてが正常かどうかを判別する、ホスト侵入防御ソフトウェアです。異常と見なされるものが見つかった場合、Cisco Security Agent ソフトウェアはそのアクティビティが発生するのを阻止します。たとえば、Cisco Unified CallManager にソフトウェア パッケージをインストールすることを試みるウイルスがあり、そのような事態が以前発生したことがない場合でも、ウイルスがインストールを実行することは阻止されます。ただし、Cisco Security Agent は感染を防止するだけで、一度感染したサーバをクリーンにすることはできないので、サーバにはアンチウイルス ソフトウェアが引き続き必要です。

マネージドではない Cisco Security Agent

シスコは、自社サーバ用のデフォルト Cisco Security Agent ポリシーを開発しました。このポリシーにより、IP テレフォニー サーバで必要なすべての機能は正しく機能し、同時に、既知および不明な攻撃が IP テレフォニー サーバに影響することは防止されます。最低でも、このマネージドではないバージョンの Cisco Security Agent をインストールおよび実行する必要があります。このソフトウェアは、アプリケーションとオペレーティング システムを、ウイルスやワーム攻撃から保護しま

す。これらのタイプの侵入からの最大限の保護を得るには、常に最新バージョンの Cisco Security Agent ソフトウェアがサーバにインストールされていることを確認してください。マネージドではないエージェントがサーバにインストールされていると、攻撃のログは、エージェントがインストールされているシステムでのみ参照できます。特定のタイプのアラームが発生したので書き込まれた可能性があるログ ファイルをチェックするには、各システムにログインする必要があります。

利点

マネージドではない Cisco Security Agent は、既知および不明の攻撃、ワーム、およびウイルスから各システムを保護します。

欠点

Cisco Security Agent を管理対象外モードで実行すると、アラームは相関されません。システムのログ ファイルを参照するには、各システムに個別にアクセスする必要があります。マネージドではない Cisco Security Agent をアップグレードする場合、新しいクライアントをインストールした後、通常は、クライアント設定を有効にするためシステムをリブートする必要があります。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

マネージド Cisco Security Agent

マネージド Cisco Security Agent は、管理対象外バージョンと同じように動作しますが、管理コンソールに、追加の利点がいくつかあります。管理対象システムを実行すると、すべてのシステムからのすべてのアラームを 1 つのコンソールで受信できます。また、この機能では、異常な状態が重大なレベルに達したときに、そのことを電子メールまたはポケットベルで通知するように設定できます。

（注） Cisco Unified CallManager 5.0 では現在、マネージド Cisco Security Agent の機能は利用できません。

利点

マネージド Cisco Security Agent では、マネージドではないシステムと同じ保護が提供されるだけでなく、エージェントの制御も行うことができます。この制御により、アップデート時にシステムをリロードすることなく、イベントの相関、管理コンソールへのグローバル レポートの返信、エージェントの Cisco Security Agent 設定のアップグレードを実行できます。

欠点

別個のサーバに、管理対象エージェントのグローバル モニタリングと設定用の別々のソフトウェアが必要です。何らかの理由によりシステムが感染した場合、Cisco Security Agent は、そのシステムをクリーンにすることはできません。セキュリティを保持し、システムを保護するには、システムでアンチウイルス ソフトウェアも実行する必要があります。

アンチウイルス

ソフトウェアを実行することが承認されているすべての IP テレフォニー サーバおよび IP テレフォニー アプリケーション サーバで、承認済みのアンチウイルス ソフトウェアを実行する必要があります。ネットワーク内の他のサーバと同様、アンチウイルス ソフトウェアは、コールの処理に影響するワームやウイルスの感染から、Cisco Unified CallManager サーバを保護します。Cisco Security

Agent はシステムの感染をクリーンにできないので、Cisco Security Agent 以外の防御ソフトウェアもシステムにインストールする必要があります。感染したシステムをクリーンにできるのはアンチウイルス ソフトウェアのみです。

Cisco Unified CallManager サーバでのアンチウイルス ソフトウェアの実行に関する追加情報は、次の Web サイトで入手可能です。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/sec_vir/index.htm

利点

アンチウイルス ソフトウェアは、アプリケーション サーバが感染して、パフォーマンスが低下するのを防止するのに役立ちます。

欠点

アンチウイルス ソフトウェアの管理には、いくらかのオーバーヘッドが含まれます。さらに、Cisco Unified CallManager および IP テレフォニー アプリケーション サーバへのインストールで、ソフトウェアのバージョンが承認されていることを確認する必要があります。

サーバに関する一般的なガイドライン

Cisco Unified CallManager およびその他の IP テレフォニー アプリケーション サーバは、通常のサーバとして扱わないでください。システムの設定時に行う任意の操作が、開始を試みているコール、または進行中のコールに影響する場合があります。他のビジネスクラス アプリケーションと同様、大規模な設定の変更は、電話の会話を遮断することがないようメンテナンス ウィンドウで行う必要があります。

アプリケーション サーバ用の標準的なセキュリティ ポリシーは、IP テレフォニー サーバには不十分な場合があります。電子メール サーバや Web サーバとは異なり、音声サーバでは、画面をリフレッシュしたり、メッセージを再送信したりすることは許可されていません。音声通信は、リアルタイムのイベントです。IP テレフォニー サーバ用のセキュリティ ポリシーでは、音声システムの設定または管理に関連付けられていない作業が、IP テレフォニー サーバで決して行われないことを保証する必要があります。ネットワーク内のアプリケーション サーバで通常のアクティビティと見なされるアクティビティ（インターネット サーフィンなど）でも、IP テレフォニー サーバで行うことはできません。

また、シスコは IP テレフォニー サーバ用に適切に定義されたパッチ システムを提供しています。IT 組織内のパッチ ポリシーに基づいて、このパッチ システムを適用する必要があります。シスコシステムズにより承認されている場合を除き、OS ベンダーのパッチ システムを使用する通常の方法でシステムにパッチを適用しないでください。すべてのパッチは、シスコシステムズの指示に従ってシスコまたは OS ベンダーからダウンロードし、パッチ インストール プロセスに応じて適用する必要があります。

Cisco Unified CallManager 用に OS を強化する方法の詳細は、Cisco Unified CallManager サーバの C:\Utils\SecurityTemplates ディレクトリにリストされています。導入済みのセキュリティ ポリシーで、デフォルト インストールで提供された以上の OS のロック ダウンが要求されている場合は、OS の強化手法を使用する必要があります。

さまざまなソフトウェア パッチが、次の Web サイトで入手可能です。

http://www.cisco.com/kobayashi/sw-center/sw-voice.shtml

（注）　このリンクにアクセスするには、Cisco.com ログイン アカウントが必要です。

上記のサイトには、IP テレフォニー サーバに重要なパッチを適用する必要が生じたときに電子メールで通知する通知ツールも含まれています。

利点

アプリケーション サーバを他のアプリケーション サーバのようではなく PBX のように扱う場合、一般的なサーバ セキュリティ プラクティスを実施すると、ウイルスやワームを減らすのに役立ちます。

欠点

追加のセキュリティ機能を設定すると、一部の Cisco Unified CallManager 機能が低下する場合があります。また、アップグレードを正常に実行するには、追加のセキュリティで無効になっている一部のサービスを有効にする必要があるため、アップグレード中は特に注意が必要です。

配置例

この項では、ロビーに設置された電話機およびファイアウォールの配置について、セキュリティ面を考慮した実施例を示します。このようなタイプと同様の配置を扱うには、適切なセキュリティ ポリシーを適用する必要があります。

ロビーに設置された電話機の例

この項の例は、物理的なセキュリティが低いロビー エリアのようなエリアで使用する、電話機およびネットワークを設定する 1 つの方法を示しています。この例に出てくる機能は、いずれもロビーに設置する電話機で要求されている機能ではありませんが、導入済みのセキュリティ ポリシーで、より強固なセキュリティが必要とされている場合は、この例でリストされている機能を使用できます。

いずれのユーザも電話機の PC ポートからネットワークにアクセスできないようにするため、電話機の背面の PC ポートを無効にして、ネットワーク アクセスを制限する必要があります（P.18-6 の「電話機の PC ポート」を参照）。また、攻撃を仕掛けようとしている人が、ロビーに設置された電話の接続先ネットワークの IP アドレスを参照できないように、電話機の設定ページも無効にする必要があります（P.18-10 の「アクセス設定」を参照）。電話機の設定を変更できないという欠点は、通常、ロビーに設置された電話機では問題になりません。

ロビーに設置された電話機が移動される可能性は非常に低いため、電話機には固定 IP アドレスを使用できます。固定 IP アドレスを使用すると、攻撃者が電話機を切断して接続することにより新しい IP アドレスを取得するのを防止できます（P.18-5 の「IP アドレッシング」を参照）。また、電話機が抜かれると、ポートの状態が変化し、電話機は Cisco Unified CallManager から登録解除されます。ロビーに設置された電話機のポートでこのイベントをトラッキングするだけで、だれかがネットワークへの接続を試行しているかどうかを判別できます。

電話機の静的ポート セキュリティを使用し、MAC アドレスを取得することを許可しない場合、攻撃者は、そのアドレスを発見できたときに、自らの MAC アドレスをその電話機の MAC アドレスに変更しなければなりません。動的ポート セキュリティを無制限タイマーと共に使用して、MAC アドレスを取得する（取得したアドレスは解除しない）場合、MAC アドレスを追加する必要はありません。これにより、電話機を交換しない限り、MAC アドレスをクリアするためにスイッチポートを変更せずにすみます。MAC アドレスは、電話機の底面のラベルにリストされています。MAC アドレスをリストすることがセキュリティの問題と見なされる場合は、ラベルを除去し、デバイスを識別するための「ロビー用」というラベルに置き換えることができます（P.18-14 の「スイッチポート」を参照）。

ポートまたはポートが接続されているスイッチに関する情報を攻撃者がイーサネット ポートから参照できないように、単一の VLAN を使用し、ポートで Cisco Discovery Protocol（CDP）を無効にできます。この場合、電話機の E911 緊急コール用のスイッチに CDP エントリは与えられません。緊急番号をダイヤルするときは、ロビーに設置された各電話機に、ラベル、またはローカル セキュリティ用の情報メッセージのいずれかが必要です。

ポート上に DHCP は存在しないため、DHCP スヌーピング バインディング テーブルに静的エントリを定義できます（P.18-17 の「DHCP スヌーピング：不正な DHCP サーバ攻撃の防止」を参照）。DHCP スヌーピング バインディング テーブルに静的エントリを定義すると、VLAN で Dynamic ARP Inspection を有効にして、攻撃者が、ネットワーク上のレイヤ 2 ネイバーの 1 つに関する他の情報を取得するのを防止できます（P.18-21 の「Dynamic ARP Inspection の要件」を参照）。

DHCP スヌーピング バインディング テーブルに静的エントリが定義されていると、IP ソース ガードを使用できます（P.18-24 の「IP ソース ガード」を参照）。攻撃者が MAC アドレスと IP アドレスを取得でき、パケットの送信を開始した場合、正しい IP アドレスが設定されたパケットだけを送信できます。

電話機が動作するのに必要なポートと IP アドレスのみを許可する、VLAN ACL を書き込むことができます（P.18-26 の「VLAN アクセス コントロール リスト」を参照）。次の例には、ネットワークへのアクセスを制御するための、レイヤ 2 または最初のレイヤ 3 デバイスのポートに適用可能な非常に小規模な ACL が含まれています（P.18-28 の「ルータのアクセス コントロール リスト」を参照）。この例は、ロビー エリアで使用されている Cisco 7960 IP Phone に基づいています。電話機への Music on Hold または電話機からの HTTP アクセスは使用しません。

この例では、次の IP アドレス範囲を使用します。

- ロビーに設置された電話機の IP アドレスは 10.0.40.5
- Cisco Unified CallManager クラスタのアドレス範囲は 10.0.20.*
- DNS サーバの IP アドレスは 10.0.30.2
- HSRP ルータの IP アドレスは 10.0.10.2 および 10.0.10.3
- ネットワーク内の他の電話機の IP アドレスの範囲は 10.0.*.*

```
10 permit icmp any any
! Allow all icmp - phone to phone, gateway to phone and NMS to phone

20 permit udp host 10.0.10.2 eq 1985 any
!Allow HSRP information in, do not allow out

30 permit udp host 10.0.10.3 eq 1985 any
! Allow in from HSRP neighbor

40 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq tftp
! Using ip host from ephemeral port range from phone to the TFPT server  port 69
(start of tftp)

50 permit udp 10.0.20.0 0.0.0.255 range 1024 5000 host 10.0.40.5 range 49152 65535
!Using IP subnet from TFTP server with ephemeral port range to ip host and ephemeral
port range for phone

60 permit udp host 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 range 1024 5000
! Using host from phone to TFTP server with ephemeral port range to ip range and
ephemeral port range for TFTP (continue the TFTP conversation)

70 permit udp host 10.0.40.5 range 49152 65535 host 10.0.30.2 eq domain
! Using IP host and ephemeral port range from phone to DNS server host

80 permit udp host 10.0.30.2 eq domain host 10.0.40.5 range 49152 65535
! Using IP from DNS server to phone host ip and ephemeral port range

90 permit tcp 10.0.40.5 range 49152 65535 10.0.20.0 0.0.0.255 eq 2000
! Using IP host and ephemeral port range from phone to Unified CM cluster for SCCP


100 permit tcp 10.0.20.0 0.0.0.255 eq 2000 host 10.0.40.5 range 49152 65535
! Using IP range and SCCP port to phone IP host and ephemeral port range


110 permit udp 10.0.0.0 0.0.255.255 range 16384 32767 host 10.0.40.5 range 16384 32767
! Using IP range and ephemeral port range from all phones or gateways outside a vlan
to the IP host to phone

120 permit udp host 10.0.40.5 range 16384 32767 10.0.0.0 0.0.255.255 range 16384 43767
! Using IP host and ephemeral port range from vlan to all other phones or gateways

130 permit udp host 172.19.244.3 range 1024 5000 host 10.0.40.5 eq snmp
!From IP host of NMS server and ephemeral port range (Different for Windows vs Sun) to
IP host of phones and SNMP port (161)

140 permit udp host 10.0.40.5 eq snmp host 172.19.244.3 range 1024 5000
! From IP host of phone with SNMP port (161) to IP host of NMS server and ephemeral
port range
```

ロビーに設置された電話機用の基本的な QoS の例

音声ストリームを G.729 に設定し、ポートに送信可能なトラフィックの量を、QoS を使用して制限します（P.18-25 の「Quality of Service」を参照）。QoS 最大値を超えても、トラフィックは、一般的な企業ネットワークで優先度が最低のトラフィックである CS1 つまり Scavenger Class にリセットされます。

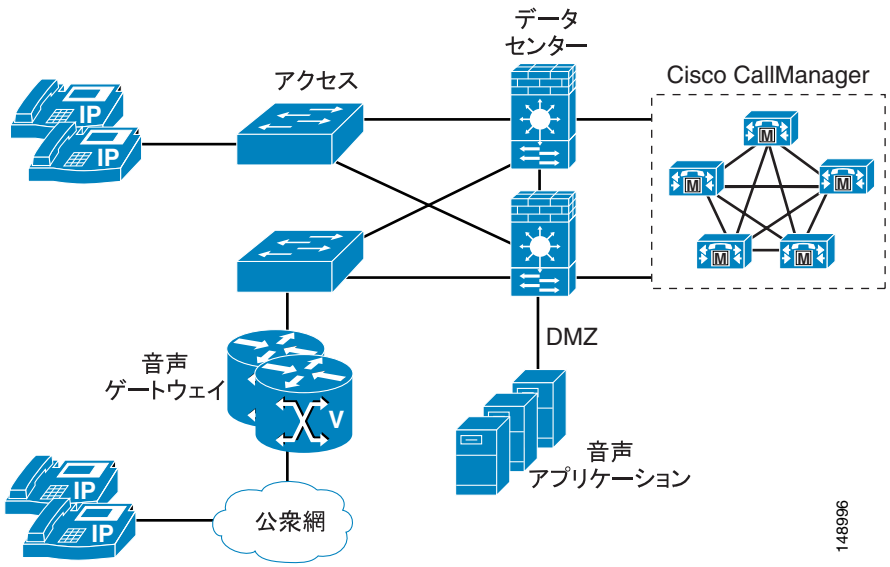
```
CAT2970(config)#mls qos map policed-dscp 0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT2970(config)#
CAT2970(config)#class-map match-all LOBBY-VOICE
CAT2970(config-cmap)# match access-group name LOBBY-VOICE
CAT2970(config-cmap)#class-map match-all LOBBY-SIGNALING
CAT2970(config-cmap)# match access-group name LOBBY-SIGNALING
CAT2970(config-cmap)#exit
CAT2970(config)#
CAT2970(config)#policy-map LOBBY-PHONE
CAT2970(config-pmap)#class LOBBY-VOICE
CAT2970(config-pmap-c)# set ip dscp 46 ! Lobby phone VoIP is marked to DSCP EF
CAT2970(config-pmap-c)# police 48000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Lobby voice traffic (g.729) is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class LOBBY-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24 ! Signaling is marked to DSCP CS3
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signaling traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)#class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 56000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1)
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)#exit
CAT2970(config)#
CAT2970(config)#interface GigabitEthernet0/1
CAT2970(config-if)# service-policy input LOBBY-PHONE ! Applies policy to int
CAT2970(config-if)#exit
CAT2970(config)#
CAT2970(config)#ip access list extended LOBBY-VOICE
CAT2970(config-ext-nacl)# permit udp any any range 16384 32767 ! VoIP ports
CAT2970(config-ext-nacl)#
CAT2970(config-ext-nacl)#ip access list extended LOBBY-SIGNALING
CAT2970(config-ext-nacl)# permit tcp any any range 2000 2002 ! SCCP ports
CAT2970(config-ext-nacl)#end
CAT2970#
```

ファイアウォールの配置例（集中型配置）

この項の例は、データ センター内において、背後に Cisco Unified CallManager を配置するファイアウォールの 1 つの展開方法を示しています（図 18-19）。この例では、Cisco Unified CallManager は、すべての電話機がファイアウォールの外側から 1 つのクラスタに接続される集中型配置として置かれています。この配置内のネットワークには、社内データ センター内でルーテッド モードで設定されたファイアウォールがすでに含まれているので、ゲートウェイの配置を決定する前に負荷が確認されます。ファイアウォールの平均的な負荷を確認した後、CPU に対するファイアウォールの負荷を 60% 未満に保つため、すべての RTP ストリームがファイアウォールを横断しないようにすることが決定されました（P.18-31 の「ゲートウェイの周囲へのファイアウォールの配置」を参照）。ゲートウェイはファイアウォールの外側に配置されています。Cisco Unified CallManager でゲートウェイとの間の TCP データ フローを制御するため、ネットワーク内の ACL を使用します。電話機の IP アドレスは適切に定義されているので、ACL は、電話機からの RTP ストリームを制御するためネットワークにも書き込まれます（P.18-5 の「IP アドレッシング」を参照）。音声アプリケーション サーバは非武装地帯（DMZ）に配置されています。Cisco Unified CallManager との間のアクセス、およびネットワーク上のユーザへのアクセスを制御するため、ファイアウォールで ACL を使用し

ます。この設定では、インスペクションを使用してファイアウォールを通過する RTP ストリームの量を制限します。これにより、既存のネットワークに新しい音声アプリケーションを追加したときの、ファイアウォールに対する影響を最小に抑えられます。

図 18-19　ファイアウォールの配置例



まとめ

この章では、ネットワーク内の音声データを保護するために有効にできるセキュリティのうち、一部のみを取り上げました。ここで取り上げた手法は、ネットワーク内のすべてのデータを保護するためにネットワーク管理者が使用できる、すべてのツールのサブセットにすぎません。逆に、ネットワーク全体のデータで必要なセキュリティのレベルによっては、これらのツールでさえ、ネットワークで有効にする必要がない場合もあります。セキュリティの方法は、注意深く選択してください。ネットワーク内のセキュリティが高くなると、それに応じて、複雑度や問題のトラブルシューティングも増加します。各企業の責任で、リスクと組織の要件の両方を定義し、ネットワークとネットワークに接続されたデバイスに適切なセキュリティを適用する必要があります。

CHAPTER 19

IP テレフォニー エンドポイント

この章では、さまざまなタイプの IP テレフォニー エンドポイントとその機能、および QoS 推奨事項について要約します。IP テレフォニー エンドポイントは、次の主要なタイプに分類できます。

- アナログ ゲートウェイ（P.19-2）
- Cisco Unified IP Phone（P.19-7）
- ソフトウェアベースのエンドポイント（P.19-11）
- 無線エンドポイント（P.19-16）
- Cisco IP Conference Station（P.19-21）
- ビデオ エンドポイント（P.19-22）
- サードパーティ製 SIP IP Phone（P.19-27）

上記の各項では、それぞれのエンドポイント タイプについて詳細情報を示します。加えて、P.19-28 の「QoS の推奨事項」の項では QoS 設定のリストを示し、P.19-43 の「エンドポイント機能の要約」の項ではエンドポイントの全機能のリストを示します。

次のリストに、IP テレフォニー エンドポイントを選択する際の基本的な推奨事項の要約を示します。

- 低密度アナログ接続には、Cisco Analog Telephone Adapter（ATA）または低密度アナログ インターフェイス モジュールを使用する。
- 中密度から高密度のアナログ接続には、高密度アナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco Communication Media Module（CMM; コミュニケーション メディア モジュール）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG224、または Cisco VG248 を使用する。
- トラフィックの発生量が少なく、コール機能に制限のあるテレフォニー ユーザには、Cisco Unified IP Phone 7902G、7905G、7911G、7912G、または 7912G-A を使用する。
- トラフィックの発生量が中程度で、トランザクション タイプのテレフォニー ユーザには、Cisco Unified IP Phone 7940G、7941G、または 7941G-GE を使用する。
- テレフォニー　トラフィックの発生量が中程度から大量の、マネージャおよびアシスタントには、Cisco Unified IP Phone 7960G、7961G、または 7961G-GE を使用する。
- テレフォニー　トラフィックの発生量が多い、拡張コール機能を使用する経営幹部には、Cisco Unified IP Phone 7970G または 7971G-GE を使用する。
- 外勤職員および在宅勤務者には、Cisco IP Communicator を使用する。
- モバイル IP Phone が必要なユーザには、Cisco Unified Wireless IP Phone 7920 を使用する。
- ビデオ コールの発信には、Cisco Unified IP Phone に関連付けられた Cisco Unified Video Advantage、Cisco IP Video Phone 7985G、または Sony 社製と Tandberg 社製の SCCP エンドポイントのいずれかを使用する。
- 正式な会議環境には、Cisco Unified IP Conference Station 7936 を使用する。

アナログ ゲートウェイ

アナログ ゲートウェイには、ルータベースのアナログ インターフェイス モジュール、24-FXS ポート アダプタ搭載の Cisco Communication Media Module（CMM）、Catalyst 6500 24-FXS アナログ インターフェイス モジュール、Cisco VG224、Cisco VG248、および Cisco Analog Telephone Adaptor（ATA）186 と 188 があります。通常、アナログ ゲートウェイは、FAX、モデム、TDD/TTY、およびアナログ電話機などのアナログ デバイスを VoIP ネットワークに接続するために使用します。これにより、アナログ信号を IP ネットワーク上でパケット化して送信できるようになります。

アナログ インターフェイス モジュール

ルータベースの Cisco アナログ インターフェイス モジュールには、低密度インターフェイス モジュール（NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1）と高密度インターフェイス モジュール（NM-HDA-4FXS および EVM-HD-8FXS/DID）があります。Cisco アナログ インターフェイス モジュールは、公衆網やその他の従来の電話機器（PBX、アナログ電話機、FAX、キー システムなど）を、Cisco マルチサービス アクセス ルータに接続するためのものです。Cisco アナログ インターフェイス モジュールは、低密度から高密度までのアナログ デバイスを、コール機能に制限がある IP ネットワークに接続する場合に最適です。

低密度アナログ インターフェイス モジュール

低密度アナログ インターフェイス モジュールには、NM-1V、NM-2V、NM-HD-1V、NM-HD-2V、NM-HD-2VE、NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 があります。NM-1V と NM-2V には、1 つまたは 2 つの音声インターフェイス カード（VIC）があります。このインターフェイス カードには、2 ポート FXS VIC（VIC-2FXS）、2 ポート FXO VIC（VIC-2FXO、VIC-2FXO-M1/M2/M3、および VIC-2FXO-EU）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2 ポート E&M VIC（VIC-2E/M）、2 ポート CAME（Centralized Automated Message Accounting）VIC（VIC-2CAMA）、および 2 ポート BRI VIC（VIC-2BRI-S/T-TE および VIC-2BRI-NT/TE）があります。NM-1V および NM-2V は、それぞれ最大で 2 個および 4 個の FXS 接続を処理できます。

（注） NM-1V と NM-2V は、Cisco 2800 および 3800 シリーズのプラットフォームではサポートされていません。Cisco 2800 および 3800 シリーズのプラットフォームでは、VIC-2DID、VIC4-FXS/DID、VIC2-2FXO、VIC-2-4FXO、VIC2-2FXS、VIC2-2E/M、および VIC2-2BRI-NT/TE を含む音声インターフェイス カードは、オンボードの高速 WIC スロットでサポートされています。

NM-HD-1V と NM-HD-2V には、それぞれ 1 つおよび 2 つの VIC があります。NM-HD-2VE には、2 つの VIC または 2 つの音声 /WAN インターフェイス カード（VWIC）、または 1 つの VIC と 1 つの VWIC の組み合せが含まれます。NM-HD-1V、NM-HD-2V、および NM-HD-2VE は、それぞれ最大で 4 個、8 個、および 8 個の FXS 接続または FXO 接続を処理できます。NM-HDV2、NM-HDV2-1T1/E1、および NM-HDV2-2T1/E1 は、最大 4 個の FXS 接続または FXO 接続を処理するデジタル T1/E1 またはアナログ /BRI のいずれかに対応させることができます。これら 3 つのインターフェイス モジュールの相違点は、NM-HDV2-1T1/E1 には 1 つの組み込み T1/E1 ポートがあるのに対し、NM-HDV2-2T1/E1 には 2 つの組み込み T1/E1 ポートがあることです。

音声インターフェイス カードには、2 ポートおよび 4 ポート FXS VIC（VIC2-2FXS および VIC-4FXS/DID）、2 ポートおよび 4 ポート FXO VIC（VIC2-2FXO および VIC2-4FXO）、2 ポート ダイヤルイン方式 VIC（VIC-2DID）、2 ポート E&M VIC（VIC2-2E/M）、および 2 ポート BRI VIC（VIC2-2BRI-NT/TE）があります。音声 /WAN インターフェイス カードには、音声および WAN 接

続両用の 1 ポートおよび 2 ポート RJ-48 マルチフレックス トランク（MFT）T1/E1 VWIC（VWIC-1MFT-T1、VWIC-2MFT-T1、VWIC-2MFT-T1-DI、VWIC-1MFT-E1、VWIC-2MFT-E1、VWIC-2MFT-E1-DI、VWIC-1MFT-G703、VWIC-2MFT-G703、VWIC2-1MFT-T1/E1、VWIC2-2MFT-T1/E1、VWIC2-1MFT-G703、および VWIC2-2MFT-G703）があります。G.703 インターフェイス カードは主としてデータ接続用ですが、場合によっては音声アプリケーションをサポートするように設定できます。

高密度アナログ インターフェイス モジュール

高密度アナログ インターフェイス モジュールには NM-HDA-4FXS と EVM-HD-8FXS/DID があります。NM-HDA-4FXS には 4 つのオンボード FXS ポートがあり、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード
- EM-HDA-4FXO/EM2-HDA-4FXO：4 ポート FXO インターフェイス カード

NM-HDA-4FXS は、4 つの組み込み FXS ポートと 2 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 12 アナログ ポート（4 FXS および 8 FXO）の構成になるか、または 4 つの組み込み FXS ポートと 1 つの EM-HDA-8FXS 拡張モジュールおよび 1 つの EM-HDA-4FXO または EM2-HDA-4FXO 拡張モジュールで最大 16 アナログ ポート（12 FXS および 4 FXO）の構成になります。2 つの 8 ポート FXS 拡張モジュールを使用する構成はサポートされていません。NM-HDA には、追加の DSP リソースを提供するドーター モジュール（DSP-HDA-16）用のコネクタもあり、8 つの高複雑度コールまたは 16 の中複雑度コールを追加処理できます。

（注） EM2-HDA-4FXO は、EM-HDA-FXO と同じ密度と機能をサポートしますが、最大 15,000 フィートのループ長のサポートや、グラウンドスタート シグナリング モードで使用して回線状態が悪い場合のパフォーマンス向上などの拡張機能があります。

EVM-HD-8FXS/DID は、基本ボード モジュール上に 8 つの独立したポートがあり、FXS または DID シグナリング用に構成可能です。また、EVM-HD-8FXS/DID には、次のオプションから 2 つの拡張モジュールを取り付けることができます。

- EM-HDA-8FXS：8 ポート FXS インターフェイス カード
- EM-HDA-6FXO：6 ポート FXO インターフェイス カード
- EM-HDA-3FXS/4FXO：3 ポート FXS および 4 ポート 4FXO インターフェイス カード
- EM-4BRI-NT/TE：4 ポート BRI インターフェイス カード

これらの拡張モジュールは任意の組み合せで使用でき、EVM-HD-8FXS/DID あたり最大 24 FXS ポートの構成になります。

アナログ インターフェイス モジュールでサポートされているプラットフォームおよび Cisco IOS 要件

Cisco アナログ インターフェイス モジュール用にサポートされているプラットフォームは、Cisco 2600、2800、3600、3700、および 3800 シリーズです。表 19-1 は、各プラットフォームでサポートされているインターフェイス モジュールの最大数を示しています。表 19-2 は必要な Cisco IOS ソフトウェアの最小バージョンを示しています。

表 19-1　各プラットフォームでサポートされるアナログ インターフェイス モジュールの最大数

プラットフォーム	サポートされているインターフェイス モジュールの最大数				
	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	1	1	なし	1	1
Cisco 2691	1	1	なし	1	1
Cisco 3640	3	3	なし	3	なし
Cisco 3660	6	6	なし	6	なし
Cisco 3725	2	2	なし	2	2
Cisco 3745	4	4	なし	4	4
Cisco 2811	なし	1	1	1	1
Cisco 2821	なし	1	1	1	1
Cisco 2851	なし	1	1	1	1
Cisco 3825	なし	2	1	2	2
Cisco 3845	なし	4	2	4	4

表 19-2　アナログ インターフェイス モジュールの Cisco IOS 最小要件

プラットフォーム	必要な Cisco IOS ソフトウェア対応リリース				
	NM-1V、-2V	NM-HDA-4FXS	EVM-HD	NM-HD-1V、-2V、-2VE	NM-HDV2、-1T1/E1、-2T1/E1
Cisco2600XM	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 2691	12.2(8)T	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 3640	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3660	12.0(1)T 以降	12.2(8)T 以降	なし	12.3.4T	なし
Cisco 3725	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 3745	12.2(8)T 以降	12.2(8)T	なし	12.3.4T	12.3(7)T
Cisco 2811	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2821	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 2851	なし	12.3.8T4	12.3.8T4	12.3.8T4	12.3.8T4
Cisco 3825	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T
Cisco 3845	なし	12.3(11)T	12.3(11)T	12.3(11)T	12.3(11)T

Cisco コミュニケーション メディア モジュール（CMM）

Cisco CMM は、Catalyst 6000 および Cisco 7600 シリーズ スイッチに、高密度アナログ、T1、および E1 ゲートウェイ接続を提供するライン カードです。Cisco CMM は、最大 72 個の 72 FXS 接続を処理できます。CMM は MGCP または H.323 ゲートウェイとして動作し、最大 480 個の IP Phone に Survivable Remote Site Telephony（SRST）サービスを提供します。

Cisco CMM に含まれるインターフェイス ポート アダプタは、24 ポート FXS アナログ ポート アダプタ（WS-SVC-CMM-24FXS）、6 ポート T1 インターフェイス ポート アダプタ（WS-SVC-CMM-6T1）、6 ポート E1 インターフェイス ポート アダプタ（WS-SVC-CMM-6E1）、および会議 / トランスコーディング ポート アダプタ（WS-SVC-CMM-ACT）です。表 19-3 は、互換性のあるポート アダプタの最小ソフトウェア要件をリストしています。

表 19-3　CMM ポート アダプタのソフトウェア要件

	WS-SVC-CMM-24FXS	WS-SVC-CMM-6T1	WS-SVC-CMM-6E1	WS-SVC-CMM-ACT
Cisco IOS リリース	12.3(8)XY	12.3(8)XY	12.3(8)XY	12.3(8)XY
CatOS リリース	7.3(1)	7.3(1)	7.3(1)	7.6.8
Native IOS リリース	12.1(15)E	12.1(14)E	12.1(13)E	12.1(13)E
CMM ごとの最大ポート アダプタ数	3	3	3	4

WS-X6624-FXS アナログ インターフェイス モジュール

Cisco WS-X6624-FXS アナログ インターフェイス モジュールは、高密度アナログ デバイスを IP テレフォニー ネットワークに接続するための MGCP ベースのデバイスで、24 個のアナログ ポートを提供します。

（注）　WS-X6624 FXS アナログ インターフェイスは販売終了になりました。

Cisco VG224 ゲートウェイ

Cisco VG224 アナログ ゲートウェイは、アナログ デバイスを IP テレフォニー ネットワークに接続するための、Cisco IOS の 24 ポート高密度ゲートウェイです。Cisco IOS Release 12.4(2)T 以降では、Cisco VG224 は、Cisco Unified CallManager 配下の Session Initiation Protocol（SIP）、Skinny Client Control Protocol（SCCP）、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）、または H.323 のエンドポイントとして動作して、フェールオーバーのシナリオでは Survivable Remote Site Telephone（SRST）ルータに「re-home」することができます。Cisco VG224 は、Cisco Unified CallManager Release 3.1 以降をサポートしています。また、Cisco VG224 は、モデム パススルー、モデム リレー、FAX パススルー、および FAX リレーもサポートしています。

Cisco VG248 ゲートウェイ

Cisco VG248 は、アナログ電話機、FAX マシン、モデム、スピーカーフォンのようなアナログ デバイスを企業の Cisco Unified CallManager（Release 3.1 以降）および音声ネットワークに接続するための、48 ポートの高密度 Skinny Client Control Protocol（SCCP）ゲートウェイです。また、Cisco VG248 は、Simplified Message Desk Interface（SMDI）、NEC Message Center Interface（MCI）、または Ericsson のボイスメール プロトコルと互換性があるレガシー ボイスメール システムおよび PBX との Cisco Unified CallManager の統合もサポートしています。Cisco VG248 は、Survivable Remote Site Telephone（SRST）へのフェールオーバーをサポートしています。

Cisco ATA 186 および 188

Cisco Analog Telephone Adaptor（ATA）186 または 188 は、IP テレフォニー ネットワークに 2 つのアナログ デバイスを接続でき、低密度アナログ デバイスを IP ネットワークに接続する場合に最適です。

Cisco ATA 186 と 188 の相違点は、前者には 10 Base-T イーサネット接続が 1 つしかないのに対し、後者には、自らの接続用と、共存する PC または他のイーサネットベース デバイスの接続用の 2 つの 10/100 Base-T イーサネット接続を提供する統合イーサネット スイッチがあることです。Cisco ATA 186 および 188 は、次のいずれかの方法で設定できます。

- Cisco ATA Web 設定ページ
- Cisco ATA 音声設定メニュー
- TFTP サーバからダウンロードした設定ファイル

SCCP ベースの ATA は、SCCP IP Phone のように動作します。別のエンドポイントから電話をかけられるように、Cisco ATA 186 または 188 を、SIP プロキシ サーバに登録された SIP クライアントとして設定することができます。Cisco ATA 186 または 188 は、SIP 要求を開始するときはユーザ エージェント クライアント（UAC）として、要求に応答するときはユーザ エージェント サーバ（UAS）として動作できます。Cisco Unified CallManager 5.0 には、Cisco ATA 186 または 188 に対するネイティブ SIP サポートはありません。

Cisco Unified IP Phone

Cisco IP Phone 製品には、ベーシック IP Phone、ビジネス IP Phone、マネージャ IP Phone、およびエグゼクティブ IP Phone があります。

Cisco ベーシック IP Phone

Cisco ベーシック IP Phone は、コール機能に制限があり、予算上の要求がある、トラフィック量の少ないユーザに最適です。ベーシック IP Phone には、Cisco Unified IP Phone 7902G、7905G、7911G、および 7912G があります。

Cisco Unified IP Phone 7902G

Cisco Unified IP Phone 7902G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。Cisco Unified IP Phone 7902G に液晶（LCD）画面はありません。Cisco Unified IP Phone 7902G は SCCP をサポートしていますが、SIP をサポートしていません。

Cisco Unified IP Phone 7905G

Cisco Unified IP Phone 7905G は単一回線をサポートし、電話機の背面に 1 つの 10 Base-T イーサネット ポートを備えています。スピーカーは、一方向のリッスン モードでのみ動作します。Cisco Unified IP Phone 7905G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

Cisco Unified IP Phone 7911G

Cisco Unified IP Phone 7911G は単一回線のみをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでのみ動作します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。Cisco Unified IP Phone 7911G は SCCP と SIP をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれのコール制御シグナリングを使用している場合でも一貫しています。

Cisco Unified IP Phone 7912G

Cisco Unified IP Phone 7912G は単一回線のみをサポートし、2 つの 10/100 Base-T イーサネット接続を備えています。スピーカーは、一方向のリッスン モードでのみ動作します。Cisco Unified IP Phone 7912G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。

（注） 最初のバージョンの Cisco Unified IP Phone 7912G は販売終了になりました。最初のバージョンの Cisco Unified IP Phone 7912G に代って、現在は Cisco Unified IP Phone 7912G-A があります。提供する機能は同一ですが、拡張イーサネット スイッチが備わりました。

Cisco ビジネス IP Phone

Cisco ビジネス IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度のトランザクション タイプの社員に最適です。ビジネス IP Phone には、Cisco Unified IP Phone 7940G、7941G、および 7941G-GE があります。

Cisco Unified IP Phone 7940G

Cisco Unified IP Phone 7940G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7940G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7940G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7940G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7940G にはビデオ サポートがありません。サポートされる機能の全リストについては、P.19-43 の「エンドポイント機能の要約」を参照してください。

Cisco Unified IP Phone 7941G

Cisco Unified IP Phone 7941G は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7941G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれのコール制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7941G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7941G は保留音をサポートしているのに対し、SIP はサポートしていません。サポートされる機能の全リストについては、P.19-43 の「エンドポイント機能の要約」を参照してください。

この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。

Cisco Unified IP Phone 7941G-GE

Cisco Unified IP Phone 7941G-GE は、最大 2 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7941G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco マネージャ IP Phone

Cisco マネージャ IP Phone は、スピーカーやヘッドセットなどの拡張コール機能を使用し、テレフォニー トラフィックの使用量が中程度から大量の、マネージャおよびアシスタントに最適です。マネージャ IP Phone には、Cisco Unified IP Phone 7960G、7961G、および 7961G-GE があります。

Cisco Unified IP Phone 7960G

Cisco Unified IP Phone 7960G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7960G は SCCP と SIP をサポートしていますが、この 2 つのコール シグナリング プロトコルで機能とユーザ インターフェイス（UI）に一貫性はありません。たとえば、SCCP を使用した Cisco Unified IP Phone 7960G はすべてのセキュリティ機能を備えていますが、SIP では以前に実装されていたセキュリティ機能を備えていません。SCCP を使用した Cisco Unified IP Phone 7960G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP を使用した Cisco Unified IP Phone 7960G にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7960G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。サポートされる機能の全リストについては、P.19-43 の「エンドポイント機能の要約」を参照してください。

Cisco Unified IP Phone 7961G

Cisco Unified IP Phone 7961G は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100 Base-T イーサネット接続を備えています。Cisco Unified IP Phone 7961G は SCCP と SIP をサポートする、Cisco Unified IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれのコール制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7961G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7961G は保留音をサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7961G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。サポートされる機能の全リストについては、P.19-43 の「エンドポイント機能の要約」を参照してください。

この電話機は高解像度の 4 ビット グレースケール ディスプレイを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポートに対応します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。

Cisco Unified IP Phone 7961G-GE

Cisco Unified IP Phone 7961G-GE は、最大 6 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7961G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

Cisco エグゼクティブ IP Phone

Cisco エグゼクティブ IP Phone は、拡張コール機能を使用する、トラフィック量の多い経営幹部ユーザに最適です。エグゼクティブ IP Phone には、Cisco Unified IP Phone 7970G および 7971G-GE があります。

Cisco Unified IP Phone 7970G

Cisco Unified IP Phone 7970G は、最大 8 つのディレクトリ番号の設定が可能で、高解像度のカラー タッチ スクリーンを備え、他の Cisco Unified IP Phone よりも多くのアクセス キーがあります。Cisco Unified IP Phone 7970G は SCCP と SIP の両方をサポートする、Cisco デスクトップ IP Phone の拡張アーキテクチャに含まれる電話機です。このアーキテクチャは、コール シグナリング プロトコルとは無関係に、Cisco デスクトップ IP Phone 間での機能と UI の一貫性を得るためのものです。サポートされる機能に関するエンドユーザの操作性は、SCCP または SIP のいずれのコール制御シグナリングを使用している場合でも一貫しています。

SCCP ではサポートされ、SIP ではサポートされない機能がいくつかあります。たとえば、SCCP を使用した Cisco Unified IP Phone 7970G は、ビデオ コールの発信に関して Cisco Unified Video Advantage ビデオ対応エンドポイントと互換性があるのに対し、SIP にはビデオ サポートがありません。SCCP を使用した Cisco Unified IP Phone 7970G は保留音をサポートしているのに対し、SIP はサポートしていません。SCCP を使用した Cisco Unified IP Phone 7970G は Cisco Unified IP Phone 拡張モジュール 7914 をサポートしているのに対し、SIP は拡張モジュールをサポートしていません。サポートされる機能の全リストについては、P.19-43 の「エンドポイント機能の要約」を参照してください。

Cisco Unified IP Phone 7970G には高解像度のカラー タッチ スクリーンを備え、機能の使用方法や Extensible Markup Language（XML）アプリケーションの拡張、およびダブル バイト言語のサポート化に対応します。電源は、IEEE 802.3af、Cisco インライン パワー、または電源アダプタ（CP-PWR-CUBE-3）によるローカル電源で供給します。Cisco Unified IP Phone 7970G で画面の輝度を最大にするには、Cisco インライン パワーと IEEE 802.3af Power over Ethernet（PoE）のどちらの場合も、外部電源アダプタ（CP-PWR-CUBE-3）を使用する必要があります。

Cisco 7971G-GE

Cisco Unified IP Phone 7971G-GE は、最大 8 つのディレクトリ番号の設定が可能で、2 つの 10/100/1000 Base-T イーサネット接続を備えている点を除いて、Cisco Unified IP Phone 7970G と同等です。ギガビット スループット機能の追加により、共存する PC 上の高ビット レートで広い帯域幅を必要とするアプリケーションに対応します。

（注） アクセス スイッチからのインライン パワー、またはローカルの壁面コンセントからの電源供給に加えて、Cisco Unified IP Phone では、パワー インジェクタ Promax による電源供給も可能です。Promax を使用すると、インライン パワーをサポートしない Cisco スイッチまたは Cisco 以外のスイッチに、Cisco Unified IP Phone を接続できます。Promax は、すべての Cisco Unified IP Phone と互換性があり、Cisco PoE と IEEE 802.3af PoE の両方をサポートしています。2 つの 10/100/1000 Base-T イーサネット接続を備え、一方をスイッチのアクセス ポートに接続し、もう一方を Cisco Unified IP Phone に接続します。

Cisco Unified IP Phone 拡張モジュール 7914

Cisco Unified IP Phone 拡張モジュール 7914 は、電話機の現在の回線容量を超える多数の回線の状態を確認する必要があるアシスタントなどに適しています。

Cisco Unified IP Phone 拡張モジュール 7914 は追加のボタンと LCD によって、Cisco Unified IP Phone 7960G、7961G、7961G-GE、7970G、または 7971G-GE の機能を拡張します。Cisco Unified IP Phone 拡張モジュール 7914 ではモジュールあたり 14 個のボタンが提供されます。Cisco Unified IP Phone 796*x*G および 797*x*G は、最大で 2 つの Cisco Unified IP Phone 拡張モジュールをサポートできます。IP Phone で Cisco インライン パワーまたは IEEE802.3af PoE を使用している場合には、Cisco Unified IP Phone 拡張モジュール 7914 に外部電源アダプタ（CP-PWR-CUBE-3）を使用する必要があります。

ソフトウェアベースのエンドポイント

ソフトウェアベースのエンドポイントには、Cisco IP Communicator および Cisco IP SoftPhone があります。ソフトウェアベースのエンドポイントは、クライアント PC にインストールされたアプリケーションであり、登録と制御は Cisco Unified CallManager で行います。

Cisco IP Communicator

Cisco IP Communicator は、コンピュータに IP Phone 機能を与える Microsoft Windows ベースのアプリケーションです。このアプリケーションを使用すると、出張中やオフィス内など、企業ネットワークにユーザがどこからアクセスする場合でも高品質の音声コールが可能になります。リモートユーザと在宅勤務者にとって最適なソリューションです。Cisco IP Communicator は配置が簡単で、現在 IP 通信で利用可能な最新テクノロジーや先端機能のいくつかが採用されています。この項では、Cisco Unified CallManager と一緒に Cisco IP Communicator を使用する場合に適用される、次の設計上の考慮事項について説明します。

- IP Communicator の最大設定の制限（P.19-11）
- コーデックの選択（P.19-11）
- コール アドミッション制御（P.19-12）

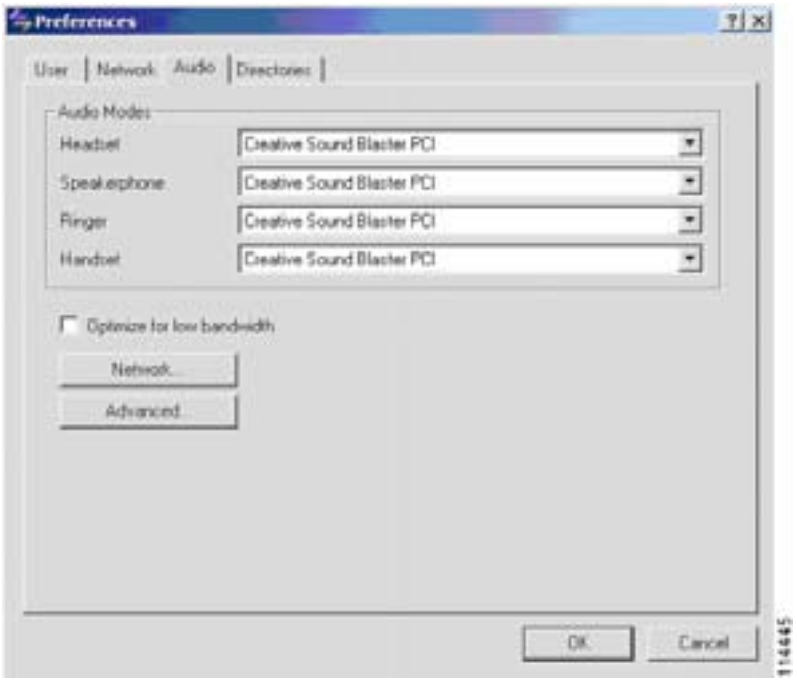
IP Communicator の最大設定の制限

Cisco IP Communicator は SCCP スタンドアロン デバイスであるため、さまざまな IP テレフォニー配置モデルに含まれる IP Phone の設計に関するガイドラインは、Cisco IP Communicator にも当てはまります。詳細については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

コーデックの選択

Cisco IP Communicator は、G.711 および G.729a コーデックをサポートします。コーデックを選択するには、Cisco IP Communicator が配置されているリージョンを設定します。G.729a 低帯域幅コーデック設定は、Cisco IP Communicator を WAN 経由で接続する在宅勤務者の環境に配置することをお勧めします。Cisco IP Communicator にも、G.711 リージョン内の低帯域幅コーデックを上書きする機能があります。この機能を有効にするには、Audio 設定ウィンドウの Optimize for Low Bandwidth オプション チェックボックスをオンにします（図 19-1 を参照）。ここでは、Cisco IP Communicator は、G.729 コーデックを使用して、同じリージョン内の別の電話機とのコールをセットアップします。

図 19-1　Cisco IP Communicator のオーディオ設定



コール アドミッション制御

コール アドミッション制御により、ネットワークを介した IP Phone コールの処理に使用可能な帯域幅が十分確保されます。コール アドミッション制御の実装には複数のメカニズムがありますが、Cisco IP Communicator は、集中型コール処理配置用として Cisco Unified CallManager で設定されるロケーション メカニズムを使用したり、非集中型コール処理配置用に RSVP メカニズムを使用したりします。Cisco Unified CallManager のロケーションを使用したコール アドミッション制御の詳細については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

ロケーションと RSVP ベースのコール アドミッション制御は、Cisco IP Communicator が単一の Cisco Unified CallManager ロケーション内でモバイルとして使用されている限り、コール帯域幅の管理で有効です。ただし、Cisco IP Communicator が複数の Cisco Unified CallManager ロケーション間を移動すると、コール アドミッション制御が問題の原因になる場合があります。詳細については、P.19-20 の「デバイス モビリティおよび Cisco Unified CallManager」を参照してください。

Cisco IP SoftPhone

この項では、Cisco Unified CallManager と一緒に Cisco IP SoftPhone を使用する場合に適用される、次の設計上の考慮事項について説明します。

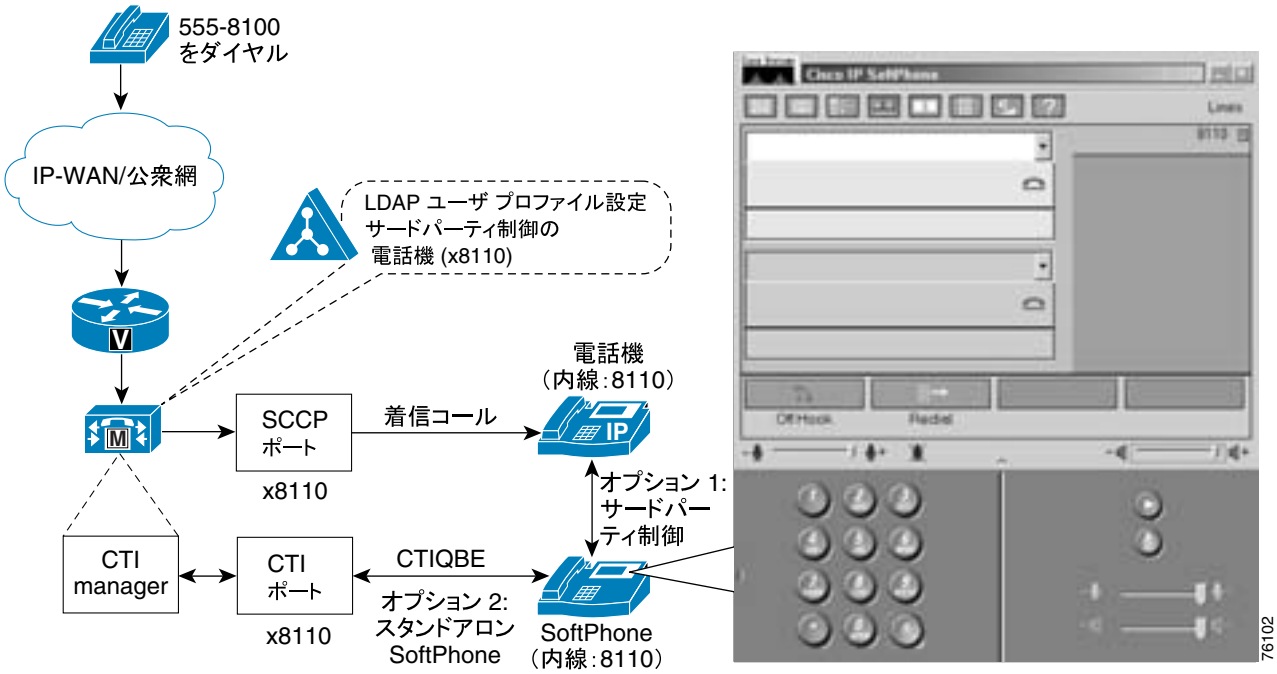
- Cisco IP SoftPhone の最大設定の制限（P.19-13）
- コーデックの選択（P.19-14）
- コール アドミッション制御（P.19-15）

この項の情報は、Cisco IP SoftPhone Release 1.3 に明示的に適用されます。Cisco IP SoftPhone の設定と機能の詳細は、次の Web サイトでオンラインで入手可能な『*Cisco IP Softphone Administrator Guide (1.3)*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/english/softphon/index.htm

図 19-2 では、Cisco IP SoftPhone アプリケーションが、関連付けられたハードウェア IP Phone をモニタまたは制御できることを示しています。サードパーティ制御の電話機の場合、Cisco IP SoftPhone は、デスクトップ IP Phone の仮想内線電話の役目をします。Cisco IP SoftPhone アプリケーションは、ハードウェア電話機の着信コールと発信コールを表示し、処理できます。デバイスと CTI リソースのプロビジョニングの観点から見ると、この設定を使用する各ユーザは、サードパーティ制御の IP Phone として設定されます。CTI ポートとしての Cisco IP SoftPhone は、デスクトップ電話機で追加の制御やモニタリングをすることなく、クライアント マシンへのコールを直接処理する専用回線です。

図 19-2　Cisco IP SoftPhone のデバイスの関連付けオプション



Cisco IP SoftPhone は、CTI ポートとサードパーティ制御の電話機を、同じディレクトリ番号 (DN) で同時に実行することはできません。図 19-2 に示されているように、ユーザは、CTI ポート、またはデスクトップ電話機の制御として、内線 8110 を使用できます。

デバイスおよびリソース プロビジョニングの詳細については、P.8-1 の「コール処理」の章を参照してください。

Cisco IP SoftPhone の最大設定の制限

サーバごとに許可されるデバイスの制限とは関係なく、Cisco Unified CallManager で設定できる最大 CTI デバイス数に制限があります。Cisco IP SoftPhone に適用される CTI デバイスの制限は、次のとおりです。

- Cisco Media Convergence Server（MCS）7825 または 7835 の場合、1 台あたり最大 800 台の Cisco IP SoftPhone。MCS 7825s または 7835s の場合、1 台あたり最大 3,200 台の Cisco IP SoftPhone。
- MCS 7845 の場合、1 台あたり最大 2,500 台の Cisco IP SoftPhone。MCS 7845s の場合、1 台あたり最大 10,000 台の Cisco IP SoftPhone。

上記の Cisco IP SoftPhone の最大限度には、次の前提が適用されます。

- 各 Cisco IP SoftPhone は、1 つのライン アピアランスで設定されます。
- 各 Cisco IP SoftPhone は、見積もりで 6 コール以下の Busy Hour Call Attempt（BHCA）を処理します。
- CTI デバイスを必要とする他の CTI アプリケーションが、その Cisco Unified CallManager クラスタで設定されていません。

コーデックの選択

Cisco IP SoftPhone は、G.711、G.723、および G.729a の各コーデックをサポートします。G.729a 低帯域幅コーデック設定は、Cisco IP SoftPhone を WAN 経由で接続する在宅勤務者の環境に配置することをお勧めします。

Cisco Unified CallManager が G.723 コーデックをサポートしていないため、Cisco IP Softphone で使用する帯域幅コーデック設定は 2 つです。デフォルト設定は G.711 で、ユーザがオプションを設定することにより、TAPI Service Provider（TSP）クライアント上で低帯域幅コーデック設定 G.729 を選択できます（図 19-3 を参照）。ネットワーク帯域幅のプロビジョニングの詳細については、P.3-1 の「ネットワーク インフラストラクチャ」の章を参照してください。

図 19-3　Cisco IP Softphone のオーディオ設定

WAN を介した低帯域幅の接続を使用する Cisco IP SoftPhone のユーザは、この低帯域幅の G.729 コーデック設定の選択を検討する必要があります。

コール アドミッション制御

コール アドミッション制御により、ネットワークを介した IP Phone コールの処理に使用可能な帯域幅が十分確保されます。コール アドミッション制御の実装には複数のメカニズムがありますが、Cisco IP SoftPhone は、集中型コール処理配置用として Cisco Unified CallManager で設定されるロケーション メカニズムを使用したり、非集中型コール処理配置用にリソース予約プロトコル（RSVP）を使用したりします。Cisco Unified CallManager のロケーションを使用したコール アドミッション制御の詳細については、P.2-1 の「IP テレフォニー配置モデル」の章を参照してください。

ロケーションと RSVP ベースのコール アドミッション制御は、Cisco IP SoftPhone が単一の Cisco Unified CallManager ロケーション内でモバイルとして使用されている限り、コール帯域幅の管理で有効です。ただし、Cisco IP SoftPhone が複数の Cisco Unified CallManager ロケーション間を移動すると、コール アドミッション制御が問題の原因になる場合があります。詳細については、P.19-20 の「デバイス モビリティおよび Cisco Unified CallManager」を参照してください。

無線エンドポイント

Cisco 無線エンドポイントは、無線アクセス ポイント（AP）経由で無線 LAN（WLAN）インフラストラクチャを使用して、テレフォニー機能を提供します。このタイプのエンドポイントは、エリア内でモバイル ユーザの必要性がある環境で、従来の有線電話では不適切であったり問題が生じたりする場合に理想的です（無線ネットワークの設計の詳細については、P.3-62 の「無線 LAN インフラストラクチャ」を参照してください）。

Cisco Unified Wireless IP Phone 7920 は、ネットワークへの 802.11b 無線 LAN 接続を可能にする組み込み型の無線アンテナを備えた、ハードウェアベースの電話機です。これらの電話機は、他のハードウェアベースの電話機や Cisco IP Communicator と同様、Skinny Client Control Protocol（SCCP）を使用して Cisco Unified CallManager に登録されます。詳細については、次の Web サイトで入手可能な『*Cisco Unified Wireless IP Phone 7920 Design and Deployment Guide*』を参照してください。

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

サイト調査

Cisco Unified Wireless IP Phone 7920 を配置する前に、完全なサイト調査を実行して、無線周波数（RF）カバレッジを提供するのに最適な AP の数と場所を判別する必要があります。サイト調査では、最適なカバレッジを提供するアンテナ タイプや RF 干渉の送信元が存在している可能性がある場所を考慮する必要があります。サイト調査では、Cisco Unified Wireless IP Phone 7920 の Site Survey ツール（**Menu** > **Network Config** > **Site Survey** からアクセス）、およびラップトップまたは PC の Cisco Aironet NIC カードと共に使用する Aironet Client Utility Site Survey ツールを使用する必要があります。追加のサードパーティ ツールもサイト調査で使用できますが、アンテナの感度と調査アプリケーションの制限によって各エンドポイントまたはクライアント無線の動作が異なるため、Cisco Unified Wireless IP Phone 7920 を使用して最終サイト調査を実行することを強くお勧めします。

認証

Cisco Unified Wireless IP Phone 7920 を無線ネットワークに接続するには、最初に次のいずれかの認証方法を使用して、AP に関連付けて通信する必要があります。

- Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST）

  この方法では、クライアントと EAP 準拠のリモート認証、認可、アカウンティングのサーバとの間に Protected Access Credential（PAC）でセキュア認証トンネルが確立されると、Cisco Unified Wireless IP Phone 7920 をユーザ名とパスワードで AP に対し 802.1X で認証できます。認証時、無線デバイスとの間のトラフィックは TKIP または WEP を使用して暗号化されます。802.1X 認証方式および PAC 認証トンネル交換を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Wi-Fi Protected Access（WPA）

  この方法では、ユーザ名とパスワードによって、Cisco Unified Wireless IP Phone 7920 を AP に対し 802.1X で認証できます。認証時、無線デバイスとの間のトラフィックは Temporal Key Integrity Protocol（TKIP）を使用して暗号化されます。802.1X 認証方式を使用するには、Cisco Secure Access Control Server（ACS）など、EAP 準拠の Remote Authentication Dial-In User Service（RADIUS）認証サーバが必要です。このサーバは、ユーザ データベースへのアクセスを提供します。

- Wi-Fi Protected Access Pre-Shared Key (WPA-PSK)

  この方法では、Cisco Unified Wireless IP Phone 7920 および AP 上の共有鍵の設定により、Cisco Unified Wireless IP Phone 7920 を AP に対し認証できます。認証時、無線デバイスとの間のトラフィックは TKIP を使用して暗号化されます。この認証方法は、企業での配置には推奨しません。

- Cisco Centralized Key Management（Cisco CKM）

  この方法では、ユーザ名とパスワードによって、Cisco Unified Wireless IP Phone 7920 を AP に対して 802.1x で認証できます。認証時、無線デバイスとの間のトラフィックは WEP 128 または TKIP を使用して暗号化されます。802.1X 認証方法には、Cisco ACS などの EAP 準拠の RADIUS 認証サーバが必要です。このサーバは、最初の認証要求のためにユーザ データベースへのアクセスを提供します。以降の認証要求は、AP において無線ドメイン サービス（WDS）によって検証されるため、再認証時間が短縮され、高速で安全なローミングが保証されます。

- Cisco LEAP

  この方法では、ユーザ名とパスワードに基づいて、Cisco Unified Wireless IP Phone 7920 と AP を相互に認証できます。認証時に動的な鍵が生成され、Cisco Unified Wireless IP Phone 7920 と AP の間のトラフィックの暗号化に使用されます。ユーザ データベースへのアクセスを提供するため、Cisco Secure Access Control Server（ACS）などの、LEAP 準拠の Radius 認証サーバが必要です。

- 共有鍵

  この方法では、Cisco Unified Wireless IP Phone 7920 と AP に、静的な 10 文字（40 ビット）または 26 文字（128 ビット）の鍵を設定します。この方法は AP ベースの認証方法で、一致する鍵がデバイスに存在する場合にネットワークへのアクセスが許可されます。

- Open 認証

  この方法では、Cisco Wireless IP Phone 7920 と AP の間で、識別情報を交換する必要はありません。この方法では音声またはシグナリングの安全な交換が提供されず、偽装したデバイスを AP に関連付けることができるため、この方法はお勧めしません。

キャパシティ

各 AP は、最大で 7 つのアクティブな G.711 音声ストリームまたは 8 つの G.729 ストリームをサポートできます。これらの数を超えると、音声パケットのドロップや遅延、またはコールのドロップが原因で、品質が低下する場合があります。AP レートが 11 Mbps より低く設定されている場合、各 AP のコール キャパシティが低下します。

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

これらのアクティブ コール キャパシティの限界と Erlang 比率に基づいて、各 AP がサポートできる Cisco Unified Wireless IP Phone 7920 の数を計算できます。たとえば、標準的なユーザ対コールのキャパシティ比率を 3:1 と想定すると、使用するコーデックが G.711 か G.729 かに応じて、1 つの AP で 21 ～ 24 台の Cisco Unified Wireless IP Phone 7920 をサポートできます。ただし、この数には、他の Cisco Unified Wireless IP Phone 7920 がこの AP にローミングする可能性は加味されていません。現実的には、AP あたりの電話機の数は上記の数より少なくなります。

VLAN またはレイヤ 2 サブネットあたりの AP の数も考慮する必要があります。AP のメモリおよびパフォーマンスを最適化するには、1 つの VLAN またはサブネットに、30 を超える数の AP を配置しないことをお勧めします。標準的なユーザ対コールのキャパシティ比率を適用すると、レイヤ 2 サブネットあたりの Cisco Unified Wireless IP Phone 7920 の数は、概算で 500（または AP あたり 15 ～ 17 の Cisco Unified Wireless IP Phone 7920）に制限されます。

これらのキャパシティは、音声アクティビティ検出（VAD）が無効で、パケット化のサンプル サイズが 20 ミリ秒（ms）であると想定して計算されました。VAD とは、コール中に音声が発生しないときに RTP パケットを送信しないことにより、帯域幅を節約するメカニズムです。ただし、VAD の有効化または無効化は、Cisco Unified CallManager で、クラスタ全体のグローバル設定パラメータで設定します（Cisco Unified CallManager では無音圧縮と呼ばれます）。このため、Cisco Unified Wireless IP Phone 7920 で VAD を有効にすると、VAD は Cisco Unified CallManager クラスタ内のすべてのデバイスで有効になります。全体の音声品質を良好に保つため、VAD（無音圧縮）を *disabled* のままにすることをお勧めします。

サンプリング レートを 20 ms に設定すると、片方向の音声コールで 50 パケット / 秒（pps）が生成されます。通常は、サンプル レートを 20 ms に設定するようにお勧めします。それより大きいサンプル サイズ（30 または 40 ms）を使用すると、AP あたりの同時コールの数を増分できますが、エンドツーエンドの遅延も大きくなります。また、サンプル サイズを大きくすると、1 つのパケットが失われたときに欠落する会話の量が大きくなるので、無線環境で許容される音声パケットの損失率は大幅に減少します。音声サンプリング サイズの詳細については、P.3-48 の「帯域幅のプロビジョニング」を参照してください。

電話機設定

Cisco Unified Wireless IP Phone 7920 は、電話機のキーパッド、または USB ケーブルで電話機に接続された PC で実行する 7920 設定ユーティリティのいずれかを使用して設定できます。いずれの場合も、次のパラメータを設定する必要があります。

- ネットワーク設定

  ネットワークの必要に応じて、DHCP サーバ アドレスを指定するか、IP アドレス、サブネット マスク、デフォルト ゲートウェイ、TFTP サーバ、DNS サーバなどの静的設定を設定します。Cisco Unified Wireless IP Phone 7920 では、これらの設定は **Menu** > **Profiles** > **Network Profile** にあります。
- 無線設定

  音声 VLAN の Service Set Identifier（SSID）および認証タイプを設定します。必要に応じて、WEP 鍵、LEAP ユーザ名、およびパスワードを設定してください。Cisco Unified Wireless IP Phone 7920 では、これらの設定は **Menu** > **Profiles** > **Network Profile** にあります。

ローミング

現在、Cisco Unified Wireless IP Phone 7920 は、レイヤ 2（同一の VLAN またはサブネット内）にローミングし、引き続きアクティブなコールを保持できます。

レイヤ 2 ローミングは、次の状況で発生します。

- Cisco Unified Wireless IP Phone 7920 の初期ブートアップ中に、電話機は初めて新しい AP にローミングします。
- Cisco Unified Wireless IP Phone 7920 が、現在関連付けられている AP からビーコンまたは応答を受信しない場合、電話機は現在の AP が使用不可であると想定し、新しい AP へのローミングと関連付けを試行します。
- Cisco Unified Wireless IP Phone 7920 は、適格な AP ローミング ターゲットのリストを保持します。現在の AP の状態が変更されると、電話機は、使用可能な AP ローミング ターゲットのリストを参照します。ローミング ターゲットの 1 つが、より適切な選択肢であると判別された場合、電話機はその新しい AP にローミングします。
- Cisco Unified Wireless IP Phone 7920 の設定済みの SSID または認証タイプが変更された場合、電話機は AP にローミングして再度関連付けする必要があります。

レイヤ 2 ローミングで適格な AP ローミング ターゲットの判別を試行するとき、無線 IP Phone は、次の変数を使用して、関連付ける最適な AP を判別します。

- Relative Signal Strength Indicator（RSSI）

  無線 IP Phone が、シグナルの長さと、RF カバレッジ エリア内で使用可能な AP の品質を判別するときに使用されます。電話機は、RSSI 値が最高で、認証 / 暗号化タイプが一致する AP との関連付けを試行します。

- QoS Basic Service Set（QBSS）

  AP が、チャネル利用率情報を無線電話機に通信するのを可能にします。チャネル利用率が高い AP は VoIP トラフィックを効率的に処理できない場合があるので、電話機は、QBSS 値を使用して、別の AP へのローミングを試行する必要があるかどうかを判別します。

無線 IP Phone のレイヤ 2 ローミング時間は、使用される認証タイプによって異なります。電話機と AP の間の認証で静的な WEP 鍵が使用されている場合、レイヤ 2 ローミングは、100 ms 未満で実行されます。LEAP（ローカルの Cisco Secure ACS 認証を使用）が使用されている場合、レイヤ 2 ローミングは 200 ～ 400 ms で実行されます。Cisco Centralized Key Management（Cisco CKM）を使用すると、ローミング時間を 100 ms 未満に短縮できます。

デバイスがレイヤ 3 で移動する場合、デバイスはネイティブ VLAN の境界を越えて AP から別の AP に移動します。Cisco Catalyst 6500 シリーズ ワイヤレス LAN サービス モジュール（WLSM）によって、Cisco Unified Wireless IP Phone 7920 は、アクティブ コールを維持しながらレイヤ 3 でローミングできます。Cisco Wireless IP Phone 7920 は、静的 WEP または Cisco CKM プロトコルを使用して、レイヤ 3 でローミングできます。Cisco CKM を使用すると、電話機は WEP 128 または TKIP 暗号化を使用しながら、完全なレイヤ 3 モビリティを実現できます。シームレスなレイヤ 3 ローミングが行われるのは、クライアントが同じモビリティ グループ内でローミングする場合だけです。Cisco WLSM およびレイヤ 3 ローミングの詳細については、次の Web サイトで入手可能な製品資料を参照してください。

http://www.cisco.com

ワイヤレス LAN で 802.1x 認証を使用している場合は、ローミングのダウンタイムを最小にするため、Cisco CKM をお勧めします。レイヤ 2 またはレイヤ 3 のどちらでローミングする場合も、デバイスのダウンタイムが 300 ～ 400 ms から 100 ms 未満に減少します。Cisco CKM は、ACS に送信する必要がある認証要求の数を減らすことによって、ACS の負荷も軽減します。

AP コール アドミッション制御

Cisco Unified CallManager またはゲートキーパー内のコール アドミッション制御メカニズムは、WAN 帯域幅の利用率を制御し、既存のコールの QoS を提供できますが、どちらのメカニズムも、コールの開始時にしか適用されません。静的なデバイス間のコールでは、このタイプのコール アドミッション制御で十分です。しかし、Cisco Unified Wireless IP Phone 7920 などの 2 つのモバイル無線デバイス間のコールの場合、無線デバイスが 1 つの AP から別の AP へと順にローミングする可能性があるので、AP レベルにもコール アドミッション制御メカニズムが必要です。

コール アドミッション制御用の AP メカニズムは QBSS です。AP は、このビーコン情報エレメントを使用して、チャネル利用率情報を無線 IP Phone に通信できます。前述のとおり、電話機はこの QBSS 値を使用して、別の AP にローミングする必要があるかどうかを判別します。QBSS 値が低いと、その AP がローミング先として適切な候補であることを示し、QBSS 値が高いと、電話機がその AP にローミングするべきでないことを示しています。

この QBSS 情報は便利ですが、ローミング中、コールが適切な QoS を保持することを保証するものではありません。Cisco Unified Wireless IP Phone 7920 が、高い QBSS を持つ AP に関連付けられている場合、AP は、コールのセットアップを拒否し、発信側の電話機に Network Busy メッセージを送信することにより、コールが開始または受信されるのを防止します。しかし、無線 IP Phone と別

のエンドポイントの間でコールがセットアップされた後は、電話機が、高い QBSS を持つ AP にローミングして関連付けを行うことができ、それによりその AP で使用可能な帯域幅のオーバーサブスクリプションが発生する場合があります。

デバイス モビリティおよび Cisco Unified CallManager

無線 IP Phone をモバイル デバイスとして使用し、1 つのロケーションから別のロケーションに移動する場合、次の問題が発生することがあります。

- Cisco Unified CallManager のロケーションベースのコール アドミッション制御用には不正確な帯域幅計算

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco Unified CallManager には、コール アドミッション制御のために電話機のロケーションを動的に更新するメカニズムはありません。そのため、実際には帯域幅を使用していないロケーションから帯域幅が差し引かれ、他のロケーションで使用可能な帯域幅がロケーションベースのコール アドミッション制御の計算に含まれない事態が生じ、WAN 帯域幅のオーバーサブスクリプションが発生する場合があります。
- 不適切なコーデックの選択

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco Unified CallManager には、コーデック タイプを判別するためにリージョンまたはデバイス プールを動的に更新するメカニズムはありません。そのため、不正なコーデックがテレフォニー ネットワーク全体で使用される場合があります。
- 不適切な公衆網ゲートウェイの選択

  無線 IP Phone が 1 つのロケーションから別のロケーションに順にローミングする場合、現在、Cisco Unified CallManager には、ローカル公衆網ゲートウェイを指定するためにダイヤル プランを動的に更新するメカニズムはありません。そのため、無線 IP Phone が、公衆網アクセス用のリモート公衆網ゲートウェイを使用する場合があります。無線 IP Phone がこのリモート公衆網ゲートウェイを使用して緊急の 911 コールをかける場合、緊急サービスは、リモート公衆網ゲートウェイのロケーションに転送され、コールを開始した無線 IP Phone のロケーションには転送されません。

（注） Cisco Emergency Responder（ER）が配置されている場合、911 コールは、ローカル公衆網ゲートウェイ、および適切な Public Safety Answering Point（PSAP）に転送されます。ただし、コール アドミッション制御は依然としてこのコールで使用される帯域幅を把握しておらず、不正なコーデックが選択される場合があります。

これらのデバイス モビリティ問題を防止するには、電話機が 1 つのロケーションから別のロケーションに物理的に移動するたびに、Cisco Unified CallManager で、次の無線 IP Phone のパラメータを手動で再設定する必要があります。

- コール アドミッション制御のロケーション
- デバイス プールおよびリージョン
- コーリング サーチ スペース

これらのパラメータは、無線 IP Phone の移動先のロケーションごとに適切に調整する必要があります。拡張機能や非標準の機能が必要な場合、状況によっては、他のパラメータを手動で再設定する必要があります。たとえば、ローカル メディア リソースが使用されており、各ロケーションで自動代替コール ルーティングが適切であることを確認するため、メディア リソース グループ リスト（会議、トランスコーディング、および Music-on-Hold リソース用）、および Automated Alternate Routing（AAR）コーリング サーチ スペースおよびグループ（AAR が設定されている場合）を再設定する必要があります。

デバイス モビリティに関するこれらの問題は、無線 IP Phone だけではなく、ロケーション間を移動するすべてのデバイスに当てはまります。これらのデバイスには、Cisco IP SoftPhone、Cisco IP Communicator、および 1 つの場所から別の場所に物理的に移動するすべての Cisco ハードウェア IP Phone が含まれます。

最後に、デバイス モビリティに関するこれらの問題は、集中型と分散型の両方のコール処理配置に影響します。

Cisco IP Conference Station

Cisco IP Conference Station は、会議室のスピーカーフォン テクノロジーと、Cisco Unified Communications テクノロジーを結合します。Cisco IP Conference Station は、360 度の室内カバレッジを提供する会議環境に最適です。

Cisco Unified IP Conference Station 7936 は、外部スピーカー 1 つと組み込み型のマイク 3 つを備えています。Cisco Unified IP Conference Station 7936 には、Cisco CallManager Release 3.3（3）SR3 以降が必要です。Cisco Unified IP Conference Station 7936 は、バックライト付きのピクセルベース LCD 画面も備えています。大きな部屋でマイクのカバレッジを拡張するため、オプションの拡張マイクも接続できます。

ビデオ エンドポイント

Cisco Unified CallManager Release 5.0 は、次のタイプのビデオ対応エンドポイントをサポートしています。

- Skinny Client Control Protocol（SCCP）を実行している Cisco Unified IP Phone 7940、7941、7960、7961、7970、または 7971 に関連付けられた Cisco Unified Video Advantage
- Cisco IP Video Phone 7985
- SCCP を実行している Tandberg 社製 2000 MXP、1500 MXP、1000 MXP、770 MXP、550 MXP、T-1000、または T-550 モデル
- SCCP を実行している Sony 社製 PCS-1、PCS-TL30、または PCS-TL50 モデル
- H.323 および SIP クライアント（Polycom、Sony、PictureTel、EyeBeam、Tandberg、VCON、VTEL、Microsoft NetMeeting など）

SCCP ビデオ エンドポイント

SCCP ビデオ エンドポイントは、Cisco Unified CallManager に直接登録し、Trivial File Transfer Protocol（TFTP）でその設定をダウンロードします。サポートされる多くの機能および補足サービスとしては、保留、転送、会議、パーク、ピックアップとグループ ピックアップ、Music On Hold、シェアドライン アピアランス、マッピング可能ソフトキー、自動転送（busy、no answer、unconditional）などがあります。

Cisco Unified Video Advantage

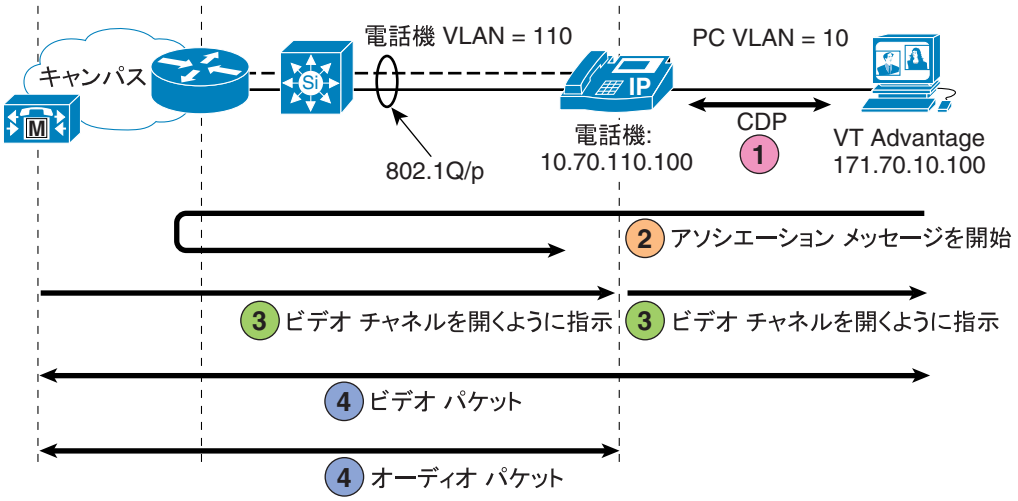
Cisco Unified Video Advantage は、Windows 2000 または Windows XP パーソナル コンピュータにインストール可能な Windows ベースのアプリケーションと USB カメラで構成されています。Skinny Client Control Protocol を実行している Cisco Unified IP Phone 7940、7941、7960、7961、7970、または 7971 の PC ポートに PC を物理的に接続すると、Cisco Unified Video Advantage アプリケーションは電話機と「アソシエーション」を行い、それによってユーザはいつもの電話操作が可能になり、ビデオ機能も追加されます。

システム管理者は、このアソシエーションをどの IP Phone に許可するかを制御するために、Cisco Unified CallManager Administration の IP Phone 設定ページで **Video Capabilities: Enabled/Disabled** 設定の切り替えを行います。この機能を有効にすると、カメラを表すアイコンが IP Phone ディスプレイの右下に表示されます。デフォルトでは、Cisco Unified Video Advantage は無効になっています。Bulk Administration Tool を使用すると、この設定を多数の電話機で一度に修正することもできます。注意する点としては、Cisco Unified Video Advantage が動作するには **PC Port: Enabled/Disabled** 設定も有効にする必要がありますが、**PC Access to Voice VLAN** 設定を有効にする必要はありません。

上記のアソシエーションのために、Cisco Unified Video Advantage は Cisco Discovery Protocol（CDP; シスコ検出プロトコル）ドライバを PC のイーサネット インターフェイスにインストールします。CDP を使用すると、PC と IP Phone は相互に自動検出できるようになります。このため、Cisco Unified Video Advantage を動作させるために、ユーザは PC または IP Phone 上で何も設定する必要はありません。したがって、ユーザがビデオ対応 IP Phone に PC を差し込めば、自動的にアソシエーションが行われます（図 19-4 を参照）。

（注） Cisco Unified Video Advantage をインストールすると、CDP パケット ドライバが PC のすべてのイーサネット インターフェイスにインストールされます。新しい Network Interface Card（NIC; ネットワーク インターフェイス カード）を追加するか、古い NIC を新しいものと置き換えたときは、Cisco Unified Video Advantage を再インストールして、CDP ドライバが新しい NIC にもインストールされるようにしてください。

図 19-4　Cisco Unified Video Advantage の動作の概要



1. 電話機と PC が CDP メッセージを交換します。電話機は CDP ネイバーの IP アドレスから TCP ポート 4224 で PC アソシエーション パケットの監視を開始します。
2. PC は TCP/IP を介して電話機に対するアソシエーション メッセージを開始します。アソシエーション パケットは VLAN 間の レイヤ 3 境界までルーティングされます。ファイアウォールまたは ACL（あるいはその両方）で TCP ポート 4224 を許可する必要があります。
3. 電話機は VT Advantage とCisco CallManager の間で SCCP プロキシとして機能します。Cisco CallManager はコールごとにビデオ チャネルを開くように電話機に指示し、電話機は PC に対するメッセージをプロキシします。
4. 電話機はオーディオを送受信し、PC はビデオを送受信します。オーディオとビデオは DSCP AF41 とマーキングされます。ビデオは UDP ポート 5445 にあります。

119453

Cisco Unified Video Advantage を使用したコールの発信では、オーディオは IP Phone で処理されますが、ビデオは PC で処理されます。2 台のデバイス間に同期メカニズムが存在しないため、ジッタ、遅延、断片化パケット、および不良パケットを最小限に抑えるために QoS が不可欠です。

IP Phone は音声 VLAN 内に存在しますが、PC はデータ VLAN 内に存在します。つまり、アソシエーションが行われるために、レイヤ 3 のルーティング パスが音声 VLAN とデータ VLAN の間に必要です。これらの VLAN の間に Access Control List（ACL; アクセス コントロール リスト）またはファイアウォールがある場合は、アソシエーション プロトコル（両方向で TCP ポート 4224 を使用）の通過を許可するように設定する必要があります。

Cisco Unified Video Advantage は、Differentiated Services Code Point（DSCP）によるトラフィックの分類をサポートしています。Cisco Unified CallManager は、電話機に送信する SCCP メッセージに DSCP 値を指定します。オーディオのみのコールの発信時に IP Phone は、SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィックに DSCP EF とマーキングします。ただし、ビデオ コールの発信時には、IP Phone は SCCP 制御トラフィックに DSCP CS3、オーディオ RTP メディア トラフィックに DSCP AF41 とマーキングし、Cisco Unified Video Advantage アプリケーションからはビデオ RTP メディア トラフィックにも DSCP AF41 とマーキングされます。IP Phone と Cisco Unified Video Advantage アプリケーションの両方が「アソシエーション」プロトコル メッセージに DSCP CS3 とマーキングするのは、それがシグナリング トラフィックであると考慮され、SCCP など、他のすべてのシグナリング トラフィックと一緒にグループ分けされるためです。

(注) Cisco Unified CallManager Release 4.0 では、Cisco Unified IP Phone 7970 および 7971 にセキュリティ機能が追加されました。これによって、Transport Layer Security（TLS）および Secure RTP（SRTP）を使用して、シグナリング トラフィックとオーディオ メディア トラフィックの認証と暗号化が可能です。アソシエーション プロトコルでは、この認証または暗号化が使用されることはなく、ビデオ RTP メディア ストリームが暗号化されることもありません。ただし、SCCP シグナリングとオーディオ RTP メディア ストリームは、暗号化が設定されていれば暗号化されます。

(注) 音声 VLAN をデータ VLAN と同じ設定にしないでください。接続に問題が起きる可能性があります。

考慮すべき点として、Cisco Unified Video Advantage は、PC 上で実行する他のアプリケーションと同様に、システム パフォーマンスに実際に影響します。Cisco Unified Video Advantage は、H.263 と Cisco VT Camera ワイドバンド ビデオ コーデックという、2 タイプのビデオ コーデックをサポートしています。Cisco VT Camera ワイドバンド ビデオ コーデックでは、PC への要求が最少になりますが、ネットワークへの要求は最多になります。H.263 では、ネットワークへの要求が最少になりますが、PC への要求は最多になります。したがって、利用可能な帯域幅がネットワークに豊富にある場合は、Cisco VT Camera ワイドバンド ビデオ コーデックを使用すると PC 上で CPU およびメモリ リソースを節約できます。

H.263 コーデックは、最高 1.5 Mbps までの範囲をサポートしています。要約すると、Cisco Unified Video Advantage を配置するときに、お客様が PC パフォーマンスとネットワーク使用率のバランスをとる必要があります。

システム要件

PC 要件の詳細については、次の Web サイトで入手可能な『*Cisco Unified Video Advantage Data Sheet*』を参照してください。

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/vtadv_ds.htm

Cisco IP Video Phone 7985G

Cisco IP Video Phone 7985G は、パーソナル デスクトップ ビデオ電話機です。PC 上で実行するアプリケーションである Cisco Unified Video Advantage とは異なり、Cisco IP Video Phone 7985G は、ビデオ機能が統合された独立型の電話機です。この電話機は、ビデオ コールの発信用に 8.4 インチのカラー LCD 画面とビデオ カメラを備えています。最高 8 つのライン アピアランスをサポートし、2 つの 10/100 Base-T イーサネット接続と、Directories、Messages、Settings、および Services の各ボタンを備えています。他の Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は CDP を使用して VLAN および CoS の情報を接続スイッチから取得し、802.1p/q マーキングで使用します。

Cisco Unified Video Advantage および Cisco IP Video Phone 7985G でサポートされているコーデック

表 19-4 は、Cisco Unified Video Advantage と Cisco IP Video Phone 7985G でサポートされるコーデックをリストしています。

表 19-4　Cisco Unified Video Advantage と Cisco IP Video Phone 7985G でサポートされるコーデック

コーデックまたは機能	Cisco Unified Video Advantage	Cisco IP Video Phone 7985G
H.264	なし	あり
H.263	あり	あり
H.261	なし	あり
G.711	あり	あり
G.722	なし	あり
G.722.1	なし	なし
G.723.1	なし	なし
G.728	なし	なし
G.729	あり	あり
Cisco Wideband	あり	なし
最高帯域幅	7 Mbps	768 Kbps
ビデオ解像度	CIF、QCIF	NTSC：4SIF、SIF PAL：4CIF、QCIF、SQCIF

サードパーティ製 SCCP ビデオ エンドポイント

ビデオ エンドポイントの 2 つの製造業者である Sony 社 と Tandberg 社 は現在、次の製品で Cisco Skinny Client Control Protocol（SCCP）をサポートしています。

- Sony 社製 PCS-1 および PCS-TL50
- Tandberg 社製 T-1000 および T-550

Sony 社製と Tandberg 社製の両方のエンドポイントでの SCCP は、Cisco Unified IP Phone 7940 での SCCP に従ってモデル化されています。複数のライン アピアランス、ソフトキー、およびボタン（Directories、Messages、Settings、Services）など、Cisco Unified IP Phone 7940 ユーザ インターフェイスにある機能のほとんどが、Sony 社製エンドポイントと Tandberg 社製エンドポイントでもサポートされています。Sony 社製と Tandberg 社製のエンドポイントは、TFTP サーバの IP アドレス検出用に DHCP の Option 150 フィールドもサポートし、TFTP サーバから設定をダウンロードします。ただし、Sony 社製および Tandberg 社製のエンドポイントのソフトウェア アップグレードは、TFTP を介しては行われません。代わりに、ベンダーから提供されるツールを使用して、お客様が各エンドポイントを手動でアップグレードする必要があります（Tandberg 社製では FTP による方法が使用され、Sony 社製では FTP または物理メモリ スティックが使用されます）。Sony 社製および Tandberg 社製のエンドポイントは、最大で 3 台の Cisco Unified CallManager サーバに登録され、1 次サーバが通信不能になったときに、2 次サーバまたは 3 次サーバにフェールオーバーします。

Sony 社製および Tandberg 社製のエンドポイントは Cisco Unified IP Phone 7940 および 7960 のソフトキー機能と類似したソフトキー機能をサポートしていますが、実際の機能サポートはベンダーおよびモデルによって異なります。サポートされる機能については、製造業者のマニュアルで確認してください。現在、一部のプラットフォーム上にない機能として、次のものがあります。

- Messages ボタン

- Directories ボタン（発信コール、受信コール、不在コール、および社内ディレクトリ）
- Settings ボタンと Services ボタン
- 一部の XML サービス（エクステンション モビリティや Berbee InformaCast など）

Sony 社製および Tandberg 社製のエンドポイントは SCCP を使用するため、エンドポイントでのビデオ コールのダイヤルは、Cisco Unified IP Phone でのオーディオ コールのダイヤルと似ています。Cisco Unified IP Phone に慣れているユーザであれば、Sony 社製および Tandberg 社製のエンドポイントも直感的に使いこなせるはずです。ユーザ インターフェイスの主な相違点は、Sony 社製および Tandberg 社製のエンドポイントに電話機のようなボタン キーパッドや受話器がないことです。代わりに、リモート コントロールを使用して機能にアクセスし、番号をダイヤルします。

（注） Sony 社製および Tandberg 社製のエンドポイントは、Cisco Discovery Protocol（CDP）または IEEE 802.Q/p をサポートしていません。したがって、その接続先のイーサネット スイッチで、VLAN ID および Quality of Service の信頼境界を手動で設定する必要があります（詳細については、P.3-1 の「ネットワーク インフラストラクチャ」を参照してください）。

Sony 社製と Tandberg 社製の SCCP エンドポイントでサポートされているコーデック

サードパーティ製 SCCP エンドポイントのコーデック サポートは、ベンダー、モデル、およびソフトウェア バージョンによって異なります。サポートされるコーデックについては、ベンダーの製品マニュアルで確認してください。

サードパーティ製 SIP IP Phone

サードパーティ製電話機には、機能アクセス ボタン（固定または可変）など、コール制御シグナリング プロトコルとは関係しない、固有のローカル機能が備わっています。基本的な SIP RFC サポートでは、特定のデスクトップ機能が Cisco Unified IP Phone と同じになるように対応し、特定機能の相互運用性にも対応します。ただし、これらのサードパーティ製 SIP 電話機は、Cisco Unified IP Phone の機能をフル装備しているわけではありません。

シスコは、新しい Cisco Unified CallManager および Cisco Unified CallManager Express の SIP 機能を利用するソリューションの開発に携わっている、Cisco Technology Development Partner Program の一員としての主要なサードパーティ ベンダーと協力して活動しています。このようなベンダーとしては、IPCelerate（教育スペース用の統一クライアント）、RIM（Blackberry 7270 無線 LAN ハンドセット）、および IP blue（ソフトフォン）があります。シスコは、サードパーティ ベンダーの Grandstream とも協力して Grandstream GXP 2000 のテストを行い、相互運用性を保証しています。

シスコは、tekVizion が提供する独立したサードパーティのテストおよび相互運用性検証プロセスにも参加しています。tekVizion が提供するこの独立サービスは、サードパーティ ベンダーのエンドポイントが Cisco Unified CallManager および CallManager Express との相互運用性をテストおよび検証できるようにするために確立されました。

シスコの回線側 SIP 相互運用性およびサードパーティ検証の詳細については、http://www.cisco.com を参照してください。

QoS の推奨事項

この項では、IP テレフォニー エンドポイントで配置される一般的な Cisco Catalyst スイッチでの、基本的な QoS ガイドラインおよび設定について説明します。詳細については、次の Web サイトで入手可能な『*Quality of Service*』を参照してください。

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

Cisco VG224 および VG248

アナログ ゲートウェイは、信頼できるエンドポイントです。Cisco VG224 および VG248 ゲートウェイの場合、VG248 パケットの DSCP 値を信頼するようにスイッチを設定します。ここでは、Cisco VG224 および VG248 アナログ ゲートウェイで配置される一般的な Cisco Catalyst スイッチを設定するためのコマンドをリストします。

（注） 次の項では、*vvlan_id* は Voice VLAN ID を表し、*dvlan_id* はデータ VLAN ID を表します。

Cisco 2950

```
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust dscp
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport access vlan vvlan_id
```

（注） **mls qos trust dscp** コマンドは、Enhanced Image（EI）でのみ使用できます。

Cisco 2970 または 3750

```
CAT2970(config)#mls qos
CAT2970(config)interface interface-id
CAT2970(config-if)#mls qos trust dscp
CAT2970(config-if)#switchport mode access
CAT2970(config-if)#switchport access vlan vvlan_id
```

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)interface interface-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#switchport mode access
Cat3550(config-if)#switchport access vlan vvlan_id
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)#qos
CAT4500(config)interface interface-id
CAT4500(config-if)#qos trust dscp
CAT4500(config-if)#switchport mode access
CAT4500(config-if)#switchport access vlan vvlan_id
```

Cisco 6500

```
CAT6500>(enable)set qos enable
CAT6500>(enable)set port qos 2/1 vlan-based
CAT6500>(enable)set vlan vvlan_id mod/port
CAT6500>(enable)set port qos mod/port  trust trust-dscp
```

Cisco ATA 186 および IP Conference Station

Cisco Analog Telephone Adaptor（ATA）186 および IP Conference Station は、信頼されているエンドポイントであるため、それらの QoS 設定は、P.19-28 の「Cisco VG224 および VG248」の項で説明されている設定とまったく同じです。

Cisco ATA 188 および IP Phone

Cisco Analog Telephone Adaptor（ATA）188 および IP Phone の場合、Voice VLAN をデータ VLAN から分離することをお勧めします。Cisco ATA 186、7902、7905、7910、および IP Conference Station の場合は、従来どおり、Voice VLAN とデータ VLAN を分離することと、Auxiliary VLAN を設定することをお勧めします。これにより、同じアクセスレイヤの設定を、異なる IP Phone モデルや ATA に使用できます。またエンドユーザは、IP Phone または ATA を、スイッチ上の異なるアクセス ポートに接続して、同じ処理を受けることができます。Cisco ATA 186、7902、7905、7910、および IP Conference Station の場合、これらのデバイスは PC に接続されていないので、接続された PC からのフレームの CoS 値を上書きするためのコマンドは何の効果もありません。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の IP Phone に対して実行できる設定コマンドをリストします。

Cisco 2950

```
CAT2950(config)#
CAT2950(config)#class-map VVLAN
CAT2950(config-cmap)# match access-group name VVLAN
CAT2950(config-cmap)#class-map VLAN
CAT2950(config-cmap)# match access-group name DVLAN
CAT2950(config-cmap)#exit
CAT2950(config)#
CAT2950(config)#policy-map IPPHONE-PC
CAT2950(config-pmap)# class VVLAN
CAT2950(config-pmap-c0#  set ip dscp 46
CAT2950(config-pmap-c)#  police 1000000 8192 exceed-action-drop
CAT2950(config-pmap)# class DVLAN
CAT2950(config-pmap-c0#  set ip dscp 0
CAT2950(config-pmap-c)#  police 5000000 8192 exceed-action-drop
CAT2950(config-pmap-c)#exit
CAT2950(config-pmap)#exit
CAT2950(config)#
CAT2950(config)#interface interface-id
CAT2950(config-if)#mls qos trust device cisco-phone
CAT2950(config-if)#mls qos trust cos
CAT2950(config-if)#switchport mode access
CAT2950(config-if)#switchport voice vlan vvlan_id
CAT2950(config-if)#switchport access vlan dvlan_id
CAT2950(config-if)#service-policy input IPPHONE-PC
CAT2950(config-if)#exit
CAT2950(config)#
CAT2950(config)#ip access-list standard VVLAN
CAT2950(config-std-nacl)# permit voice_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#exit
CAT2950(config)#ip access-list standard DVLAN
CAT2950(config-std-nacl)# permit data_IP_subnet wild_card_mask
CAT2950(config-std-nacl)#end
```

（注）　**mls qos map cos-dscp** コマンドは、Enhanced Image（EI）でのみ使用できます。Standard Image（SI）では、このコマンドを使用できません。CoS から DSCP へのデフォルトのマッピングは、次のとおりです。

Cos 値	0	1	2	3	4	5	6	7
DSCP 値	0	8	16	24	32	40	48	56

Cisco 2970 または 3750

```
CAT2970(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT2970(config)# mls qos map policed-dscp 0 24 to 8
CAT2970(config)#
CAT2970(config)#class-map match-all VVLAN-VOICE
CAT2970(config-cmap)# match access-group name VVLAN-VOICE
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT2970(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT2970(config-cmap)#
CAT2970(config-cmap)#class-map match-all VVLAN-ANY
CAT2970(config-cmap)# match access-group name VVLAN-ANY
CAT2970(config-cmap)#
CAT2970(config-cmap)# policy-map IPPHONE-PC
CAT2970(config-pmap)#class VVLAN-VOICE
CAT2970(config-pmap-c)# set ip dscp 46
CAT2970(config-pmap-c)# police 128000 8000 exceed-action drop
CAT2970(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT2970(config-pmap-c)# set ip dscp 24
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class VVLAN-ANY
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# class class-default
CAT2970(config-pmap-c)# set ip dscp 0
CAT2970(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT2970(config-pmap-c)# exit
CAT2970(config-pmap)# exit
CAT2970(config)#
CAT2970(config)#
CAT2970(config)#interface interface-id
CAT2970(config-if)# switchport voice vlan vvlan_id
CAT2970(config-if)# switchport access vlan dvlan_id
CAT2970(config-if)# mls qos trust device cisco-phone
CAT2970(config-if)# service-policy input IPPHONE-PC
CAT2970(config-if)# exit
CAT2970(config)#
CAT2970(confiig)#ip access list extended VVLAN-VOICE
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384
32767 dscp ef
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002
dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002
dscp
Af31
CAT2970(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT2970(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061
dscp cs3
CAT2970(config-ext-nacl)# exit
CAT2970(config)#ip access list extended VVLAN-ANY
CAT2970(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT2970(config-ext-nacl)# end
CAT2970#
```

Cisco 3550

```
CAT3550(config)# mls qos map cos-dscp 0 8 16 24 34 46 48 56
CAT3550(config)# mls qos map policed-dscp 0 24 26 46 to 8
CAT3550(config)#class-map match-all VOICE
CAT3550(config-cmap)# match ip dscp 46
CAT3550(config-cmap)#class-map match-any CALL SIGNALING
CAT3550(config-cmap)# match ip dscp 26
CAT3550(config-cmap)# match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-VOICE
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map CALL SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all ANY
CAT3550(config-cmap)# match access-group name ACL_Name
CAT3550(config-cmap)#
CAT3550(config-cmap)# class-map match-all VVLAN-ANY
CAT3550(config-cmap)# match vlan vvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all DVLAN-ANY
CAT3550(config-cmap)# match vlan dvlan_id
CAT3550(config-cmap)# match class-map ANY
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map IPPHONE-PC
CAT3550(config-pmap)# class VVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
CAT3550(config-pmap-c)# police 128000 8000 exceed-action drop
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class VVLAN-ANY
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class DVLAN-VOICE
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
CAT3550(config-pmap-c)#exit
CAT3550(config-pmap)#exit
CAT3550(config)#interface interface-id
CAT3550(config-if)# switchport voice vlan vvlan_id
CAT3550(config-if)# switchport access vlan dvlan_id
CAT3550(config-if)# mls qos trust device cisco-phone
CAT3550(config-if)# service-policy input IPPHONE-PC
CAT3550(config-if)# exit
CAT3550(config)#
CAT3550(confiig)#ip access list standard ACL_ANY
CAT3550(config-std-nacl)# permit any
CAT3550(config-std-nacl)# end
CAT3550#
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config)# qos map cos 5 to dscp 46
CAT4500(config)# qos map cos 0 24 26 46 to dscp 8
CAT4500(config)#
CAT4500(config)#class-map match-all VVLAN-VOICE
CAT4500(config-cmap)# match access-group name VVLAN-VOICE
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-CALL-SIGNALING
CAT4500(config-cmap)# match access-group name VVLAN-CALL-SIGNALING
CAT4500(config-cmap)#
CAT4500(config-cmap)#class-map match-all VVLAN-ANY
CAT4500(config-cmap)# match access-group name VVLAN-ANY
CAT4500(config-cmap)#
CAT4500(config-cmap)# policy-map IPPHONE-PC
CAT4500(config-pmap)#class VVLAN-VOICE
CAT4500(config-pmap-c)# set ip dscp 46
CAT4500(config-pmap-c)# police 128 kps 8000 byte exceed-action drop
CAT4500(config-pmap-c)# class VVLAN-CALL-SIGNALING
CAT4500(config-pmap-c)# set ip dscp 24
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class VVLAN-ANY
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 32 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# class class-default
CAT4500(config-pmap-c)# set ip dscp 0
CAT4500(config-pmap-c)# police 5 mpbs 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c)# exit
CAT4500(config-pmap)# exit
CAT4500(config)#
CAT4500(config)#
CAT4500(config)#interface interface-id
CAT4500(config-if)# switchport voice vlan vvlan_id
CAT4500(config-if)# switchport access vlan dvlan_id
CAT4500(config-if)# qos trust device cisco-phone
CAT4500(config-if)# service-policy input IPPHONE-PC
CAT4500(config-if)# exit
CAT4500(config)#
CAT4500(confiig)#ip access list extended VVLAN-VOICE
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any range 16384
32767 dscp ef
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-CALL-SIGNALING
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002
dscp cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 2000 2002
dscp
Af31
CAT4500(config-ext-nacl)# permit udp Voice_IP_Subnet  Subnet_Mask any eq 5060 dscp cs3
CAT4500(config-ext-nacl)# permit tcp Voice_IP_Subnet  Subnet_Mask any range 5060 5061
dscp cs3
CAT4500(config-ext-nacl)# exit
CAT4500(config)#ip access list extended VVLAN-ANY
CAT4500(config-ext-nacl)# permit ip Voice_IP_Subnet  Subnet_Mask any
CAT4500(config-ext-nacl)# end
CAT4500#
```

Cisco 6500

```
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate VVLAN-VOICE rate 128 burst 8000 drop
CAT6500> (enable) set qos policer aggregate VVLAN-CALL-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate VVLAN-ANY rate 5000 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 46 aggregate VVLAN-VOICE udp
Voice_IP_Subnet Subnet_Mask any range 16384 32767
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING tcp
Voice_IP_Subnet Subnet_Mask any  range 2000 2002
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING
tcp Voice_IP_Subnet Wildcard_bits any  range 5060 5061
CAT6500> (enable)  set qos acl ip IPPHONE-PC dscp 24 aggregate VVLAN-CALL-SIGNALING
udp Voice_IP_Subnet Wildcard_bits  any  eq 5060
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate VVLAN-ANY Voice_IP_Subnet
Subnet_Mask any
CAT6500> (enable) set qos acl ip IPPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl IPPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust-device ciscoipphone
CAT6500> (enable) set qos acl map IPPHONE-PC mod/port
CAT6500> (enable)
```

ソフトウェアベースのエンドポイント

Cisco IP SoftPhone および IP Communicator は、それぞれシグナリング パケットおよびメディア パケットをマーキングしますが、Cisco IP SoftPhone または IP Communicator を実行している PC から、パケットの DSCP 値を再度マーキングするようにお勧めします。その PC は、ネットワーク上で信頼されているデバイスではないからです。メディア パケット用の UDP（ユーザ データグラム プロトコル）ポート（16384 ～ 32767）の全範囲を使用する代わりに、特定の UDP ポートを使用するように Cisco IP Softphone と IP Communicator を設定できます。

Cisco IP SoftPhone の場合、**Network Audio Settings** > **Audio Output Port** で UDP ポートとポート範囲を指定できます。Cisco IP Communicator の場合、次のいずれかのオプションを使用して UDP ポートを指定できます。

- IP Communicator 設定ページの製品固有のセクションで、**RTP Port Range Start** および **RTP Port Range End** を指定します。
- **Preferences** > **Audio Settings** > **Network** > **Port Range** を選択し、ポート範囲を指定します。

両方のオプションを使用して UDP ポートおよびポート範囲を設定する場合、2 番目のオプションでの設定値の方が 1 番目のオプションより優先されます。

次の項では、一般的に配置されている Cisco Catalyst スイッチ上の Cisco IP SoftPhone および IP Communicator に対して実行できる QoS 設定コマンドをリストします。

Cisco 2950（Enhanced Image 対応）

Cisco Catalyst 2950 シリーズ スイッチを、ソフトウェアベースのエンドポイント QoS の実装で使用することは推奨されていません。原因は、次の 2 つの制限です。

- Cisco 2950 では、**range** キーワードを使用して ACL 設定内で UDP ポート範囲を指定することはサポートされていません。この制限の回避策は、前の項で説明した方法で、使用する Cisco IP SoftPhone 用の単一の静的 UDP ポートを設定することです。
- Cisco 2950 は、FastEthernet ポートで 1 Mbps の増分のみサポートしています。これにより、許可されていないネットワーク トラフィックにかなり大きなホールが発生し、コール シグナリングまたはメディアの模倣が発生することがあります。

Cisco 2970 または 3750

```
CAT2970 (config) #mls qos
CAT2970 (config) #mls qos map policed-dscp 0 24 26 46 to 8
CAT2970 (config) #
CAT2970 (config) #class-map match-all SOFTPHONE-VOICE
CAT2970 (config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT2970 (config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT2970 (config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT2970 (config-cmap) #exit
CAT2970 (config) #
CAT2970 (config) #policy-map SOFTPHONE-PC
CAT2970 (config-pmap-c) #class SOFTPHONE-VOICE
CAT2970 (config-pmap-c) # set ip dscp 46
CAT2970 (config-pmap-c) # police 128000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c) #class SOFTPHONE-SIGNALING
CAT2970 (config-pmap-c) # set ip dscp 24
CAT2970 (config-pmap-c) # police 32000 8000 exceed-action policed-dscp-transmit
CAT2970 (config-pmap-c) #class class-default
CAT2970 (config-pmap-c) # set ip dscp 0
CAT2970 (config-pmap-c) # police 5000000 8000 exceed-action policed-dscp transmit
CAT2970 (config-pmap-c) # exit
CAT2970 (config-pmap) #exit
CAT2970 (config) #
CAT2970 (config) #interface FastEthernet interface-id
CAT2970 (config-if) # switchport access vlan vvlan_id
CAT2970 (config-if) # switchport mode access
CAT2970 (config-if) # service-policy input SOFTPHONE-PC
CAT2970 (config-if) # exit
CAT2970 (config) #ip access list extended SOFTPHONE-VOICE
CAT2970 (config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT2970 (config-ext-nacl) # exit
CAT2970(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT2970(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT2970(config-ext-nacl)# exit
```

Cisco 3550

```
CAT3550 (config) #mls qos
CAT3550 (config) #mls qos map policed-dscp 0 24 26 46 to 8
CAT3550 (config) #
CAT3550 (config) #class-map match-all SOFTPHONE-VOICE
CAT3550 (config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT3550 (config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT3550 (config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT3550 (config-cmap) #exit
CAT3550 (config) #
CAT3550 (config) #policy-map SOFTPHONE-PC
CAT3550 (config-pmap-c) #class SOFTPHONE-VOICE
CAT3550 (config-pmap-c) # set ip dscp 46
CAT3550 (config-pmap-c) # police 128000 8000 exceed-action policed-dscp-transmit
CAT3550 (config-pmap-c) #class SOFTPHONE-SIGNALING
CAT3550 (config-pmap-c) # set ip dscp 24
CAT3550 (config-pmap-c) # police 32000 8000 exceed-action policed-dscp-transmit
CAT3550 (config-pmap-c) #class class-default
CAT3550 (config-pmap-c) # set ip dscp 0
CAT3550 (config-pmap-c) # police 5000000 8000 exceed-action policed-dscp transmit
CAT3550 (config-pmap-c) # exit
CAT3550 (config-pmap) #exit
CAT3550 (config) #
CAT3550 (config) #interface FastEthernet interface-id
CAT3550 (config-if) # switchport access vlan vvlan_id
CAT3550 (config-if) # switchport mode access
CAT3550 (config-if) # service-policy input SOFTPHONE-PC
CAT3550 (config-if) # exit
CAT3550 (config) #ip access list extended SOFTPHONE-VOICE
CAT3550 (config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT3550 (config-ext-nacl) # exit
CAT3550(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT3550(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT3550(config-ext-nacl)# exit
```

Cisco 4500（SUPIII、IV、または V 使用）

```
CAT4500(config) #qos
CAT4500(config) #qos map policed-dscp 0 24 26 46 to 8
CAT4500(config) #
CAT4500(config) #class-map match-all SOFTPHONE-VOICE
CAT4500(config-cmap) #  match access-group name SOFTPHONE-VOICE
CAT4500(config-cmap) #class-map match-all SOFTPHONE-SIGNALING
CAT4500(config-cmap) #  match access-group name SOFTPHONE-SIGNALING
CAT4500(config-cmap) #exit
CAT4500(config) #
CAT4500(config) #policy-map SOFTPHONE-PC
CAT4500(config-pmap-c) #class SOFTPHONE-VOICE
CAT4500(config-pmap-c) # set ip dscp EF
CAT4500(config-pmap-c) # police 128 kps 8000 byte exceed-action policed-dscp-transmit
CAT4500(config-pmap-c) #class SOFTPHONE-SIGNALING
CAT4500(config-pmap-c) # set ip dscp CS3
CAT4500(config-pmap-c) # police 32000 kps 8000 byte exceed-action
policed-dscp-transmit
CAT4500(config-pmap-c) #class class-default
CAT4500(config-pmap-c) # set ip dscp default
CAT4500(config-pmap-c) # police 5 mpbs 8000 byte exceed-action policed-dscp transmit
CAT4500(config-pmap-c) # exit
CAT4500(config-pmap) #exit
CAT4500(config) #
CAT4500(config) #interface FastEthernet interface-id
CAT4500(config-if) # switchport access vlan vvlan_id
CAT4500(config-if) # switchport mode access
CAT4500(config-if) # service-policy input SOFTPHONE-PC
CAT4500(config-if) # exit
CAT4500(config) #ip access list extended SOFTPHONE-VOICE
CAT4500(config-ext-nacl) #  permit udp host PC_IP_address eq fixed_port_number any
CAT4500(config-ext-nacl) # exit
CAT4500(config)#ip access-list extended SOFTPHONE-SIGNALING
CAT4500(config-ext-nacl)# permit tcp host PC_IP_address host CallManager_IP_address eq
2748 or 2000
CAT4500(config-ext-nacl)# exit
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos policed-dscp-map 0, 24, 26, 46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer aggregate SOFTPHONE-VOICE rate 128 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate SOFTPHONE-SIGNALING rate 32 burst 8000
policed-dscp
CAT6500> (enable) set qos policer aggregate PC-DATA rate 5000 burst 8000 policed-dscp
CAT6500> (enable)
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 46 aggregate SOFTPHONE-VOICE udp
host PC_IP_address eq fixed_port_number any
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 24 aggregate SOFTPHONE-SIGNALING
tcp host PC_IP_address host CallManager_IP_address eq 2748 or 2000
CAT6500> (enable) set qos acl ip SOFTPHONE-PC dscp 0 aggregate PC-DATA any
CAT6500> (enable) commit qos acl SOFTPHONE-PC
CAT6500> (enable) set vlan vvlan_id mod/port
CAT6500> (enable) set port qos mod/port trust untrusted
CAT6500> (enable) set qos acl map SOFTPHONE-PC mod/port
CAT6500> (enable)
```

（注） DSCP の再マーキングは、レイヤ 3 対応のスイッチが行う必要があります。アクセス レイヤ スイッチ（Cisco Catalyst 2950 with Standard Image または Cisco 3524XL など）にこの機能がない場合、DSCP の再マーキングは分散レイヤ スイッチで行う必要があります。

Cisco Unified Wireless IP Phone 7920

デフォルトでは、Cisco Unified Wireless IP Phone 7920 は、Per-Hop Behavior（PHB）値 CS3、または Differentiated Services Code Point（DSCP）値 24（ToS 値 0x60 に相当）を使用して SCCP シグナリング メッセージをマーキングし、PHB 値 EF、または DSCP 値 46（ToS 値 0xB8 に相当）を使用して RTP 音声パケットをマーキングします。AP でキューイングが正しく設定されており、アップストリームの最初のホップのスイッチが AP のポートを信頼するように設定されている場合、無線 IP Phone のトラフィックは、有線 IP Phone のトラフィックと同じように処理されます。この方法により、LAN と WLAN 環境で QoS 設定の一貫性を保つことができます。

さらに、Cisco Unified Wireless IP Phone 7920 は、Cisco Discovery Protocol（CDP）を使用して、その存在を AP に自動的に伝えます。CDP パケットは無線 IP Phone から AP に送信され、これらのパケットにより電話機が特定されます。これにより、AP は、その IP Phone へのすべてのトラフィックを高プライオリティ キューに入れることができます。

通常、イーサネット スイッチ ポートは 100 Mbps での送受信が可能ですが、802.11b AP ではスループット レートがより低く、可能なデータ レートは最大で 11 Mbps です。さらに、無線 LAN は共有メディアであり、このメディアで発生するコンテンションが原因で、実際のスループットは大幅に低くなります。スループットにミスマッチがあることは、トラフィックのバースト時に AP でパケットがドロップされ、それが原因でプロセッサに過剰な負荷がかかりパフォーマンスが低下する可能性を示しています。

Cisco Catalyst 3550 および 6500 シリーズ スイッチのポリシングおよびレート制限を活用すると、AP へのトラフィックをレート制限またはポリシングするようにアップストリーム スイッチ ポートを設定することにより、AP が過剰なパケットをドロップする必要性をなくすことができます。次の項のスイッチ ポート設定は、ポートでの 802.11b のスループットを現実的な 7 Mbps にレート制限し、高優先度の音声および制御トラフィックのために 1 Mbps を確保します。また、設定例が示しているとおり、AP から送られるパケットは信頼されている必要があり、各パケットの VLAN タグに基づいて DSCP マーキングを保持またはダウンとマーキングする必要があります。このように、音声 VLAN 上の Cisco Unified Wireless IP Phone 7920 が送信元であるパケットは、適切な DSCP マーキングを保持する必要があり、データ VLAN 上のデータ デバイスが送信元であるパケットは、DSCP 値 0 に再マーキングする必要があります。

Cisco 3550

```
CAT3550(config)#mls qos
CAT3550(config)#mls qos map cos-dscp 0 8 16 24 32 46 48 56
CAT3550(config)#mls qos map policed-dscp  24 46 to 8
CAT3550(config)#mls qos aggregate-policer AGG-POL-1M-VOICE-OUT 1000000 8000
exceed-action policed-dscp-transmit
CAT3550(config)#mls qos aggregate-policer AGG-POL-6M-DEFAULT-OUT 6000000 8000
exceed-action drop
CAT3550(config)#
CAT3550(config)#class-map match-all EGRESS-DSCP-0
CAT3550(config-cmap)#match ip dscp 0
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-8
CAT3550(config-cmap)#match ip dscp 8
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-16
CAT3550(config-cmap)#match ip dscp 16
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-32
CAT3550(config-cmap)#match ip dscp 32
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-48
CAT3550(config-cmap)#match ip dscp 48
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all EGRESS-DSCP-56
CAT3550(config-cmap)#match ip dscp 56
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE-SIGNALING
CAT3550(config-cmap)#match ip dscp 24
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all VOICE
CAT3550(config-cmap)#match ip dscp 46
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DATA
CAT3550(config-cmap)#match any
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-VVLAN-VOICE-SIGNALING
CAT3550(config-cmap)#match vlan vvlan-id
CAT3550(config-cmap)#match class-map VOICE-SIGNALING
CAT3550(config-cmap)#
CAT3550(config-cmap)#class-map match-all INGRESS-DVLAN
CAT3550(config-cmap)#match vlan dvlan-id
CAT3550(config-cmap)#match class-map INGRESS-DATA
CAT3550(config-cmap)#
CAT3550(config-cmap)#policy-map EGRESS-RATE-LIMITER
CAT3550(config-pmap)#class EGRESS-DSCP-0
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-8
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-16
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-32
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-DSCP-48
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#class EGRESS-DSCP-56
CAT3550(config-pmap-c)#police aggregate AGG-POL-6M-DEFAULT-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class EGRESS-VOICE
CAT3550(config-pmap-c)#police aggregate AGG-POL-1M-VOICE-OUT
CAT3550(config-pmap-c)#
```

```
CAT3550(config-pmap-c)#class EGRESS-VOICE-SIGNALING
CAT3550(config-pmap-c)#police aggregate AGG-POL-1M-VOICE-OUT
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#policy-map INGRESS-QOS
CAT3550(config-pmap)#class INGRESS-VVLAN-VOICE
CAT3550(config-pmap-c)#set ip dscp 46
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-VVLAN-CALL-SIGNALING
CAT3550(config-pmap-c)#set ip dscp 24
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class INGRESS-DVLAN
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)#set ip dscp 0
CAT3550(config-pmap-c)#
CAT3550(config-pmap-c)#interface interface id
CAT3550(config-if)#description 11Mb towards Wireless Access Point
CAT3550(config-if)#switchport access dvlan-id
CAT3550(config-if)#switchport voice vvlan-id
CAT3550(config-if)#mls qos trust dscp
CAT3550(config-if)#service-policy output EGRESS-RATE-LIMITER
CAT3550(config-if)#service-policy input INGRESS-QOS
```

Cisco 6500

```
CAT6500> (enable) set qos enable
CAT6500> (enable) set qos cos-dscp-map 0 8 16 24 32 46 48 56
CAT6500> (enable) set qos policed-dscp-map 24,46:8
CAT6500> (enable)
CAT6500> (enable) set qos policer microflow VOICE-OUT rate 1000 burst 32 policed-dscp
CAT6500> (enable) set qos policer microflow DATA-OUT rate 6000 burst 32 drop
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 24 microflow VOICE-OUT ip any
any dscp-field 24
CAT6500> (enable) set qos acl ip AP-VOICE-EGRESS dscp 46 microflow VOICE-OUT ip any
any dscp-field 46
CAT6500> (enable) set qos acl ip AP-DATA-EGRESS dscp 0 microflow DATA-OUT ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl ip AP-VOICE-INGRESS trust-dscp ip any any
CAT6500> (enable) set qos acl ip AP-DATA-INGRESS dscp 0 ip any any
CAT6500> (enable)
CAT6500> (enable) set qos acl map AP-VOICE-EGRESS vvlan-id output
CAT6500> (enable) set qos acl map AP-DATA-EGRESS dvlan-id output
CAT6500> (enable) set qos acl map AP-VOICE-INGRESS vvlan-id input
CAT6500> (enable) set qos acl map AP-DATA-INGRESS dvlan-id input
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port vlan-based
CAT6500> (enable)
CAT6500> (enable) set port qos mod/port trust trust-dscp
CAT6500> (enable)
```

ビデオ テレフォニー エンドポイント

ここでは、次のタイプのエンドポイント デバイスでトラフィックがどのように分類されるかについて説明します。

- Cisco Unified Video Advantage と Cisco Unified IP Phone（P.19-40）
- Cisco IP Video Phone 7985G（P.19-41）
- Sony 社製と Tandberg 社製の SCCP エンドポイント（P.19-41）
- H.323 と SIP のビデオ エンドポイント（P.19-41）

Cisco Unified Video Advantage と Cisco Unified IP Phone

ユーザの PC 上にある Cisco Unified Video Advantage アプリケーションは、DSCP を使用したビデオ トラフィックの分類をサポートし、レイヤ 3 でのみ分類を行えます。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するように設定する必要があります。PC パケットは 802.1Q タグを持つ可能性が低いため、802.1p CoS ビットはサポートできません。このように PC が 802.1p をサポートしないため、次のオプションで Cisco Unified Video Advantage に QoS を実現できます。

オプション 1

現在の QoS モデルで信頼を IP Phone にまで広げた場合、ネットワークへの着信時に音声パケットとシグナリング パケットは正しくマーキングされます。ポートに UDP ポート 5445 と一致する ACL を追加すると、ビデオ メディア チャネルも PHB AF41 に分類されます。この ACL がないと、ビデオ メディアは Best Effort に分類されて、画像の品質低下やリップシンクの問題が起きます。同じ ACL を使用すると、TCP ポート 4224（CS3 と分類）を使用した、Cisco Unified Video Advantage PC と IP Phone 間の CAST 接続の照合も可能ですが、このことで得られる利点はほとんどありません。データ VLAN 上にある PC からのシグナリング パケットは、同じ高速ポート経由で音声 VLAN に返されます。したがって、パケットで輻輳が発生する可能性は非常に低くなります。

オプション 2

『*Enterprise QoS Solution Reference Network Design Guide*』のバージョン 3.1（http://www.cisco.com/go/srnd で入手可能）には、別の方法が示されています。この方法で推奨されていることは、CoS を信頼する代わりに、着信トラフィックの DSCP を信頼するようにポートを変更し、一連の Per-Port/Per-VLAN ACL に着信パケットを通過させることです。この ACL では、そのとき他の基準とともに TCP/UDP ポートに基づいてパケットが照合され、適切なレベルにポリシングされます。たとえば、DSCP を信頼するようにスイッチ ポートが設定されている状態では、Cisco Unified Video Advantage はビデオ パケットに DSCP AF41 とマーキングします。パケットは ACL で照合されますが、その照合は、パケットが UDP ポート 5445 を使用し、DSCP AF41 とマーキングされ、データ VLAN 上に着信していることに基づいて行われます。この ACL は、その後、DSCP を信頼してトラフィックを N kbps（N はポートごとに許可するビデオ帯域幅）にポリシングするために、クラス マップまたはポリシー マップで使用されます。類似した ACL やポリシング機能が、音声 VLAN 内の IP Phone からの音声パケットやシグナリング パケットに存在します。

Cisco IP Video Phone 7985G

他の多くの Cisco Unified IP Phone と同様に、Cisco IP Video Phone 7985G は、電話機からの発信トラフィック用に 802.1p/Q タギングをサポートしています。また、Cisco IP Video Phone 7985G は PC アクセス用に別のイーサネット インターフェイスを備えているので、接続デバイスからの発信トラフィックもサポートしています。Cisco Unified Communications の設計上の現在のベスト プラクティスとしては、電話機が接続されたアップストリーム イーサネット スイッチを、電話機からの 802.1p CoS を信頼するよう設定する必要があります。信頼を電話機の PC ポートにまで広げないことをお勧めしますが、スイッチでサポートされているときは、音声、ビデオ、およびシグナリングのトラフィックの最大量を制限するようにポリシング機能を設定することをお勧めします。

Sony 社製と Tandberg 社製の SCCP エンドポイント

Sony 社製と Tandberg 社製の SCCP エンドポイントは、DSCP を使用してレイヤ 3 でメディア パケットおよびシグナリング パケットを正しくマーキングします。ただし、802.1Q をサポートしていないため、802.1p CoS を使用して分類することはできません。UDP と TCP のポート照合オプションを使用した場合、SCCP シグナリングを CS3 として、またビデオ メディアを AF41 として正しく分類できますが、UDP ポートが音声のみのコールで使用されている場合は判別ができないため、EF としての分類が必要になります。そのような場合、コール アドミッション制御メカニズムは帯域幅を正しく処理できません。この状況を避けるために、Sony 社製または Tandberg 社製のエンドポイントからのトラフィックを分類して信頼する方法として実行可能なオプションは、次の 1 つだけです。

オプション 1

Sony 社製または Tandberg 社製のエンドポイントで使用されているポート上で DSCP を信頼します。スイッチで許可されている場合は、そのポート上で受信可能な EF、F41、CS3 トラフィックの最大量を制限するようにポリシング機能を設定します。そのポートに接続された他のデバイスは、DSCP を使用してパケットが分類されていても、信頼できるとは限りません。このオプションは、Sony 社製または Tandberg 社製のシステムがオフィスや小規模な会議室に固定的に設置されている場合に適しています。

Sony 社製または Tandberg 社製のデバイスは CDP をサポートしていないため、このエンドポイントを音声 VLAN に配置する必要がある場合は、VLAN に配置するときに手動の修正が必要です。音声 VLAN にエンドポイントを直接配置することの利点は、システム内の他の IP テレフォニー エンドポイントと同様に扱えることです。欠点は、ポートが音声 VLAN に直接アクセスするため、セキュリティ上のリスクが発生する可能性があることです。一方、Sony 社製または Tandberg 社製のエンドポイントをデータ VLAN に残すこともできますが、Cisco Unified CallManager に対する SCCP シグナリングを許可し、UDP メディア ストリームが音声コール中またはビデオ コール中にデータ VLAN および音声 VLAN 間を通過できるようにするには、データ VLAN と音声 VLAN 間のアクセスでのロビジョニングが必要です。

H.323 と SIP のビデオ エンドポイント

このタイプのエンドポイントは、H.323 および SIP ビデオ エンドポイントにはさまざまなものがあり、実装と機能も多様なため、QoS の点で大きな課題があります。これらのエンドポイントには主に 2 つの QoS オプションがあります。1 つは、H.323 または SIP のビデオ エンドポイントに依存してすべてのトラフィックのマーキングを正しく行う方法で、もう 1 つは、使用する TCP ポートおよび UDP ポートの詳細な認識に依存する方法です。

オプション 1

エンドポイントがメディア トラフィックおよびシグナリング トラフィックのマーキングを正しく行った場合は（シグナリングには SIP、H.225、H.245、および RAS が含まれる）、その分類を信頼できます。エンドポイントで 802.1Q（結果的に 802.1p CoS）がサポートされる可能性は低いため、この場合は IP Precedence または DSCP を使用します。分類タイプの選択は、そのベンダー、モデル、およびソフトウェア バージョンに左右されます。

（注） H.323 または SIP のエンドポイントがそのパケットのマーキングを正しく行う可能性は非常に低くなります。

オプション 2

送信元、宛先、または TCP と UDP の両方のポート番号（多くは、IP アドレスも含む）を組み合せて使用することによって、トラフィックを正しく照合および分類する ACL を定義できます。さらに、ポリシング機能も適用し、ネットワークで許可されるトラフィック クラスごとにその量を制限することもお勧めします。このオプションには、オプション 1 と同様に、音声のみのコールを誤って分類する可能性があります。

エンドポイント機能の要約

次の各表は、この章で説明した各種のエンドポイント デバイスでサポートされる機能を要約したものです。

- 表 19-5 は、Cisco アナログ ゲートウェイの Cisco Unified Communications 機能を要約したものです。
- 表 19-6 は、SCCP および SIP プロトコルを使用する Cisco ベーシック IP Phone の機能を要約したものです。
- 表 19-7 は、SCCP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 19-8 は、SIP プロトコルを使用する Cisco ビジネス、マネージャ、およびエグゼクティブの各 IP Phone の機能を要約したものです。
- 表 19-9 は、Cisco Unified IP Phone 7920、7935、7936G、および 7985G などの専用エンドポイントの機能を要約したものです。
- 表 19-10 は、Cisco IP Communicator および Cisco IP SoftPhone などのソフトウェアベースのデバイスの機能を要約したものです。

表 19-5　Cisco アナログ ゲートウェイの機能

機能	アナログ インターフェイス カード	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG224	VG248	ATA 186 および 188
イーサネット接続	N	N	N	Y[1]	Y[2]	Y[3]
アナログ ポートの最大数	24[4]	72	24	24	48	2
発信者 ID	Y	N	N	Y	Y	Y
コール ウェイティング	N	N	N	N	Y	Y
コール ウェイティング時の発信者 ID	N	N	N	N	Y	Y
保留	N	N	N	Y[5]	N	Y
コール転送	N	N	N	Y[5]	Y	Y
自動転送	N	N	N	N	Y[6]	Y
自動応答	N	N	N	N	N	N
Ad Hoc 会議	N	N	N	N	Y	Y
Meet-Me 会議	N	N	N	N	N	Y
コール ピックアップ	N	N	N	N	N	Y
グループ ピックアップ	N	N	N	N	N	Y
リダイヤル	N	N	N	N	Y[7]	Y[7]
短縮ダイヤル	N	N	N	N	Y	Y
オンフック ダイヤル	N	N	N	N	N	N
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y[8]
メッセージ待機インジケータ（MWI）	N	N	N	N	Y	Y[8]
Survivable Remote Site Telephony（SRST）サポート	N	N	N	Y	Y	Y
Music On Hold（MoH）	Y	Y	Y	N	Y	Y
消音	N	N	N	N	N	N
Multilevel Precedence and Preemption（MLPP）	N	N	N	N	N	N

表 19-5　Cisco アナログ ゲートウェイの機能（続き）

機能	アナログ インターフェイス カード	Ws-svc-cmm-24fxs	Ws-x6624-fxs	VG224	VG248	ATA 186 および 188
割り込み	N	N	N	N	N	N
C 割り込み	N	N	N	N	N	N
コール保持	N	N	N	N	Y[9]	N
コール アドミッション制御	Y	N	N	N	N	N
ローカル ボイス ビジーアウト	Y	N	N	N	N	N
PLAR（Private Line Automatic Ringdown）	Y	N	N	N	N	Y
グループのハント	Y	N	N	N	N	N
ダイヤル プランのマッピング	Y	N	N	N	N	N
監視切断	Y	N	N	N	N	N
シグナリング パケット ToS 値のマーキング	0x68	0x68[10]	0x68	0x68	0x68	0x68
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
FAX パススルー	Y[11]	Y	Y[12]	Y	Y[11]	Y
FAX リレー	Y	Y	N	Y	Y	N
SCCP（Skinny Client Control Protocol）	N	N	N	N	Y	Y
Session Initiation Protocol（SIP）	N	N	N	Y	N	Y
H.323	Y	Y	N	Y	N	Y
メディア ゲートウェイ コントロール プロトコル（MGCP）	Y	Y	Y	Y	N	Y[13]
G.711	Y	Y	Y	Y	Y	Y
G.722	N	N	N	N	N	N
G.723	Y	Y	N	N	N	Y
G.726	Y	N	N	N	N	N
G.729	Y	Y	Y	Y	Y	Y
音声アクティビティ検出（VAD）	Y	Y	N	Y	N	Y
コンフォート ノイズ生成（CNG）	Y	Y	N	Y	N	Y

1. 2 つの 10/100 Base-T。
2. 1 つの 10/100 Base-T。
3. ATA 188 では 2 つの 10/100 Base-T、ATA 186 では 1 つの 10 Base-T。
4. EVM-HD-8FXS/DID は、基本ボード上に 8 つのポートがあり、FXS または DID シグナリング用に構成可能です。また、EM-HDA-8FXS には 2 つの拡張モジュールを取り付けることができます。
5. H.323 および SIP でのコール制御。
6. Call Forward All。
7. リダイヤル。
8. SCCP および SIP バージョンのみ。
9. VG248 バージョン 1.2 以降でサポート。
10. UDP ポート 2427 では MGCP シグナリングをマーキングしますが、TCP ポート 2428 ではベストエフォート型の MGCP キープアライブ パケットをマーキングします。
11. FAX パススルーおよび FAX リレー。
12. FAX パススルー。
13. Cisco Unified CallManager は、ATA を使用する MGCP をサポートしていません。

表 19-6　Cisco ベーシック IP Phone（SCCP または SIP 使用）

	SCCP						SIP		
機能	7902G	7905G	7910G	7910 +SW	7911G	7912G /G-A	7905G	7911G	7912G /G-A
イーサネット接続	Y[1]	Y[1]	Y[1]	Y[2]	Y[2]	Y[2]	Y[1]	Y[1]	Y[3]
イーサネット スイッチ（PC ポート）	N	N	N	Y	Y	Y[4]	N	Y	Y[4]
Cisco Power-Over-Ethernet（PoE）	Y	Y	Y	Y	Y	Y	Y	Y	Y
IEEE 802.3af Power-Over-Ethernet（PoE）	N	N	N	N	Y	N	N	Y	N
ローカリゼーション	N	Y	N	N	Y	Y	N	Y	N
ディレクトリ番号	1	1	1	1	1	1	1	1	1
回線あたりの最大コール数	200	200	200	200	200	200	2	50	2
液晶ディスプレイ	N	Y	Y	Y	Y	Y	Y	Y	Y
発信者 ID	N	Y	Y	Y	Y	Y	Y	Y	Y
コール ウェイティング	N	Y	Y	Y	Y	Y	Y	Y	Y
コール ウェイティング時の発信者 ID	N	Y	Y	Y	Y	Y	Y	Y	Y
保留	Y	Y	Y	Y	Y	Y	Y	Y	Y
ブラインド転送	N	N	N	N	N	N	Y	Y	Y
初期在席転送	Y	Y	Y	Y	Y	Y	N	Y	N
打診転送	Y	Y	Y	Y	Y	Y	Y	Y	Y
自動転送	Y	Y	Y	Y	Y	Y	Y[5]	Y	Y[5]
自動応答	N	Y[6]	N	N	Y[6]	Y[6]	N	Y[6]	N
Ad Hoc 会議	Y	Y	Y	Y	Y	Y	Y	Y	Y
Meet-Me 会議	N	Y	Y	Y	Y	Y	N	Y	N
コール ピックアップ	N	Y	Y	Y	Y	Y	N	Y	N
グループ ピックアップ	N	Y	Y	Y	Y	Y	N	Y	N
リダイヤル	Y[7]	Y[7]	Y[7]	Y[7]	Y[7]	Y[7]	Y[7]	Y	Y[7]
短縮ダイヤル	Y	Y	Y	Y	Y	Y	Y[8]	Y	Y[8]
オンフック ダイヤル	N	Y	Y	Y	Y	Y	Y	Y	Y
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y	Y	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y	Y	Y	Y	Y	Y	Y	Y
ビデオ コール	N	N	N	N	N	N	N	N	N
Survivable Remote Site Telephony（SRST）サポート	Y	Y	Y	Y	Y	Y	Y	Y	Y
ユニキャスト MoH	Y	Y	Y	Y	Y	Y	Y	Y	Y
マルチキャスト MoH	Y	Y	Y	Y	Y	Y	N	Y	N
保留音	Y	Y	Y	Y	Y	Y	N	N	N
スピーカー	N	Y[6]	Y[6]	Y[6]	Y[6]	Y[6]	Y[6]	Y[6]	Y[6]
ヘッドセット ジャック	N	N	N	N	N	N	N	N	N
消音	N	N	Y	Y	N	N	N	Y	N
Multilevel Precedence and Preemption（MLPP）	Y	Y	Y	Y	Y	Y	N	N	N
割り込み	N	N	N	N	N	Y	N	Y	N
C 割り込み	N	Y	N	N	Y	Y	N	Y	N

表 19-6　Cisco ベーシック IP Phone（SCCP または SIP 使用）（続き）

機能	SCCP						SIP		
	7902G	7905G	7910G	7910 +SW	7911G	7912G /G-A	7905G	7911G	7912G /G-A
General Attribute Registration Protocol（GARP）の無効化	Y	Y	Y	Y	Y	Y	Y	Y	Y
シグナリングおよびメディア暗号化	N	N	N	N	N	N	N	Y	N
シグナリングの完全性	N	N	N	N	N	N	N	Y	N
製造元でインストールされる証明書（X.509v3）	N	N	N	N	N	N	N	Y	N
現場でインストールされる証明書	N	N	N	N	N	N	N	N	N
サードパーティの XML サービス	N	Y	N	N	Y	Y	N	Y	N
外部マイクおよびスピーカー	N	N	N	N	N	N	N	N	N
ダイヤル プラン	N	N	N	N	N	N	Y	Y	Y
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	Y	Y	Y	Y	Y	Y	Y	Y	Y
G.722	N	N	N	N	N	N	N	N	N
G.723	N	Y	N	N	N	N	N	Y	N
G.726	N	Y	N	N	N	N	N	N	N
G.729	Y	Y	Y	Y	Y	Y	Y[9]	Y[9]	Y[9]
ワイドバンド オーディオ	N	N	N	N	N	N	N	N	N
ワイドバンド ビデオ	N	N	N	N	N	N	N	N	N
音声アクティビティ検出（VAD）	Y	Y	Y	Y	Y	Y	Y	Y	Y
コンフォート ノイズ生成（CNG）	Y	Y	Y	Y	Y	Y	Y	Y	Y
DTMF：H.245	N	N	N	N	N	N	N	N	N
DTMF：SCCP	Y	Y	Y	Y	Y	Y	N	N	N
DTMF：RFC2833	N	N	N	N	Y	N	Y	Y	Y
DTMF：KMPL	N	N	N	N	N	N	N	Y	N
DTMF：サブスクライブ / 通知	N	N	N	N	N	N	N	Y	N

1. 1 つの 10 Base-T。
2. 2 つの 10/100 Base-T。
3. 1 つの 10/100 Base-T。
4. Cisco Unified IP Phone 7912GA は、拡張版イーサネット スイッチを備えています。
5. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Cisco Unified CallManager で電話機の設定が認識されないので、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Cisco Unified CallManager の User ページで有効にされている場合、Cisco Unified CallManager はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Cisco Unified CallManager の User ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. 一方向のオーディオ モニタ モード。
7. リダイヤル。
8. 短縮ダイヤルは、これらのモデルの電話機だけに設定可能です。
9. これらの IP Phone モデルは、受信モードでだけ G.729b と G.729ab をサポートします。

表 19-7　Cisco ビジネス、マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）

機能	7940G	7941G/G-GE	7960G	7961G/G-GE	7970G	7971G-GE
イーサネット接続	Y[1]	Y[2]	Y[1]	Y[3]	Y[1]	Y[4]
イーサネット スイッチ（PC ポート）	Y	Y	Y	Y	Y	Y
Cisco Power-Over-Ethernet（PoE）	Y	Y	Y	Y	Y	Y
IEEE 802.3af Power-Over-Ethernet（PoE）	N	Y	N	Y	Y	Y
ローカリゼーション	Y	Y	Y	Y	Y	Y
ディレクトリ番号	2	2	6	6	8	8
回線あたりの最大コール数	200	200	200	200	200	200
液晶ディスプレイ	Y	Y	Y	Y	Y	Y
発信者 ID	Y	Y	Y	Y	Y	Y
コール ウェイティング	Y	Y	Y	Y	Y	Y
コール ウェイティング時の発信者 ID	Y	Y	Y	Y	Y	Y
保留	Y	Y	Y	Y	Y	Y
ブラインド転送	N	N	N	N	N	N
初期在席転送	Y	Y	Y	Y	Y	Y
打診転送	Y	Y	Y	Y	Y	Y
自動転送	Y	Y	Y	Y	Y	Y
自動応答	Y	Y	Y	Y	Y	Y
Ad Hoc 会議	Y	Y	Y	Y	Y	Y
Meet-Me 会議	Y	Y	Y	Y	Y	Y
コール ピックアップ	Y	Y	Y	Y	Y	Y
グループ ピックアップ	Y	Y	Y	Y	Y	Y
リダイヤル	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]	Y[5]
短縮ダイヤル	Y	Y	Y	Y	Y	Y
オンフック ダイヤル	Y	Y	Y	Y	Y	Y
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y	Y	Y	Y	Y
ビデオ コール	Y	Y	Y	Y	Y	Y
Survivable Remote Site Telephony（SRST）サポート	Y	Y	Y	Y	Y	Y
ユニキャスト MoH	Y	Y	Y	Y	Y	Y
マルチキャスト MoH	Y	Y	Y	Y	Y	Y
保留音	Y	Y	Y	Y	Y	Y
スピーカー	Y	Y	Y	Y	Y	Y
ヘッドセット ジャック	Y	Y	Y	Y	Y	Y
消音	Y	Y	Y	Y	Y	Y
Multilevel Precedence and Preemption（MLPP）	Y	Y	Y	Y	Y	Y
割り込み	Y	Y	Y	Y	Y	Y
C 割り込み	Y	Y	Y	Y	Y	Y
General Attribute Registration Protocol（GARP）の無効化	Y	Y	Y	Y	Y	Y

表 19-7　Cisco ビジネス、マネージャ、およびエグゼクティブ IP Phone（SCCP 使用）（続き）

機能	7940G	7941G/G-GE	7960G	7961G/G-GE	7970G	7971G-GE
シグナリングおよびメディア暗号化	Y	Y	Y	Y	Y	Y
シグナリングの完全性	Y	Y	Y	Y	Y	Y
製造元でインストールされる証明書（X.509v3）	N	Y	N	Y	Y	Y
現場でインストールされる証明書	Y	N	Y	N	N	N
サードパーティの XML サービス	Y	Y	Y	Y	Y	Y
外部マイクおよびスピーカー	Y	Y	Y	Y	Y	Y
ダイヤル プラン	N	N	N	N	N	N
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	Y	Y	Y	Y	Y	Y
G.722	N	N	N	N	N	N
G.723	N	N	N	N	N	N
G.726	N	N	N	N	N	N
G.729	Y	Y	Y	Y	Y	Y
ワイドバンド オーディオ	N	N	N	N	N	N
ワイドバンド ビデオ	N	N	N	N	N	N
音声アクティビティ検出（VAD）	Y	Y	Y	Y	Y	Y
コンフォート ノイズ生成（CNG）	Y	Y	Y	Y	Y	Y
DTMF：H.245	N	N	N	N	N	N
DTMF：SCCP	Y	Y	Y	Y	Y	Y
DTMF：RFC2833	N	Y	N	Y	Y	Y
DTMF：KMPL	N	N	N	N	N	N
DTMF：サブスクライブ / 通知	N	N	N	N	N	N

1. 2 つの 10/100 Base-T。
2. Cisco Unified IP Phone 7941G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7941GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
3. Cisco Unified IP Phone 7961G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7961GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
4. Cisco Unified IP Phone 7971G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7971GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
5. リダイヤル。

表 19-8　Cisco ビジネス、マネージャ、およびエグゼクティブ IP Phone（SIP 使用）

機能	7940G	7941G/G-GE	7960G	7961G/G-GE	7970G	7971G-GE
イーサネット接続	Y[1]	Y[2]	Y[1]	Y[3]	Y[1]	Y[4]
イーサネット スイッチ（PC ポート）	Y	Y	Y	Y	Y	Y
Cisco Power-Over-Ethernet（PoE）	Y	Y	Y	Y	Y	Y
IEEE 802.3af Power-Over-Ethernet（PoE）	N	Y	N	Y	Y	Y
ローカリゼーション	N	Y	N	Y	Y	Y
ディレクトリ番号	2	2	6	6	8	8
回線あたりの最大コール数	2	50	2	50	50	50
液晶ディスプレイ	Y	Y	Y	Y	Y	Y
発信者 ID	Y	Y	Y	Y	Y	Y
コール ウェイティング	Y	Y	Y	Y	Y	Y
コール ウェイティング時の発信者 ID	Y	Y	Y	Y	Y	Y
保留	Y	Y	Y	Y	Y	Y
ブラインド転送	Y	Y	Y	Y	Y	Y
初期在席転送	Y	Y	Y	Y	Y	Y
打診転送	Y	Y	Y	Y	Y	Y
自動転送	Y[5]	Y	Y[5]	Y	Y	Y
自動応答	Y[6]	Y[7]	Y[6]	Y	Y	Y
Ad Hoc 会議	Y[8]	Y	Y[8]	Y	Y	Y
Meet-Me 会議	N	Y	N	Y	Y	Y
コール ピックアップ	N	Y	N	Y	Y	Y
グループ ピックアップ	N	Y	N	Y	Y	Y
リダイヤル	Y[9]	Y[9]	Y[9]	Y[9]	Y[9]	Y[9]
短縮ダイヤル	Y[10]	Y[10]	Y	Y	Y	Y
オンフック ダイヤル	N	Y	N	Y	Y	Y
ボイスメールへのアクセス	Y	Y	Y	Y	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y	Y	Y	Y	Y
ビデオ コール	N	N	N	N	N	N
Survivable Remote Site Telephony（SRST）サポート	Y	Y	Y	Y	Y	Y
ユニキャスト MoH	Y	Y	Y	Y	Y	Y
マルチキャスト MoH	Y	Y	Y	Y	Y	Y
保留音	N	N	N	N	N	N
スピーカー	Y	Y[7]	Y	Y	Y	Y
ヘッドセット ジャック	Y	Y	Y	Y	Y	Y
消音	Y	Y	Y	Y	Y	Y
Multilevel Precedence and Preemption（MLPP）	N	N	N	N	N	N
割り込み	N	Y	N	Y	Y	Y
C 割り込み	N	Y	N	Y	Y	Y
General Attribute Registration Protocol（GARP）の無効化	Y	Y	Y	Y	Y	Y

表 19-8　Cisco ビジネス、マネージャ、およびエグゼクティブ IP Phone（SIP 使用）（続き）

機能	7940G	7941G/G-GE	7960G	7961G/G-GE	7970G	7971G-GE
シグナリングおよびメディア暗号化	N	Y	N	Y	Y	Y
シグナリングの完全性	N	Y	N	Y	Y	Y
製造元でインストールされる証明書（X.509v3）	N	Y	N	Y	Y	Y
現場でインストールされる証明書	N	N	N	N	N	N
サードパーティの XML サービス	Y[11]	Y	Y[11]	Y	Y	Y
外部マイクおよびスピーカー	Y	Y	Y	Y	Y	Y
ダイヤル プラン	Y	Y	Y	Y	Y	Y
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0xB8	0xB8	0xB8	0xB8
G.711	Y	Y	Y	Y	Y	Y
G.722	N	N	N	N	N	N
G.723	Y	Y	Y	Y	Y	Y
G.726	N	N	N	N	N	N
G.729	Y[12]	Y[12]	Y[12]	Y[12]	Y[12]	Y[12]
ワイドバンド オーディオ	N	N	N	N	N	N
ワイドバンド ビデオ	N	N	N	N	N	N
音声アクティビティ検出（VAD）	Y	Y	Y	Y	Y	Y
コンフォート ノイズ生成（CNG）	Y	Y	Y	Y	Y	Y
DTMF：H.245	N	N	N	N	N	N
DTMF：SCCP	N	N	N	N	N	N
DTMF：RFC2833	Y	Y	Y	Y	Y	Y
DTMF：KMPL	N	Y	N	Y	Y	Y
DTMF：サブスクライブ / 通知	N	Y	N	Y	Y	Y

1. 2 つの 10/100 Base-T。
2. Cisco Unified IP Phone 7941G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7941GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
3. Cisco Unified IP Phone 7961G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7961GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
4. Cisco Unified IP Phone 7971G は 2 つの 10/100 Mbps イーサネット スイッチを備え、Cisco Unified IP Phone 7971GE は 2 つの 10/100/1000 Mbps イーサネット スイッチを備えています。
5. Cisco Unified IP Phone 7905、7912、7940、または 7960 で SIP を使用する場合、CFWDALL が電話機に設定されているときは、Cisco Unified CallManager で電話機の設定が認識されないので、CFWDALL が機能するには電話機を使用中の状態にする必要があります。この動作は、休止中でも CFWDALL が機能する SCCP 電話機とは異なっています。CFWDALL が Cisco Unified CallManager の User ページで有効にされている場合、Cisco Unified CallManager はこの変更を処理できますが、コールが転送されることを示す状況表示行は電話機にありません。Cisco Unified CallManager の User ページでの CFWDALL 設定は、電話機の設定よりも優先されます。
6. この機能は、電話機でローカルに設定できます。
7. 一方向のオーディオ モニタ モード。
8. IP を使用する Cisco Unified IP Phone 7940 および 7960G でサポートされているのは、Ad Hoc 会議用のローカル ミキシングと最大 3 者による会議だけです。
9. リダイヤル。
10. 短縮ダイヤルは、電話機だけで設定可能です。
11. 限定的なサポート。
12. これらの IP Phone モデルは、受信モードでだけ G.729b と G.729ab をサポートします。

表 19-9　専用エンドポイント

機能	7920	7936	7985G
イーサネット接続	N	Y[1]	Y[2]
イーサネット スイッチ（PC ポート）	N	N	Y
Cisco Power-Over-Ethernet（PoE）	N	N	N
IEEE 802.3af Power-Over-Ethernet（PoE）	N	N	Y
ローカリゼーション	Y	N	Y
ディレクトリ番号	12	1	2
回線あたりの最大コール数	2	2	100
液晶ディスプレイ	Y	Y	Y
発信者 ID	Y	Y	Y
コール ウェイティング	Y	Y	Y
コール ウェイティング時の発信者 ID	Y	Y	Y
保留	Y	Y	Y
ブラインド転送	N	N	N
初期在席転送	Y	Y	Y
打診転送	Y	Y	Y
自動転送	Y	Y	Y
自動応答	N	N	Y
Ad Hoc 会議	Y	Y	Y
Meet-Me 会議	Y	Y	Y
コール ピックアップ	Y	Y	Y
グループ ピックアップ	Y	Y	Y
リダイヤル	Y[3]	Y	Y
短縮ダイヤル	Y	N	Y
オンフック ダイヤル	Y	Y	Y
ボイスメールへのアクセス	Y	N	Y
メッセージ待機インジケータ（MWI）	Y	N	Y
ビデオ コール	N	N	Y
Survivable Remote Site Telephony（SRST）サポート	Y	Y	Y[4]
ユニキャスト MoH	Y	Y	Y
マルチキャスト MoH	Y	Y	N
保留音	Y	Y	Y
スピーカー	N	Y	Y
ヘッドセット ジャック	Y	N	Y
消音	Y	Y	Y
Multilevel Precedence and Preemption（MLPP）	N	N	Y
割り込み	N	N	Y
C 割り込み	N	N	Y
General Attribute Registration Protocol（GARP）の無効化	N	N	N
シグナリングおよびメディア暗号化	Y	N	N

表 19-9　専用エンドポイント（続き）

機能	7920	7936	7985G
シグナリングの完全性	N	N	N
製造元でインストールされる証明書（X.509v3）	N	N	N
現場でインストールされる証明書	N	N	N
サードパーティの XML サービス	Y	N	N
外部マイクおよびスピーカー	N	N	N
シグナリング パケット ToS 値のマーキング	0x60	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8	0x88
G.711	Y	Y	Y
G.722	N	N	Y
G.723	N	N	N
G.726	N	N	N
G.729	Y	Y	Y
ワイドバンド オーディオ	N	N	N
ワイドバンド ビデオ	N	N	N
H.261	N	N	Y
H.263	N	N	Y
H.263+	N	N	Y
H.264	N	N	Y
音声アクティビティ検出（VAD）	Y	Y	Y
コンフォート ノイズ生成（CNG）	Y	Y	Y
DTMF：H.245	N	N	N
DTMF：SCCP	Y	Y	Y
DTMF：RFC2833	N	N	N

1. 1 つの 10/100 Base-T。
2. 2 つの 10/100 Base-T。
3. リダイヤル。
4. SRST ではオーディオだけがサポートされます。

表 19-10　ソフトウェア デバイスの機能

機能	IP Communicator	IP SoftPhone
ディレクトリ番号	8	6
発信者 ID	Y	Y
コール ウェイティング	Y	Y
コール ウェイティング時の発信者 ID	Y	Y
保留	Y	Y
コール転送	Y	Y
自動転送	Y	Y
自動応答	Y	Y
Ad Hoc 会議	Y	Y
Meet-Me 会議	Y	N
コール ピックアップ	Y	N
グループ ピックアップ	Y	N
リダイヤル	Y	Y
短縮ダイヤル	Y	N
オンフック ダイヤル	Y	Y
ボイスメールへのアクセス	Y	Y
メッセージ待機インジケータ（MWI）	Y	Y
ビデオ コール	N	N
Survivable Remote Site Telephony（SRST）サポート	Y	N
Music On Hold（MoH）	Y	Y
スピーカー	Y	Y
消音	Y	Y
Multilevel Precedence and Preemption（MLPP）	Y	Y
割り込み	Y	N
C 割り込み	N	N
General Attribute Registration Protocol（GARP）の無効化	Y	N
シグナリングおよびメディア暗号化	N	N
シグナリングの完全性	N	N
製造元でインストールされる証明書（X.509v3）	N	N
現場でインストールされる証明書	N	N
サードパーティの XML サービス	Y	N
シグナリング パケット ToS 値のマーキング	0x60	0x60
メディア パケット ToS 値のマーキング	0xB8	0xB8
SCCP（Skinny Client Control Protocol）	Y	N
Session Initiation Protocol（SIP）	N	N
H.323	N	Y
メディア ゲートウェイ コントロール プロトコル（MGCP）	N	N

表 19-10　ソフトウェア デバイスの機能（続き）

機能	IP Communicator	IP SoftPhone
Telephony Application Programming Interface（TAPI）	N	Y
G.711	Y	Y
G.722	N	N
G.723	N	Y
G.726	N	N
G.729	Y	Y
ワイドバンド オーディオ	Y	N
ワイドバンド ビデオ	N	N
音声アクティビティ検出（VAD）	Y	N
コンフォート ノイズ生成（CNG）	Y	N

CHAPTER 20

Cisco Unified CallManager アプリケーション

Cisco Unified CallManager アプリケーションは、基本となる IP テレフォニーに多数の動作および機能の拡張を提供します。External eXtensible Markup Language（XML）生産性向上アプリケーションまたは IP Phone Service は、Web サーバまたはほとんどの Cisco Unified IP Phone 上のクライアント（あるいはその両方）で実行できます。たとえば、ユーザのデスク上の IP Phone を使用して、株式相場、天気情報、フライト情報など各種の Web ベースの情報を取得できます。また、カスタム IP Phone サービス アプリケーションを作成すると、ユーザが在庫を追跡したり、時間単位で顧客に課金したり、会議室の環境（照明、ビデオ画面、室温など）を制御できます。Cisco Unified CallManager には、次のような追加機能を提供する統合アプリケーションも多数あります。

- エクステンション モビリティ（EM）

  Cisco Unified CallManager のエクステンション モビリティ機能では、モバイル ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone を独自に設定することが可能です。
- Cisco Unified CallManager Assistant（Unified CM Assistant）

  Unified CM Assistant とは、アシスタントが 1 人以上のマネージャの着信電話コールを処理できるようにする Cisco Unified CallManager に統合されたアプリケーションです。
- Attendant Console（AC）

  Attendant Console を使用すると、1 人以上の受け付け係が組織内でコールに応答および転送（または送信）できます。
- WebDialer

  WebDialer は Cisco Unified CallManager のクリックダイヤル アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できるようになります。

場合によっては、これらの統合アプリケーションが追加機能を提供するために、IP Phone Service を呼び出すこともあります。

この章では、次の Cisco Unified CallManager アプリケーションについて説明します。

- IP Phone Service（P.20-2）
- エクステンション モビリティ（EM）（P.20-8）
- Cisco Unified CallManager Assistant（Unified CM Assistant）（P.20-14）
- Attendant Console（P.20-29）
- WebDialer（P.20-40）

IP Phone Service

Cisco Unified IP Phone サービス は、Web クライアントやサーバ、および Cisco Unified IP Phone の XML 機能を利用するアプリケーションです。Cisco Unified IP Phone のファームウェアには、限定的な Web ブラウジング機能を可能にするマイクロブラウザが含まれています。これらの電話サービス アプリケーションは、ユーザのデスクトップ電話機上で直接実行することで、付加価値サービスと生産性向上の可能性を提供します。この章で「電話サービス」という用語は、Cisco Unified IP Phone を宛先および発信元としてコンテンツを送受信するアプリケーションを指します。

IP Phone Service をサポートする電話機

次の電話機は IP Phone Service をサポートしています。

- Cisco Unified IP Phone 7940G、7941G、および 7941G-GE
- Cisco Unified IP Phone 7960G、7961G、および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

IP Phone Service は次の IP Phone でも実行できます。ただし、これらの電話機モデルは、テキストベースの XML アプリケーションだけをサポートします。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified IP Phone 7920

上記のすべての IP Phone は、電話機と実行中の電話サービスを含む Web サーバの間でユーザ インターフェイス（UI）を有効にするために、Cisco が定義する XML オブジェクトの限定されたセットを処理できます。

上記の電話機は、Skinny Client Control Protocol（SCCP）と Session Initiation Protocol（SIP）の両方で電話サービスをサポートすることに注意してください。

Cisco Unified CallManager サービスと IP Phone Service のエンタープライズ サービス パラメータ

IP Phone Service を有効にするには、システム管理者は Cisco Unified CallManager Serviceability インターフェイスから Cisco Unified CallManager 機能サービスをアクティブにし、起動する必要があります。また、管理者は Cisco Unified CallManager のサービス パラメータを使用すると、Cisco Unified CallManager の特定の部分とアプリケーションの動作をカスタマイズし、設定することができます。次の項で説明するように、IP Phone Service に対して設定およびカスタマイズのためのオプションを提供するエンタープライズ サービス パラメータがいくつかあります。

IP Phone Service の Cisco Unified CallManager サービス

IP Phone Service はその機能を、Cisco Unified CallManager 上の Cisco Unified CallManager Cisco Unified IP Phone Service の機能サービスに依存しています。この機能は、Cisco Unified CallManager がサーバにインストールされたときにデフォルトでインストールされますが、システム管理者はこの機能を手動でアクティブにする必要があります。

IP Phone Service の エンタープライズ サービス パラメータ

IP Phone Service には、関連するいくつかのエンタープライズ サービス パラメータがあります。次の項目は、IP Phone Service および IP Phone の XML 処理に関連する、Cisco Unified CallManager Enterprise Service Parameters 設定ページの Phone URL Parameters セクションにある設定パラメータの一部です。

- URL Authentication（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/authenticate.jsp）

  この URL は、Cisco Unified CallManager の authenticate.jsp サービスを指します。このサービスは、Cisco Unified IP Phones と Cisco Unified CallManager の間で認証プロキシ サービスを提供します。この URL は、電話サービスによって電話機に直接行われた「プッシュ」要求を検証するために使用されます。これは、インストール時に自動的に設定されます。このパラメータに値を指定しない場合、電話サービスは電話機にコンテンツをプッシュできません。

- URL Directories（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/xmldirectory.jsp）

  この URL は、Cisco Unified CallManager の xmldirectory.jsp サービスを指します。このサービスは、ユーザが電話機の Directories（またはブック アイコン）ボタンを押したときに表示されるディレクトリ メニューを生成して返します。この URL は、インストール時に自動的に設定されます。このパラメータに値を指定しないと、ユーザが Directories ボタンを押したときに、ディレクトリ メニューを利用できません。

- URL Idle（デフォルト値 = < *ブランク* >）

  指定された場合、この URL は、電話機がアイドル状態のときに電話機の画面に表示されるテキストまたはイメージを提供するサービスを指します。このパラメータは、サービスを開始するまでの電話機のアイドル時間を示す URL Idle Time パラメータと密接に関連しています。デフォルトで、このパラメータはインストール時にブランクのままになります（設定されません）。

- URL Idle Time（デフォルト値 = 0）

  このパラメータは、電話機が URL Idle サービスを開始するまでに待機する時間を秒単位で示します。デフォルトで、このパラメータはインストール時に 0（ゼロ）に設定され、電話機がアイドル状態にならないことを示します。

- URL Information（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/GetTelecasterHelpText.jsp）

  この URL は、Cisco Unified CallManager の GetTelecasterHelpText.jsp サービスを指します。このサービスは、ユーザが（キーボードの右側にある）Help（「i」または「?」）ボタンを押したときに電話機のキーおよびコール統計に関する画面上の電話機ヘルプを生成して返します。この URL は、インストール時に自動的に設定されます。このパラメータに値を指定しないと、Help ボタンを押したときにヘルプ情報が表示されません。

- URL Services（デフォルト値 = http://<*CM_IP_address*>:8080/ccmcip/getservicesmenu.jsp）

  この URL は、Cisco Unified CallManager の getservicesmenu.jsp サービスを指します。このサービスは、Services（または地球のアイコン）ボタンを押したときに電話機のユーザ加入電話サービスのリストを表示します。これは、インストール時に自動的に設定されます。このパラメータに値を指定しないと、Services ボタンを押したときに加入サービスのリストが表示されません。

IP Phone Service のアーキテクチャ

IP Phone サービスは、次のような複数の方法で開始できます。

- ユーザ起動（プル）

  IP Phone ユーザが Services ボタンを押すと、ユーザ加入電話サービスのリストを表示するために、HTTP GET メッセージが Cisco Unified CallManager に送信されます。図 20-1 は、この機能を示しています。

- 電話機起動（プル）

  IP Phone ファームウェア内で、アイドル時間の値は URL Idle Time パラメータによって設定できます。このタイムアウト値を超えた場合、IP Phone のファームウェア自体が URL Idle パラメータで指定されるアイドル状態の URL の場所に対して、HTTP GET を開始します。

- 電話サービス起動（プッシュ）

  電話サービス アプリケーションは、電話機に HTTP POST メッセージを送信することによって、IP Phone にコンテンツをプッシュできます。

(注) 電話サービスを呼び出すために電話機の Web クライアントが使用されるユーザ起動および電話機起動のプル機能とは異なり、電話サービス起動のプッシュ機能は、電話機の（クライアントではなく）Web サーバに（HTTP POST を通じて）コンテンツをポストすることによって、電話機上の処理を呼び出します。

図 20-1 は、ユーザが開始する IP Phone サービス処理の詳細を示しています。ユーザが Services ボタンを押したときに、デフォルトでは、HTTP GET メッセージが IP Phone から Cisco Unified CallManager の getservicesmenu.jsp スクリプトに送信されます（ステップ 1）。URL Services パラメータを変更すると、異なるスクリプトを指定できます（P.20-3 の「IP Phone Service の エンタープライズ サービス パラメータ」を参照してください）。getservicesmenu.jsp スクリプトは、個々のユーザが加入している電話サービス URL ロケーションのリストを返します（ステップ 2）。HTTP 応答は、IP Phone にこのリストを返します（ステップ 3）。ユーザによって選択される追加の電話サービス メニュー オプションは、ユーザと選択された電話サービス アプリケーションを含む Web サービス間で HTTP メッセージングを継続します（ステップ 4）。

図 20-1　ユーザ起動の IP Phone Service のアーキテクチャ

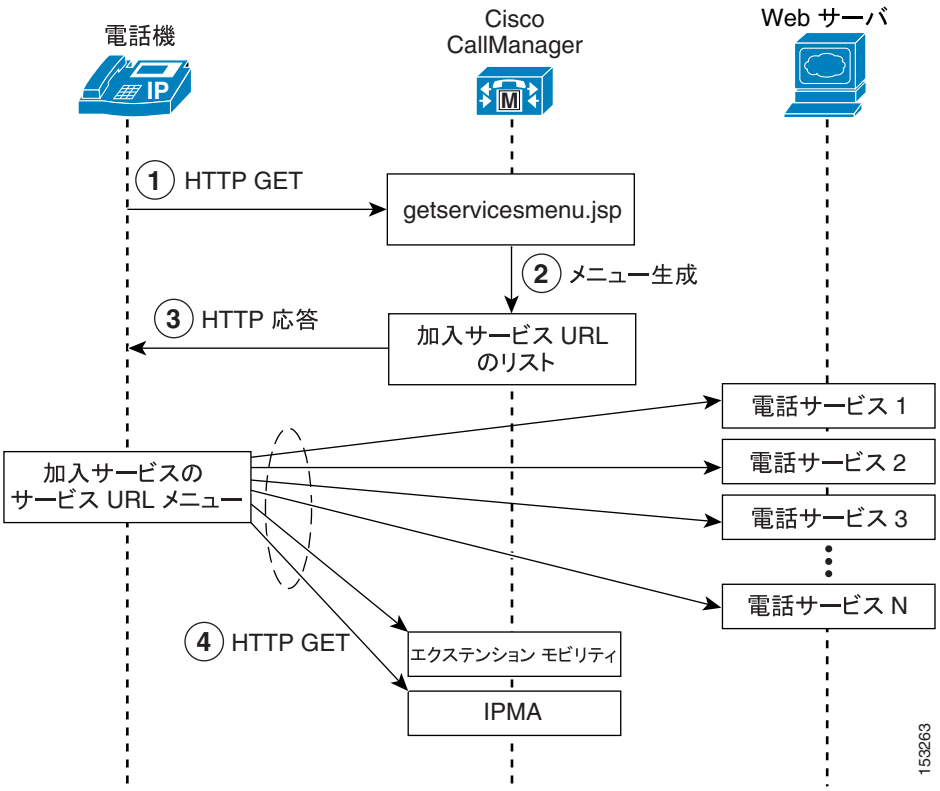
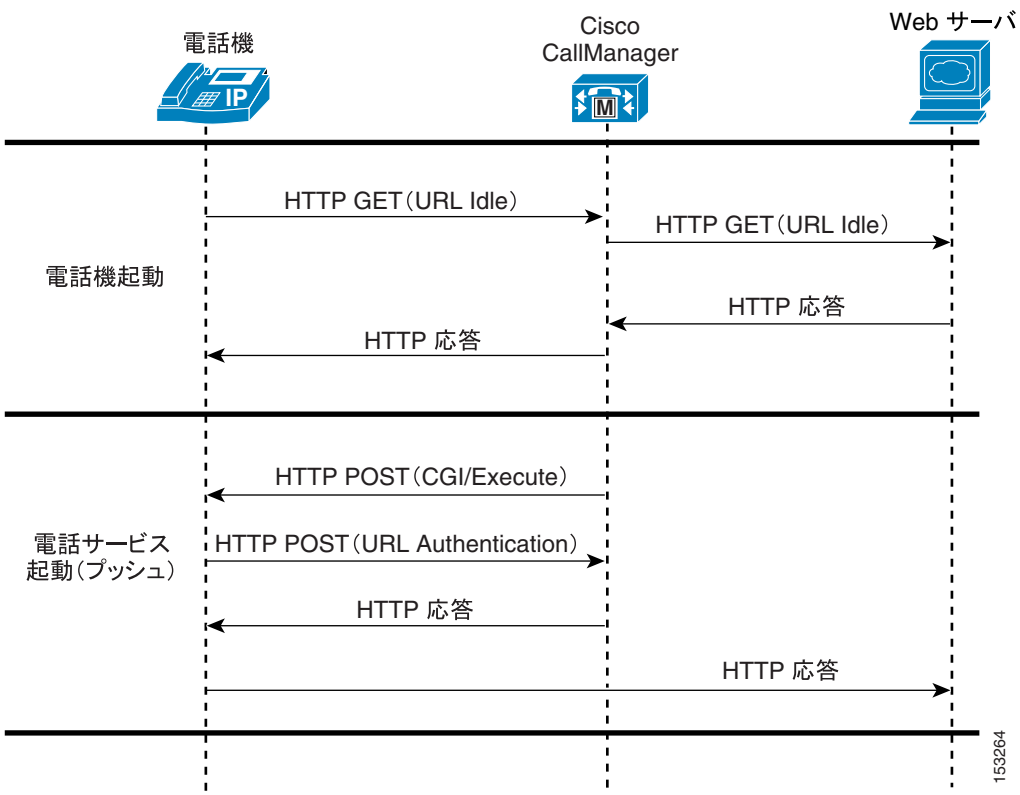


図 20-2 は、電話機起動と電話サービス起動の両方のプッシュ機能の例を示しています。電話機起動の機能の例で、電話機は、URL Idle Time に達したときに URL Idle パラメータで指定されるロケーションに HTTP GET を自動的に送信します（P.20-3 の「IP Phone Service の エンタープライズ サービス パラメータ」を参照してください）。HTTP GET は、Cisco Unified CallManager を通じて外部 Web サーバに転送されます。この Web サーバは HTTP 応答を返し、この応答は Cisco Unified CallManager によって電話機にリレーされ、電話機は画面にテキストまたはイメージ（あるいはその両方）を表示します。

電話サービス起動のプッシュの例で、外部 Web サーバ上の電話サービスは電話機の Web サーバに対して、Common Gateway Interface（CGI）または Execute 呼び出しで HTTP POST を送信します。CGI または Execute 呼び出しを実行する前に、電話機は URL Authentication パラメータで指定されるプロキシ認証サービスを使用して要求を認証します（P.20-3 の「IP Phone Service の エンタープライズ サービス パラメータ」を参照してください）。このプロキシ認証サービスは、電話機に対する直接の要求を検証するための、電話機と Cisco Unified CallManager ディレクトリ間のインターフェイスを提供します。要求が認証された場合、Cisco Unified CallManager は電話機に HTTP 応答を転送します。次に、電話機の Web サーバは要求された処理を実行し、電話機は外部 Web サーバに HTTP 応答を返します。認証に失敗した場合、Cisco Unified CallManager は、HTTP 否定応答を転送し、電話機は要求された CGI または Execute 処理を実行しないで、HTTP 否定応答を外部 Web サーバに転送します。

図 20-2　電話機起動および電話サービス起動の IP Phone Service のアーキテクチャ



IP Phone Service の冗長性

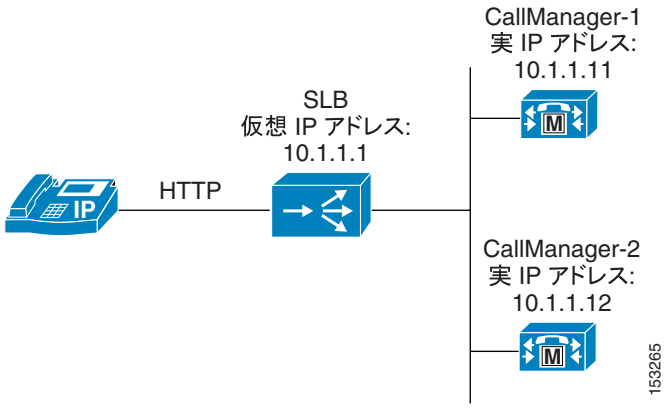
電話機のユーザに対して信頼性の高いサービスを確保するには、システムの障害時に冗長システムにシームレスに移行することにより、高レベルのシステムの可用性を維持する必要があります。電話サービスのほとんどのバックエンド処理は Web サーバで発生しますが、電話機は電話サービスへの処理の転送を Cisco Unified CallManager に依存します。また、エクステンション モビリティおよび Cisco Unified CallManager Assistant 電話サービスの場合、実際にはサービスが Cisco Unified CallManager サーバで実行されます。

図20-1 および図20-2 に示す IP Phone サービス機能のアーキテクチャおよびメッセージ フローでは、次の 2 つの主な障害のシナリオを検討する必要があります。

障害シナリオ 1：Cisco Unified CallManager の Cisco Unified IP Phone Service サーバの障害

この場合の冗長性は、図 20-3 に示すように、一種の Server Load Balancing（SLB; サーバ ロード バランシング）に依存します。この SLB では、1 つ以上の Cisco Unified CallManager サーバを指すために仮想 IP アドレスが使用されます。この仮想 IP アドレスは、URL Services パラメータの設定時に使用されます。このため、Cisco Unified CallManager サーバに障害が発生しても、電話機の Services ボタンが押されたときに、IP Phone Service 加入リストは電話機に正常に返されます。また、Cisco Unified CallManager サーバで実行されるエクステンション モビリティおよび Unified CM Assistant などの電話サービスも、この方法によって冗長性を持つ可能性があります。

図 20-3　電話サービスに冗長性を提供する方法



障害シナリオ 2：特定の IP Phone Service をホストしている外部 Web サーバの障害

このシナリオでは、Cisco Unified CallManager サーバへの接続は保持されますが、ユーザ加入電話サービスをホストしている Web サーバへのリンクに障害が発生します。Services ボタンが押されたときに IP Phone は引き続き Cisco Unified CallManager サーバにアクセスできるため、これは冗長性を提供するための比較的容易なシナリオです。この場合、IP Phone は Web サーバにアクセスする他の IP Phone に似ています。このため、（図 20-3 に示すような）一種の SLB 機能を再び使用して、電話機から、ユーザ加入電話サービスをホストしている 1 つ以上の冗長 Web サーバに HTTP 要求を転送できます。

IP Phone Service のスケーラビリティ

Cisco Unified IP Phone サービスの大部分は、HTTP クライアントとして機能します。ほとんどの場合、加入サービスのロケーションへの転送サーバとしてだけ Cisco Unified CallManager が使用されます。Cisco Unified CallManager は電話サービスへの転送サーバとして機能するため、ユーザが Services キーを押して電話サービス要求を起動したときに、Cisco Unified CallManager へのパフォーマンスの影響は最小限になります。

(注)　エクステンション　モビリティおよび　Unified CM Assistant　電話サービスの場合、Cisco　Unified CallManager は転送サーバ以上の役割を果たすので、パフォーマンスへの影響を検討する必要があります。これらのアプリケーションの特定のパフォーマンスおよびスケーラビリティの考慮事項については、P.20-8 の「エクステンション モビリティ（EM）」および P.20-14 の「Cisco Unified CallManager Assistant（Unified CM Assistant）」の項を参照してください。

IP Phone はクライアントまたはサーバのいずれかであるため、IP Phone サービスで使用される必要帯域幅の推定は、Web 運用サーバにある HTTP コンテンツと同じテキストにアクセスする HTTP ブラウザの帯域幅の推定に似ています。

IP Phone Service のガイドラインと制限

統合エクステンション モビリティおよび Unified CM Assistant アプリケーションの電話サービスを除き、IP Phone　サービスは独立した　Web　サーバに存在する必要があります。Cisco　Unified CallManager サーバでエクステンション モビリティおよび IP Manager Application 以外の電話サービスを実行することはサポートされていません。

エクステンション モビリティ（EM）

Cisco Unified CallManager の Extension Mobility（EM; エクステンション モビリティ）機能では、ユーザがその電話機にログインすることで、一時的に Cisco Unified IP Phone を独自に設定することが可能です。ユーザがログインすると、IP Phone は、回線番号、短縮ダイヤル、サービス リンク、およびその他のユーザ固有の電話機のプロパティなど、ユーザの個別のデバイス プロファイル情報を受け入れます。たとえば、ユーザ X がデスクに向かって電話機にログインした場合は、そのユーザのディレクトリ番号、短縮ダイヤル、およびその他のプロパティがその電話機に表示されますが、ユーザ Y が別のときに同じデスクを使用した場合は、ユーザ Y の情報が表示されます。EM 機能では、認証されたユーザのデバイス プロファイルに従って電話機が動的に設定されます。このアプリケーションの利点は、電話機が EM をサポートしている限り、物理的な場所に関係なく、ユーザが Cisco Unified CallManager クラスタ内の任意の電話機で自分の内線番号に接続できることです。

EM Phone のサポート

次の Skinny Client Control Protocol（SCCP）電話機は EM をサポートしています。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified IP Phone 7920
- Cisco Unified IP Phone 7940G、7941G、および 7941G-GE
- Cisco Unified IP Phone 7960G、7961G、および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

次の Session Initiation Protocol（SIP）Phone は、EM をサポートしています。

- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7941G および 7941G-GE
- Cisco Unified IP Phone 7961G および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

（注） EM は、SIP ロードを実行している Cisco Unified IP Phone 7905G、7912G、7940G、または 7960G ではサポートされません。

Cisco Unified CallManager および EM のサービス パラメータ

EM アプリケーションを有効にするには、システム管理者は Cisco Unified CallManager Serviceability インターフェイスからいくつかの Cisco Unified CallManager サービスをアクティブにし、起動する必要があります。また、EM サービス パラメータは、EM アプリケーションの動作を決定するための設定およびカスタマイズのオプションを提供します。

EM 用の Cisco Unified CallManager サービス

EM アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco エクステンション モビリティ
- Cisco Unified CallManager の Cisco Unified IP Phone Service

EM は、ネットワーク サービスの Cisco エクステンション モビリティ アプリケーションにも依存します。このサービスは、インストール時に Cisco Unified CallManager で自動的にアクティブになります。

Cisco エクステンション モビリティ アプリケーション サービスは、EM ユーザ電話機と Cisco エクステンション モビリティ サービスとの間のインターフェイスを提供します。また、Cisco エクステンション モビリティ アプリケーション サービスは、クラスタ内の変更通知インジケータにサブスクライブして、アクティブな Cisco エクステンション モビリティ サービスがあるクラスタ内のノードのリストを維持します。クラスタ内の変更通知にサブスクライブすることによって、EM サービス パラメータに変更を加えた後に、Cisco Tomcat ネットワーク サービスおよび Cisco エクステンション モビリティ機能サービスを再起動する必要がなくなります。

Cisco Unified CallManager の Cisco Unified IP Phone Service サービスは、EM 電話サービスへのアクセスを提供するために必要です。EM 電話サービスの定義に使用される URL は、次のとおりです。

http://<*Publisher_IP-Address*>:8080/emapp/EMAppServlet?device=#DEVICENAME#

次の例を参考にしてください。

http://10.1.1.1:8080/emapp/EMAppServlet?device=#DEVICENAME#

EM のサービス パラメータ

次の項目は、エクステンション モビリティ機能に関連する Cisco EM サービス パラメータの一部のリストです。

- Enforce Maximum Login Time（デフォルト値 = False）

  このパラメータは、Maximum Login Time に達したときに、EM ユーザを自動的にログアウトするかどうかを示します。デフォルトでは、この値は False に設定され、EM ユーザを自動的にログアウトしません。

- Maximum Login Time（デフォルト値 = 8:00）

  このパラメータは、EM ユーザが自動的にログアウトするまでにログイン状態を維持できる時間と分（*hh*:*mm*）を示します。Enforce Maximum Login Time パラメータを True に設定した場合にだけ、指定した時刻に自動ログアウトが行われます。

- Multiple Login Behavior（デフォルト値 = Multiple Logins Not Allowed）

  このパラメータは、同時に複数のデバイスにログインすることを EM ユーザに許可するかどうかを示します。デフォルトでは、1 人のユーザの複数のログインは許可されず、1 台のデバイスにログオンしているときに別のデバイスにログインしようとすると、次のメッセージが表示されます。

  ```
  Login Unsuccessful
  [25]User logged in elsewhere.
  ```

- Remember the Last User Logged In（デフォルト値 = False）

  このパラメータは、デバイスへのログインに前回使用されたユーザ ID を、次回同じデバイスにログインしようとするときまで記録するかどうかを示します。この値を True に設定すると、前回のログインに使用されたユーザ ID 情報は Cisco Unified CallManager データベースのテーブルに保存され、効率的に取得されます。次回のログイン試行時に、電話機のログイン画面の UserID フィールドには、保存されたユーザ ID の値があらかじめ表示されます。

- Clear the call log（デフォルト値 = False）

  このパラメータは、EM ログインおよびログアウト時に、Directories ボタン メニューに指定されたコール ログをクリアするかどうかを指定します。このパラメータは、Missed Calls、Received Calls、および Placed Calls のログに影響を与えます。この値を True に設定した場合、これらのログはログインおよび手動ログアウト時にクリアされます。

例外として、ユーザを自動的にログアウトする場合、これらのログはクリアされません。したがって、Maximum Login Time に達してユーザを電話機から自動的にログアウトするときに、ログはクリアされません（Enforce Maximum Login Time が True に設定されている場合）。同様に、Cisco Unified CallManager 管理者が、電話機またはデバイスの設定画面の Extension セクションで Log Out ボタンをクリックした場合も、ログはクリアされません。

EM のアーキテクチャ

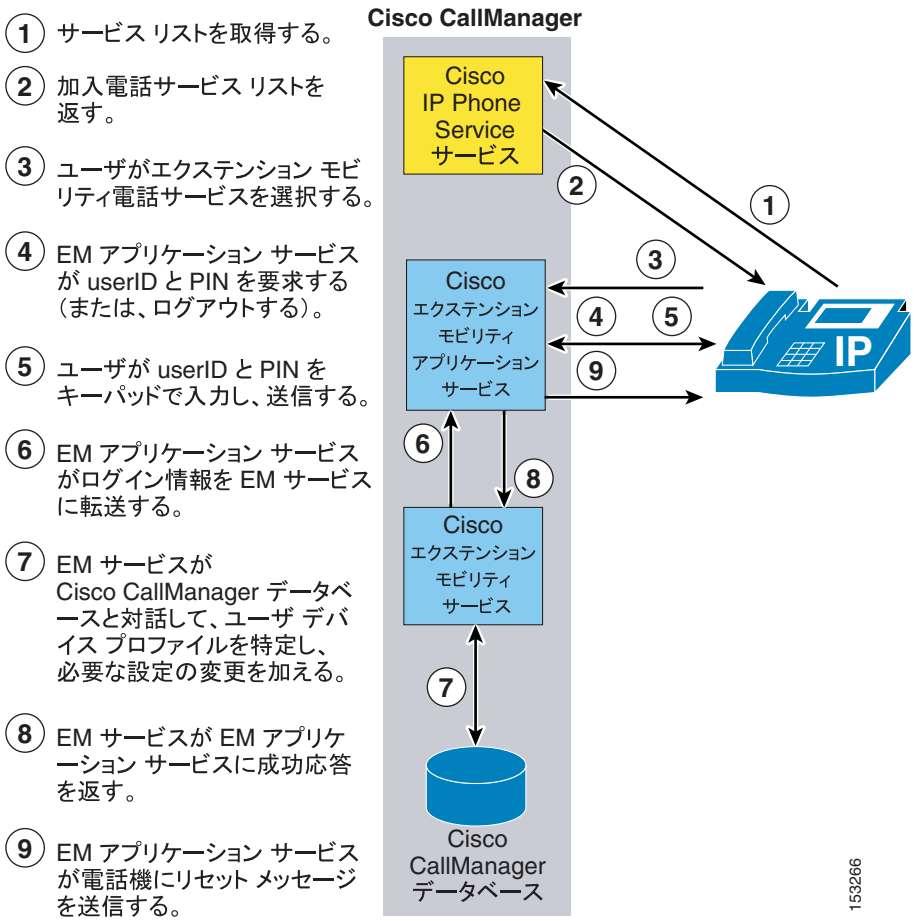
図 20-4 は、EM アプリケーションのメッセージ フローとアーキテクチャを示しています。電話機のユーザが EM アプリケーションにアクセスする場合、次の一連のイベントが発生します。

1. ユーザが電話機の Services ボタンを押すと、Enterprise Parameter 設定ページの URL Services パラメータで指定した URL へのコールが生成されます（P.20-3 の「IP Phone Service の エンタープライズ サービス パラメータ」を参照）（図 20-4 のステップ 1 も参照）。
2. HTTP/XML コールが IP Phone Service に対して生成され、このコールはユーザの電話機が加入しているすべてのサービスのリストを返します（図 20-4 のステップ 2 を参照）。

（注）ユーザの電話機の EM に対して Service URL ボタンを設定すると、ユーザが回線ボタンまたは短縮ダイヤル ボタンを押して、エクステンション モビリティ アプリケーション サービスへの直接コールを生成できます。この場合、電話機と IP Phone Service（ステップ 1 および 2）の対話はバイパスされます。

3. 次に、ユーザはエクステンション モビリティ電話サービスのリストを選択します。この選択によって、電話機と Cisco エクステンション モビリティ サービス間のインターフェイスの役割を果たす エクステンション モビリティ アプリケーション サービスに対して HTTP コールが生成されます（図 20-4 のステップ 3 を参照）。
4. 次に、エクステンション モビリティ アプリケーション サービスは、ユーザ ログイン クレデンシャル（ユーザ ID および PIN）を要求している電話機に XML 応答を返すか、またはユーザがすでにログインしている場合は、ユーザに電話機からログオフするかどうかを尋ねる応答を返します（図 20-4 のステップ 4 を参照）。
5. ユーザがログインしようとしている場合、そのユーザは電話機のキーパッドを使用して有効なユーザ ID および PIN を入力する必要があります。ユーザが Submit ソフトキーを押した後に、入力したユーザ ID および PIN を含む応答が、エクステンション モビリティ アプリケーション サービスに返されます（図 20-4 のステップ 5 を参照してください）。
6. 次に、エクステンション モビリティ アプリケーションは、このログイン情報を エクステンション モビリティ サービスに転送します。このサービスは、Cisco Unified CallManager データベースと対話して、ユーザのクレデンシャルを検証します（図 20-4 のステップ 6 を参照）。
7. ユーザのクレデンシャルの検証に成功したときに、エクステンション モビリティ サービスも Cisco Unified CallManager データベースと対話して、適切なユーザ デバイス プロファイルを読み取って選択し、デバイスのプロファイルに基づいて電話機の設定に必要な変更を書き込みます（図 20-4 のステップ 7 を参照）。
8. これらの変更が加えられると、エクステンション モビリティ サービスは、エクステンション モビリティ アプリケーション サービスに成功応答を返します（図 20-4 のステップ 8 を参照）。
9. 次にエクステンション モビリティ アプリケーション サービスは電話機にリセット メッセージを送信し、電話機はリセットされ、新しい電話設定を受け入れます（図 20-4 のステップ 9 を参照）。

図 20-4　EM アプリケーションのアーキテクチャとメッセージ フロー



EM の冗長性

図 20-4 に示す EM アーキテクチャに従って、Cisco Unified CallManager データベースの読み取りおよび書き込みが要求されます。現在の Cisco Unified CallManager クラスタ アーキテクチャに基づいて、パブリッシャ サーバは Cisco Unified CallManager データベースに書き込むことができる唯一のノードです。したがって、EM 機能はパブリッシャ サーバに依存します。パブリッシャを使用できない場合、EM のログインとログアウトは行えません。パブリッシャの冗長性メカニズムは存在しないため、パブリッシャは EM 動作における単一の障害点になります。このため、EM に必要な 3 つのサービス（IP Phone Service、エクステンション モビリティ、および エクステンション モビリティ アプリケーション サービス）をすべてパブリッシャで実行することをお勧めします。パブリッシャを使用できない場合、クラスタ内の他のノードでこれらのサービスを実行しても、機能が提供されないため意味がありません。

（注） エクステンション モビリティ アプリケーション サービスは、クラスタ内のすべてのノードで常にアクティブになり、実行されます。ただし、EM 電話サービスを設定する場合は、常にパブリッシャ ノードを指すように Service URL を設定してください。

前述したように、エクステンション モビリティ アプリケーション サービスはクラスタの変更通知にサブスクライブするので、エクステンション モビリティ サービスがアクティブになっているクラスタ内のすべてのノードのリストを維持します。したがって、エクステンション モビリティ サービスはクラスタ内の複数のサーバで実行でき、エクステンション モビリティ アプリケーション サービスはエクステンション モビリティ サービスを実行している他のノードに対して自動フェールオーバーを提供できます。ただし、この自動フェールオーバーは、エクステンション モビリティ サービスだけを対象としています。これは、パブリッシャでエクステンション モビリティ サービスに障害が発生しても、その他すべてのサービス、Cisco Unified CallManager データベース、およびノード自体が動作している非常にまれな状況を除き、実際のエクステンション モビリティ機能に対してフェールオーバーを提供しません。一般に、障害シナリオは 1 つのサービスだけではなく、ノード全体、ノード アップリンク スイッチ、またはスイッチ ポートが関係します。したがって、EM 冗長性に関して、パブリッシャ以外のノードで必要なエクステンション モビリティ サービスまたは IP Phone Service を実行する必要はありません。ただし、管理者は、クラスタ内の追加のノードでエクステンション モビリティ サービスを実行することにより、前述のまれな障害シナリオに対して、このサービスの冗長性を提供できます。図 20-3 に示すように、SLB および仮想 IP アドレスと実際の IP アドレス間のマッピングを通じて、IP Phone Service およびエクステンション モビリティ アプリケーション サービスに対して追加の冗長性を提供することもできます。ただし、この方法では、パブリッシャでこれらのサービスすべてに障害が発生しても、パブリッシャおよび Cisco Unified CallManager データベースが動作し続け、EM ログイン要求およびログアウト要求を処理しているまれな状況だけに冗長性を提供します。

EM のガイドラインと制限

次のガイドラインと制限は、Cisco Unified CallManager テレフォニー環境内の EM の配置と動作に関連して適用されます。

- EM は、単一の Cisco Unified CallManager クラスタ内だけでサポートされます。

  現在、クラスタ間で EM はサポートされていません。ある Cisco Unified CallManager クラスタの EM ユーザは、2 番目のクラスタでそのユーザに対して別個のデバイス プロファイルおよびユーザ ID が作成されない限り、2 番目のクラスタで電話機にログオンすることはできません。

- EM ユーザは、Automated Alternate Routing（AAR）または Voice over PSTN（VoPSTN）、あるいはその両方の配置モデルが使用されている場合、クラスタ内のロケーションまたはサイト間で移動することはできません。

  EM 機能は、コール ルーティングを IP ネットワークの使用に依存します。E.164 公衆網番号は静的で、公衆網はホーム サイトからの EM ユーザのディレクトリ番号（DN）の移動を考慮に入れられないため、公衆網を通じたコール ルーティングにはより多くの問題が伴います。AAR は、VoPSTN 配置モデルと同様に、コール ルーティングを公衆網に依存します。いずれの場合も、ロケーションおよびサイト間の EM ユーザの移動は、ユーザの移動するすべてのサイトが同じ AAR グループに属する場合にだけサポートされます。詳細については、P.10-31 の「エクステンション モビリティ」を参照してください。

- EM 機能は、Cisco Unified CallManager パブリッシャ サーバに完全に依存しています。

  Cisco Unified CallManager パブリッシャがダウンしている場合、EM ユーザは電話機にログオンしたり、電話機からログオフしたりすることができません。

EM のパフォーマンスとキャパシティ

Cisco EM アプリケーションは、ログインおよびログアウト機能をパブリッシャ サーバに依存します。EM は、次のパブリッシャ キャパシティをサポートしています。

- Cisco MCS-7845 サーバは、1 分あたり 50 回の順次ログインまたはログアウト（あるいはその両方）をサポートできます。
- Cisco MCS-7835 サーバは、1 分あたり 30 回の順次ログインまたはログアウト（あるいはその両方）をサポートできます。

EM のキャパシティの詳細については、次の Web サイトにある Cisco Unified CallManager のデータシート、マニュアル、およびリリース ノートを参照してください。

http://www.cisco.com

EM 相互作用：Unified CM Assistant、AC、および WebDialer

Unified CM Assistant Manager ユーザと Attendant Console ユーザの両方が、それぞれの電話機へのログインに EM を使用できます。このような他のアプリケーションでの EM の使用に関する詳細とガイドラインについては、P.20-28 の「Unified CM Assistant と EM の相互作用」および P.20-38 の「AC と EM の相互作用」を参照してください。

WebDialer ユーザも、EM を使用してそれぞれの電話機にログオンできます。詳細については、P.20-48 の「WebDialer と EM の相互作用」を参照してください。

Cisco Unified CallManager Assistant（Unified CM Assistant）

Cisco Unified CallManager Assistant は、Cisco Unified CallManager に統合されたアプリケーションであり、1 人以上のマネージャに代わってアシスタントが着信コールを処理できるようにします。Unified CM Assistant Console デスクトップ アプリケーションを使用すると、アシスタントが手早くマネージャの状態を確認し、コールをどうするかを決定できます。アシスタントは、自分の電話機のソフトキーを使用したり、キーボード ショートカットまたはドロップダウン メニューで PC インターフェイスを使用したり、コールをマネージャのプロキシ回線にドラッグ アンド ドロップしたりすることで、コールを操作することができます。

Unified CM Assistant Phone のサポート

次の SCCP 電話機が Unified CM Assistant をサポートしています。

- Cisco Unified IP Phone 7940G、7941G、および 7941G-GE
- Cisco Unified IP Phone 7960G、7961G、および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

(注) Cisco Unified IP Phone Expansion Module 7914 は、Csco Unified IP Phone 7960G、7961G、7961G-GE、7970G、または 7971G-GE のすべての電話機でサポートされています。電話機あたり最大 2 つの Cisco 7914 Module がサポートされています。

SIP 電話機では、Unified CM Assistant はサポートされていません。

Cisco Unified CallManager および Unified CM Assistant のサービス パラメータ

Unified CM Assistant　アプリケーションを有効にするには、システム管理者は　Cisco　Unified CallManager Serviceability インターフェイスから複数の Cisco Unified CallManager 機能サービスをアクティブにし、起動する必要があります。また、Unified CM Assistant サービス パラメータは、Unified CM Assistant アプリケーションとサービスの動作を決定するための設定およびカスタマイズのオプションを提供します。

Unified CM Assistant 用の Cisco Unified CallManager サービス

Unified CM Assistant アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco Unified CallManager Assistant
- Cisco CTIManager
- Cisco Unified CallManager の Cisco Unified IP Phone Service

Cisco CallManager IP Manager Assistant サービスは、Unified CM Assistant Console アプリケーションおよび Manager Configuration アプリケーション用のインターフェイスを提供し、Cisco CTIManager サービスおよび Cisco Unified CallManager データベースと対話します。Cisco CTIManager サービスは、電話とコールの制御のために Cisco CallManager Service および Cisco CallManager IP Manager Assistant サービスとインターフェイスし、対話します。

Cisco Unified IP Phone Service は、マネージャの電話機から Unified CM Assistant 電話サービスへのアクセスを提供するために必要です。Unified CM Assistant 電話サービスを定義するために使用される URL は、次のとおりです。

http://<*Server_IP-Address*>:8080/ma/servlet/MAService?cmd=doPhoneService&Name=#DEVICENAME#

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

Unified CM Assistant のサービス パラメータ

次の項目は、Unified CM Assistant 機能に関連する Cisco CallManager IP Manager Assistant サービス パラメータの一部のリストです。

- CTIManager Connection Security Flag（デフォルト値 = False）

  このパラメータは、Cisco CallManager IP Manager Assistant サービスと CTIManager との間でセキュアな Transport Layer Security（TLS; トランスポート レイヤ セキュリティ）接続を使用するかどうかを決定します。このパラメータを True に設定した場合、アプリケーション ユーザの Unified CM AssistantSecureSysUser のインスタンス ID に対して設定した Certificate Authority Proxy Function（CAPF）プロファイルを使用して、セキュアな接続が設定されます。このインスタンス ID は、サービス パラメータの CAPF Profile Instance ID for Secure Connection to CTIManager で指定する必要があります。

  （注） アプリケーション ユーザの Unified CM AssistantSecureSysUser は、インストール時に自動的に作成されるシステム アカウントです。削除することはできません。

- CAPF Profile Instance ID for Secure Connection to CTIManager（デフォルト値 = <None>）

  CAPF Profile Instance ID は、Unified CM AssistantSecureSysUser アプリケーション ユーザに対して、Unified CM Assistant サーバと CTIManager との間で確立される TLS 接続またはインスタンスを識別するために使用される、数値または文字（あるいはその両方）の一意のストリングです。CTI Manager Connection Security Flag パラメータを True に設定した場合、このパラメータに値を設定する必要があります

- CTIManager (Primary) IP Address（デフォルト値 = < ブランク >）

  このパラメータは、Cisco Unified CM Assistant サーバがコールの処理に使用するプライマリ CTIManager の IP アドレスを指定します。プライマリ CTIManager は、各 Unified CM Assistant サーバで設定できます。

- CTIManager (Backup) IP Address（デフォルト値 = < ブランク >）

  このパラメータは、プライマリ CTIManager がダウンしている場合に、この Cisco Unified CM Assistant サーバがコールの処理に使用するバックアップ CTIManager の IP アドレスを指定します。バックアップ CTIManager は、各 Unified CM Assistant サーバで設定できます。

- Cisco Unified CM Assistant Server (Primary) IP Address（デフォルト値 = < ブランク >）

  このパラメータは、プライマリ Cisco Unified CM Assistant サーバの IP アドレスを指定します。これはクラスタ全体のパラメータで、プライマリとバックアップという 2 つの Unified CM Assistant サーバだけを設定できます。

- Cisco Unified CM Assistant Server (Backup) IP Address（デフォルト値 = < ブランク >）

  このパラメータは、バックアップ Cisco Unified CM Assistant サーバの IP アドレスを指定します。バックアップ サーバは、プライマリ Unified CM Assistant サーバに障害が発生した場合に、Unified CM Assistant サービスを提供します。これはクラスタ全体のパラメータです。

- Cisco Unified CM Assistant Console Heartbeat Interval（デフォルト値 = 30）

  このパラメータは、Unified CM Assistant サーバが、各 Unified CM Assistant Console デスクトップ アプリケーションにキープアライブ メッセージ（ハートビートとも呼ばれる）を送信する頻度を秒単位で指定します。Unified CM Assistant Console デスクトップ アプリケーションは、指定された時間が経過するまでにプライマリ サーバからキープアライブ メッセージを受信しないと、バックアップ Unified CM Assistant サーバへのフェールオーバーを開始します。

- Cisco Unified CM Assistant Console Request Timeout（デフォルト値 = 30）

  このパラメータは、Unified CM Assistant Console デスクトップ アプリケーションが、アクティブまたはプライマリ Unified CM Assistant サーバからの応答の受信を待機する時間を秒単位で指定します。

- Cisco Unified CM Assistant RNA Forward Calls（デフォルト値 = False）

  このパラメータを True に設定した場合、Cisco Unified CM Assistant RNA Timeout パラメータで指定される RNA 値が経過すると、アシスタントの電話機へのコールを、マネージャの次の応答可能なアシスタントに無応答時（RNA）転送することができます。このパラメータを False に設定した場合、コールは最初のアシスタントをいつまでも呼び続けるか、または、ボイスメール プロファイルが設定されているときはボイスメールにコールが転送されます。

- Cisco Unified CM Assistant RNA Timeout（デフォルト値 = 10）

  このパラメータは、Cisco Unified CM Assistant サーバが、応答のないコールを次の応答可能なアシスタントに RNA 転送するまで待機する時間を秒単位で指定します。RNA 転送は、Cisco Unified CM Assistant RNA Forward Calls パラメータを True に設定した場合にだけ発生します。回線でボイスメール プロファイルが設定され、他のアシスタントを利用できない場合は、タイムアウトするとボイスメールにコールが転送されます。

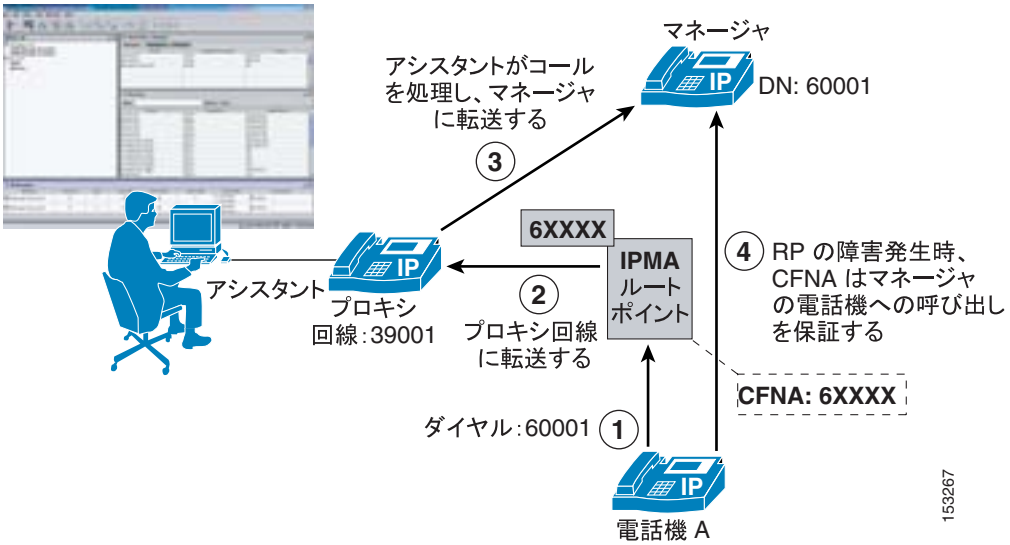
Unified CM Assistant の機能とアーキテクチャ

Unified CM Assistant アプリケーションは、プロキシ回線モードとシェアドライン モードの 2 つのモードで動作できます。各モードの動作と機能は異なり、それぞれに長所と短所があります。どちらのモードも、1 つのクラスタ内で設定できます。ただし、同一のアシスタントでモードを混合させることはできません。1 人以上のマネージャにサポートを提供している 1 人のアシスタントは、シェアドライン モードまたはプロキシ回線モードのいずれかでこれらのマネージャをサポートできます。

Unified CM Assistant のプロキシ回線モード

図 20-5 は、プロキシ回線モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、ディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。CTI/Unified CM Assistant Route Point（RP）は、6XXXX に設定された DN に基づいてこのコールを代行受信します。次に、マネージャの DN に基づいて、コールはルート ポイントにより、アシスタントの電話機上のマネージャのプロキシ回線（DN：39001）に転送されます（ステップ 2）。次に、アシスタントはコールに応答または処理し、必要に応じてマネージャの電話機にコールを転送します（ステップ 3）。Unified CM Assistant アプリケーションまたは Unified CM Assistant RP に障害が発生した場合に、マネージャの DN へのコールがマネージャの電話機を直接呼び出すよう、RP の Call Forward No Answer（CFNA）の 6XXXX 設定による呼び出しメカニズムが存在します（ステップ 4）。

図 20-5　Unified CM Assistant のプロキシ回線モード

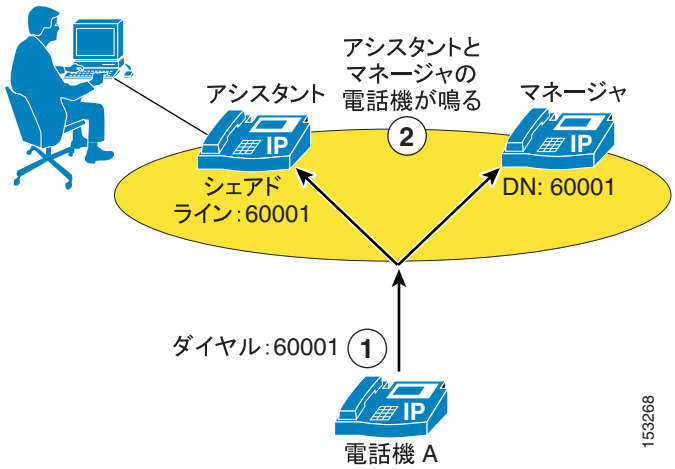


（注） 図 20-5 に示す CFNA による呼び出しメカニズムでは、Unified CM Assistant RP のディレクトリ番号設定ページの Forward No Answer Internal フィールドと Forward No Answer External フィールドの両方で、Unified CM Assistant RP ディレクトリ番号と同じ集約番号桁の設定が必要です。また、これらの各コール転送パラメータの Calling Search Space（CSS; コーリング サーチ スペース）フィールドは、Unified CM Assistant RP または Unified CM Assistant アプリケーションに障害が発生した場合に マネージャの電話機の DN に到達できるように、マネージャの電話機の DN が設定されたパーティションを含むコーリング サーチ スペースで設定する必要があります。

Unified CM Assistant のシェアドライン モード

図 20-6 は、シェアドライン モードでの Unified CM Assistant の単純なコール フローを示しています。この例で、電話機 A は、アシスタントの電話機のシェアドラインであるディレクトリ番号（DN）60001 でマネージャの電話機をコールします（ステップ 1）。このコールは、アシスタントとマネージャの電話機の両方で着信音を鳴らします。ただし、マネージャが Do Not Disturb（DND）機能を呼び出した場合、着信音が鳴るのはアシスタントの電話機だけになります（ステップ 2）。

図 20-6　Unified CM Assistant のシェアドライン モード



Unified CM Assistant のシェアドライン モードでは、マネージャの電話機へのコールを代行受信するために Unified CM Assistant RP は必要ありません。ただし、マネージャの電話機および Unified CM Assistant Console デスクトップ アプリケーションの Do Not Disturb（DND）機能は、Cisco Unified CallManager Assistant および Cisco CTIManager サービスに依存します。さらに、Unified CM Assistant シェアドライン モードでは、コール フィルタリング、コール代行受信、アシスタント選択、Assistant Watch などの機能は使用できません。

Unified CM Assistant のアーキテクチャ

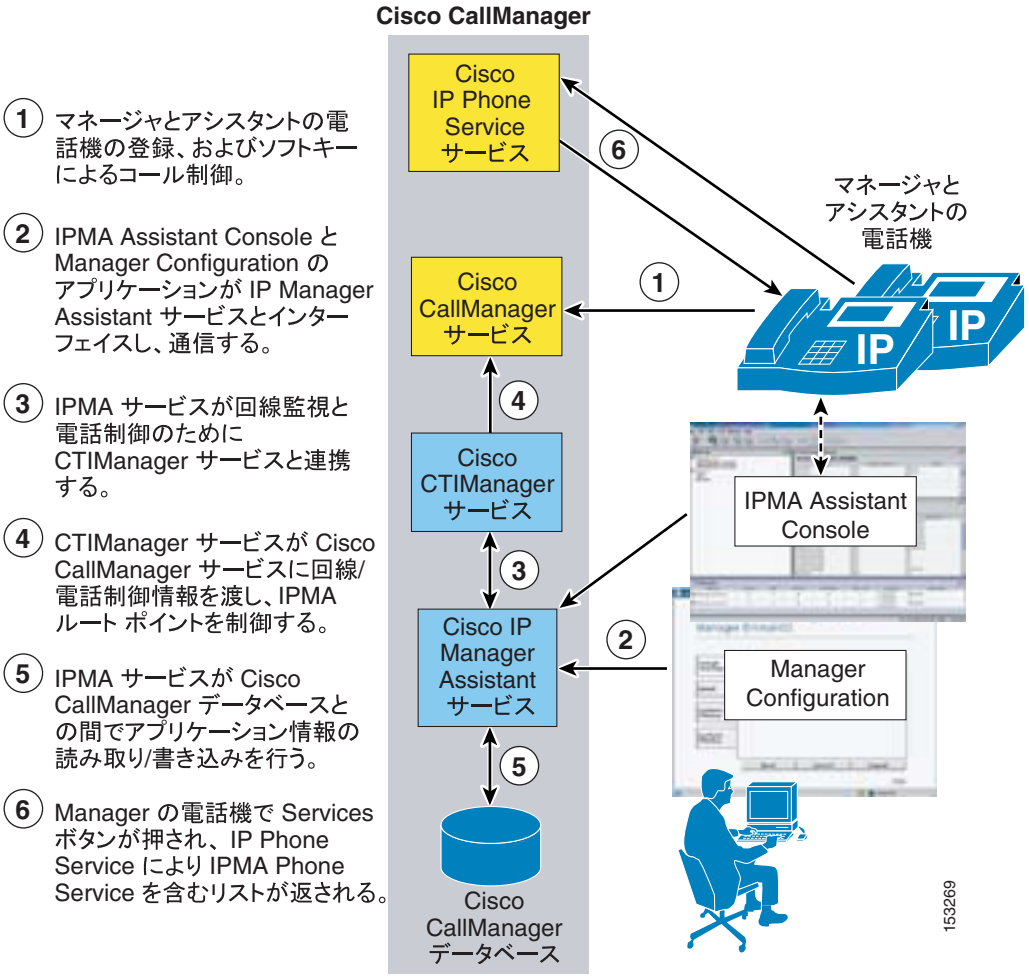
Unified CM Assistant アプリケーションの機能と同様に、そのアーキテクチャについても理解することが重要です。図 20-7 は、Unified CM Assistant のメッセージ フローとアーキテクチャを示しています。Unified CM Assistant のマネージャおよびアシスタント ユーザに対して Unified CM Assistant を設定すると、次の一連の対話とイベントが発生します。

1. マネージャとアシスタントの電話機は Cisco Unified CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 20-7 のステップ 1 を参照してください）。
2. Unified CM Assistant Console デスクトップ アプリケーションと Manager Configuration Web ベース アプリケーションは、どちらも Unified CM Assistant サービスと通信およびインターフェイスします（図 20-7 のステップ 2 を参照してください）。
3. 次に、Unified CM Assistant サービスは、回線監視情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 20-7 のステップ 3 を参照してください）。
4. CTIManager サービスは、Unified CM Assistant 電話制御情報を Cisco CallManager Service に渡し、さらに Unified CM Assistant RP を制御します（図 20-7 のステップ 4 を参照してください）。
5. それと並行して、Unified CM Assistant サービスは、Cisco Unified CallManager データベースとの間で、Unified CM Assistant アプリケーション情報の読み取りと書き込みを行います（図 20-7 のステップ 5 を参照してください）。
6. マネージャは、Services ボタンを押すことにより、Unified CM Assistant 電話サービスを呼び出して、その電話機が加入している（Unified CM Assistant 電話サービスを含む）すべてのサービスのリストを返す IP Phone Service サービスへのコールを生成できます（図 20-7 のステップ 6 を参照してください）。

Unified CM Assistant 電話サービスは Unified CM Assistant サービスで制御され、電話機を使用してマネージャによって加えられた設定の変更は、Unified CM Assistant サービスを通じて処理および伝達されます。

（注）　ユーザが回線ボタンまたは短縮ダイヤル ボタンを押して、Unified CM Assistant サービスへの直接コールを生成することで、IP Phone Service をバイパスできるように、マネージャの電話機で Service URL ボタンを Unified CM Assistant 電話サービス用に設定することもできます。

図 20-7　Unified CM Assistant のアーキテクチャ



（注）　図 20-7 は、すべて同じノードで実行されている IP Phone Service、Cisco Unified CallManager、CTIManager、および Unified CM Assistant サービスを示していますが、この設定は必須ではありません。これらのサービスではクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Unified CM Assistant のダイヤル プランの考慮事項

ダイヤル プラン設定は、プロキシ回線モードで設定される Unified CM Assistant では非常に重要です。マネージャの DN に対するコールが Unified CM Assistant RP で代行受信され、アシスタントの電話機に転送されることを保証するには、Unified CM Assistant RP およびアシスタントの電話機上のマネージャのプロキシ回線を除いて、すべてのデバイスからマネージャの DN に到達できないように、コーリング サーチ スペースおよびパーティションを設定する必要があります。

図 20-8 は、ダイヤル プラン コンポーネント内の各種デバイスのコーリング サーチ スペース、パーティション、および設定に対する最小要件を持つ、プロキシ回線モードの Unified CM Assistant ダイヤル プランの例を示しています。プロキシ回線モードでは 3 つのパーティションが必要です。図 20-7 の例では、次のパーティションになります。

- すべての IPMA RP DN を含む IPMA パーティション
- すべてのアシスタントとその他のユーザの電話機 DN を含む IPMA_Everyone パーティション
- すべてのマネージャの電話機の DN を含む IPMA_Manager パーティション

また、2 つのコーリング サーチ スペースが必要です。図 20-7 の例では、次のコーリング サーチ スペースになります。

- IPMA パーティションおよび IPMA_Everyone パーティションを含む IPMA_EVERYONE_CSS コーリング サーチ スペース
- IPMA_Manager パーティションおよび IPMA_Everyone パーティションを含む MANAGER_EVERYONE_CSS コーリング サーチ スペース

これは、この例でのダイヤル プランの範囲です。ただし、コール ルーティングが必要に応じて動作するように、適切なコーリング サーチ スペースでさまざまな電話機および IPMA RP DN または回線を適切に設定することも重要です。この場合、すべてのユーザの回線、アシスタントのプライマリ（またはパーソナル）回線、およびマネージャの電話回線は、これらの回線すべてが IPMA_Everyone パーティションおよび IPMA パーティションのすべての DN に到達できるように、IPMA_EVERYONE_CSS コーリング サーチ スペースで設定します。テレフォニー ネットワーク内のデバイスで設定されるインターコムなどの回線は、この同じコーリング サーチ スペースで設定します。すべてのマネージャのプロキシ回線およびすべての IPMA_RP 回線は、これらの回線すべてが IPMA_Manager パーティションのマネージャ DN および IPMA_Everyone パーティションに属するすべての DN に到達できるように、MANAGER_EVERYONE_CSS コーリング サーチ スペースで設定します。この方法により、ダイヤル プランでは、アシスタントの電話機の IPMA_RP 回線およびマネージャのプロキシ回線だけが、マネージャの電話機 DN に直接到達できるようになります。

図 20-8　Unified CM Assistant のプロキシ回線モードのダイヤル プランの例

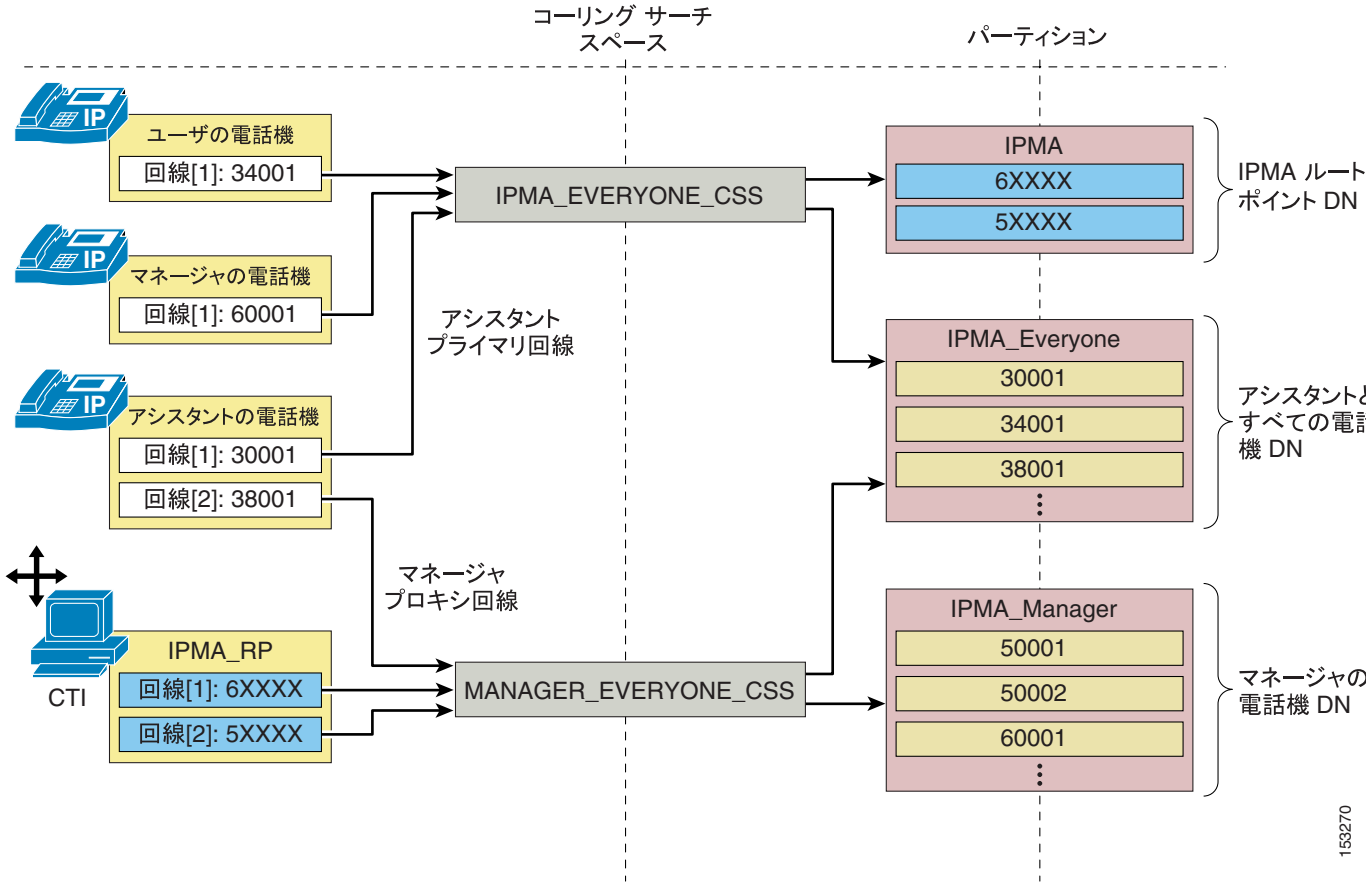


図 20-8 の例では、プロキシ回線モードでの Unified CM Assistant に関するダイヤル プランの最小要件を示しています。ただし、実際のテレフォニー ネットワークには、ほとんどの場合、Unified CM Assistant のコーリング サーチ スペースおよびパーティションとの統合が必要な追加または既存のダイヤル プラン要件があります。図 20-9 は、このような統合ダイヤル プランを示しています。この例では、前述したダイヤル プランは、2 つの追加のパーティションと 1 つの追加のコーリング サーチ スペースを処理する必要があります。図 20-9 では On Cluster パーティションが追加され、追加の電話機 DN もいくつか含まれています。On Cluster パーティションは、既存のデバイスがこれらの追加 DN に到達できるように、既存の IPMA コーリング サーチ スペースの両方（IPMA_EVERYONE_CSS および MANAGER_EVERYONE_CSS）に追加されています。UNRESTRICTED_CSS コーリング サーチ スペースも、既存のダイヤル プランに追加されています。このコーリング サーチ スペースは IPMA、IPMA_Everyone、および新たに追加した On Cluster パーティションで設定します。また、PSTN という 2 番目の新しいパーティションが追加されています。これには、共通ルート リスト（RL）、ルート グループ（RG）、およびボイス ゲートウェイ メカニズムを通じて、公衆網にコールをルーティングするために使用されるルート パターンのセットが含まれています。この PSTN パーティションは、UNRESTRICTED_CSS コーリング サーチ スペースの一部として設定します。

電話機およびデバイス回線のコーリング サーチ スペースの設定は、新しく追加したパーティションおよびコーリング サーチ スペースを組み込むために調整することができます。ただし、IPMA_RP およびアシスタントの電話機のマネージャ プロキシ回線は、MANAGER_EVERYONE_CSS コーリング サーチ スペースに割り当てたままにする必要があります。この例で、マネージャには公衆網への無制限アクセスが与えられる可能性があるため、マネージャの電話回線は、最初に設定された IPMA_EVERYONE_CSS コーリング サーチ スペースから、新しい UNRESTRICTED_CSS に移動されています。

図 20-9　Unified CM Assistant のプロキシ回線モードのダイヤル プラン統合の例

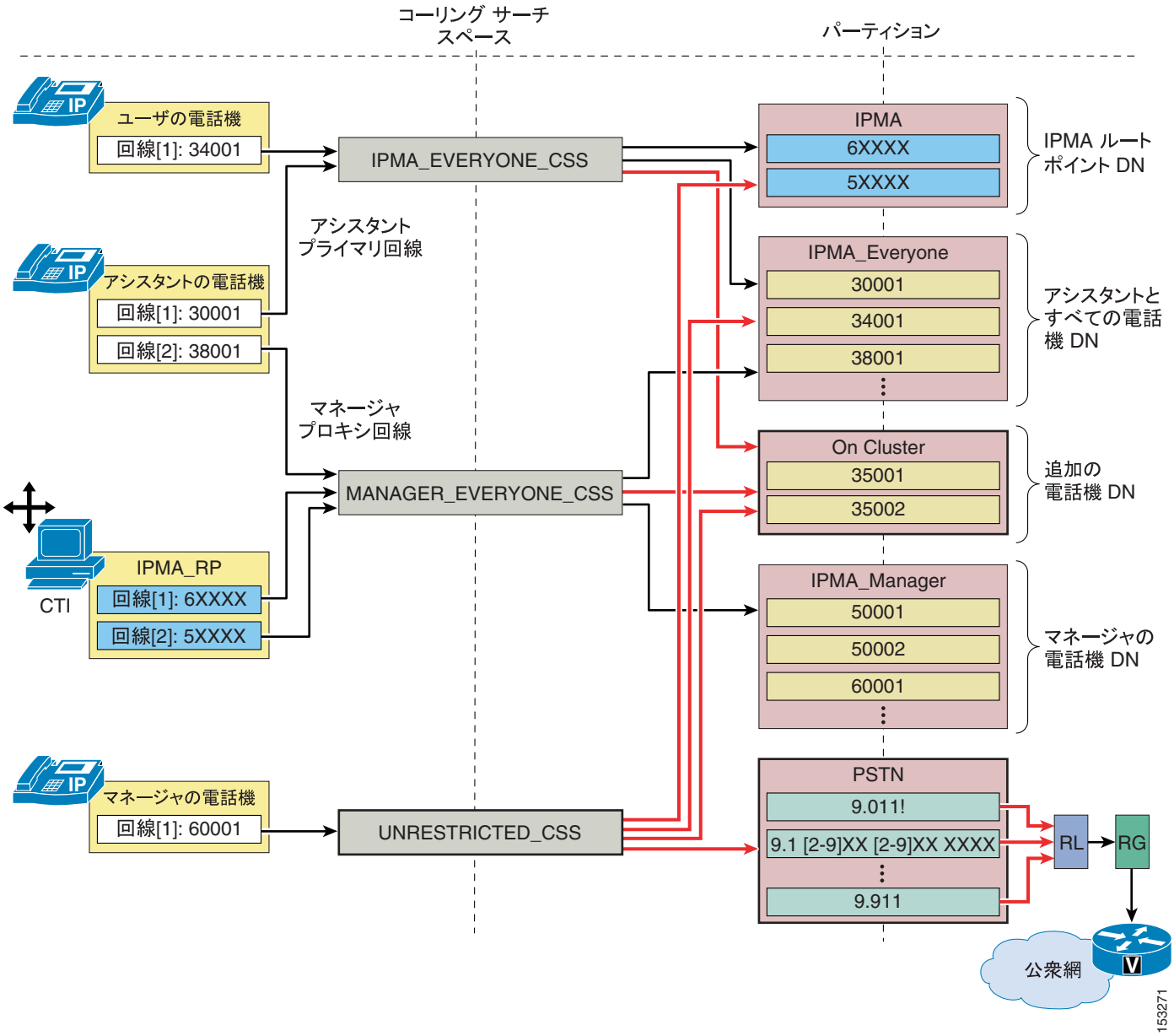


図 20-9 に示すように、追加のパーティションとコーリング サーチ スペースを新規または既存の Unified CM Assistant ダイヤル プランに統合することはできますが、基になるプロキシ回線モードのメカニズムが影響を受けないように注意する必要があります。

Unified CM Assistant シェアドライン モードでは、特別なダイヤル プランのプロビジョニングは必要ありません。注意の必要な Unified CM Assistant RP またはプロキシ回線が存在しないため、マネージャとアシスタントの電話機は、ネットワーク内の他の電話機と同様にコーリング サーチ スペースおよびパーティションで設定できます。シェアドライン モードに関する唯一の要件は、シェアドラインの機能を実現できるように、マネージャとアシスタントの DN が同じパーティションに属する必要があることです。

Unified CM Assistant Console

Unified CM Assistant Console デスクトップ アプリケーションは、アシスタントがマネージャの代わりにコールを処理するために必要です。このアプリケーションは、コールを処理するためのグラフィカル インターフェイスをアシスタントに提供します。また、このアプリケーションは、クリックダイヤルの短縮ダイヤルとディレクトリ エントリ、マネージャの電話機と環境の設定、すべてのマネージャの電話機の回線ステータスと可用性の表示など、その他の多くの機能を備えています。

Unified CM Assistant Console のインストール

Unified CM Assistant Console デスクトップ アプリケーションは、次の URL からインストールできます。

https://<*Server_IP-Address*>:8443/ma/Install/Unified CM AssistantConsoleInstall.jsp

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

Unified CM Assistant Console の QoS

インストール後に、マネージャに代わってコールを処理するには、アシスタントがユーザ ID とパスワード（Cisco Unified CallManager の End-user ディレクトリで設定）を入力してアプリケーションにログオンし、Go Online アイコンまたはメニュー項目をクリックして、ステータスを「オンライン」に切り替える必要があります。ユーザがログインし、オンライン状態になると、デスクトップ アプリケーションは TCP ポート 2912 で Cisco Unified CallManager Unified CM Assistant サーバと通信します。このアプリケーションは、トラフィックを受信する場合に一時的な TCP ポートを選択します。Cisco Unified CallManager 上の Unified CM Assistant サーバは、コール制御（コール フローの生成と処理）のためにデスクトップ アプリケーションとインターフェイスするので、TCP ポート 2912 で Cisco Unified CallManager から受信されたトラフィックは、Cisco Unified CallManager によって 24 の Differentiated Services Code Point（DSCP）または CS3 の Per Hop Behavior（PHB）として、QoS マーキングされます。この方法により、Unified CM Assistant 電話制御トラフィックは、その他のすべてのコール シグナリング トラフィックと同様に、ネットワークを通じてキューに入れることができます。

対称的なマーキングとキューを保証するため、Cisco Unified CallManager の TCP ポート 2912 を宛先とする Unified CM Assistant Console アプリケーション トラフィックも、DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Cisco Unified CallManager および Unified CM Assistant サーバに向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。Unified CM Assistant Assistant Console アプリケーションは、すべてのトラフィックをベストエフォートとしてマーキングします。つまり、スイッチ ポート レベル（または、可能な限りコンソール PC に近いネットワーク パスに沿った場所で）Access Control List（ACL; アクセス コントロール リスト）を適用することで、アプリケーション PC から送信され、TCP ポート 2912 の Cisco Unified CallManager を宛先とするトラフィックを、DSCP 0（PHB Best Effort）から DSCP 24（PHB CS3）に再マーキングする必要があります。

Unified CM Assistant Console のディレクトリ ウィンドウ

Assistant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、アシスタントは Cisco Unified CallManager Directory エンドユーザを検索できます。ディレクトリ ウィンドウの Name フィールドに入力する検索文字列は、Unified CM Assistant サーバに送信され、Cisco Unified CallManager データベースに対して検索が直接実行されます。次に、Unified CM Assistant サーバによって、検索照会への応答がデスクトップ アプリケーションに返されます。

デスクトップ アプリケーションのディレクトリ検索によって生じる追加のトラフィックはわずかですが、1 つ以上の Unified CM Assistant コンソール アプリケーションがリモート サイトで実行されている集中型のコール処理配置では、このトラフィックが問題になることがあります。1 つのエントリが得られるディレクトリ検索では、Unified CM Assistant サーバからデスクトップ アプリケーションへの約 1 キロビットのトラフィックが発生します。1 回の検索あたり最大 25 のエントリを取得できるため、デスクトップ アプリケーションで実行される検索ごとに最大約 25 キロビットのトラフィックが生成されることがあります。ただし、Unified CM Assistant サーバからの低速 WAN リンクを通じて、複数の Unified CM Assistant Console デスクトップ アプリケーションでディレクトリ検索が実行されると、輻輳、遅延、およびキューの発生する可能性が高くなります。また、ディレクトリ検索トラフィックは、デスクトップに対するその他すべての Unified CM Assistant トラフィックと同様に、TCP ポート 2912 の Cisco Unified CallManager から発生します。つまり、ディレクトリ検索トラフィックも DSCP 24（PHB CS3）としてマーキングされるため、コール シグナリング トラフィックと同様にキューに入れられます。このため、ディレクトリ検索によって、コール制御トラフィックの輻輳、オーバーラン、または遅延が生じる可能性があります。

（注） ディレクトリ検索で 25 を超えるエントリが生成される場合、アシスタントには、ダイアログボックスで警告メッセージ「Your search returned more than 25 entries.Please refine your search.」が表示されます。

ネットワーク輻輳の可能性を考慮に入れて、管理者は Unified CM Assistant Console ユーザに次の操作の実行を推奨することをお勧めします。

- ディレクトリ ウィンドウ検索機能の使用を制限する。
- 返されるエントリの数を減らすため、この機能を使用するときは、Name フィールドにできる限り多くの情報を入力し、ワイルドカードやブランクでの検索は実行しない。

これらの推奨事項は、次のいずれかの条件が該当する場合は特に重要です。

- クラスタ内に多数の Unified CM Assistant Assistants が存在する。
- Cisco Unified CallManager または Unified CM Assistant サーバ（あるいはその両方）から低速 WAN リンクによって分離されている多数のアシスタントが存在する。

Unified CM Assistant の冗長性

Unified CM Assistant アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、Unified CM Assistant サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、アシスタントとマネージャの電話機、Unified CM Assistant ルート ポイント、および Unified CM Assistant Console デスクトップ アプリケーションに関連して検討し、さらにアシスタントとマネージャの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 20-7 に示すように、Unified CM Assistant 機能は、主に Cisco CallManager IP Manager Assistant サービスおよび Cisco CTIManager サービスに依存します。いずれの場合も、冗長性はプライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Cisco Unified CM Assistant Server (Primary) IP Address および Cisco Unified CM Assistant Server (Backup) IP Address のサービス パラメータを使用すると、2 つの Unified CM Assistant サーバ（Cisco Unified CM Assistant サービスを実行しているノード）を 1 つのクラスタ内で定義できます（P.20-15 の「Unified CM Assistant のサービス パラメータ」を参照してください）。これらのパラメータを設定することで、必要な Unified CM Assistant サービスに冗長性が与えられます。プライマリ Unified CM Assistant に障害が発生した場合、バックアップまたはスタンバイ Unified CM Assistant サーバが Unified CM Assistant サービス要求を処理できます。任意の時点でアクティブになり、要求を処理する Unified CM Assistant サーバは 1 つだけです。その他の Unified CM Assistant サーバはスタンバイ状態になり、アクティブなサーバに障害が発生しない限り、要求を処理しません。

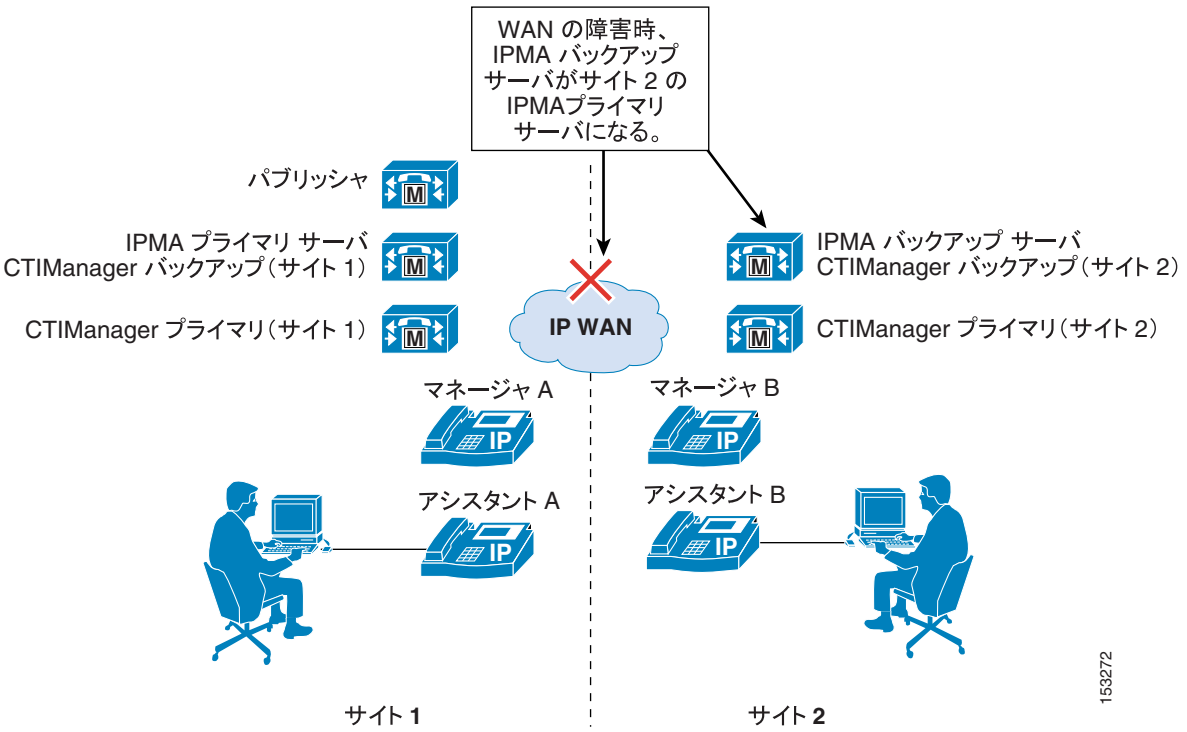
また、CTIManager (Primary) IP Address および CTIManager (Backup) IP Address サービス パラメータを使用して、2 つの CTIManager サーバまたはサービスを各 Unified CM Assistant サーバ用に定義できます（P.20-15 の「Unified CM Assistant のサービス パラメータ」を参照してください）。これによって、Unified CM Assistant アプリケーションで使用する CTIManager が、クラスタあたり合計で最大 4 つ得られます。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。クラスタ ノードのすべての Unified CM Assistant および CTIManager サービスに障害が発生した場合は、Unified CM Assistant ルート ポイントおよび Unified CM Assistant Console デスクトップ アプリケーションがダウンし、その結果 Unified CM Assistant アプリケーション全体がダウンします。

（注） Unified CM Assistant シェアドライン モードで設定した場合、Unified CM Assistant および CTIManager サービスが障害によって完全に停止しても、電話機は 1 本の回線を共有し続けるため、アシスタントは引き続きマネージャの代わりにコールを処理できます。ただし、Unified CM Assistant Console デスクトップ アプリケーションと DND の機能は、使用できなくなります。

図 20-10 は、WAN を通じたクラスタ化で、2 サイトの配置による Unified CM Assistant および CTIManager のプライマリ サーバとバックアップ サーバの冗長設定を示しています。最大限の冗長性を実現するため、サイト 1 のノードはプライマリ Unified CM Assistant サーバとして設定し、サイト 2 のノードはバックアップ Unified CM Assistant サーバとして設定します。WAN に障害が発生した場合、既存のプライマリ Unified CM Assistant サーバはサイト 2 から到達できなくなるため、サイト 2 のバックアップ Unified CM Assistant サーバがプライマリ Unified CM Assistant サーバになります。このようにすることで、WAN を通じたクラスタ環境で、Unified CM Assistant サーバは WAN の障害に対して冗長性を持つことができます。さらに、サイト 1 とサイト 2 の両方でプライマリおよびバックアップ CTIManager を設定すると、CTIManager は WAN の障害に対する冗長性を持ち、各サイトで CTIManager の障害に対して追加の冗長性が提供されます。

（注） 図 20-10 で説明するシナリオは、特別な状況を示しています。通常の動作時に、同じクラスタ内に 2 つのアクティブまたはプライマリ Unified CM Assistant サーバは存在できません。2 つの Unified CM Assistant サーバがネットワークを通じて通信できる場合、一方のサーバはバックアップ モードとなり、要求を処理できません。

図 20-10　WAN を通じた 2 サイト クラスタ化による Unified CM Assistant の冗長性



前述のように、パブリッシャは Cisco Unified CallManager データベースへの書き込み時に単一の障害点となります。Unified CM Assistant アプリケーションに対するパブリッシャの障害の影響は、エクステンション モビリティに対する影響ほど大きくありません。パブリッシャに障害が発生しても、Unified CM Assistant　アプリケーションのすべての部分が引き続き動作します。ただし、Unified CM Assistant アプリケーション設定を変更できなくなります。パブリッシャが回復するまで、Unified CM Assistant Console デスクトップ アプリケーション、Manager Configuration Web ベース アプリケーション、電話機のソフトキー、または Unified CM Assistant 電話サービスを通じて設定を変更できません。この条件には、Do Not Disturb、DivertAll、Assistant Watch、コール フィルタリングなどの機能の有効化や無効化、およびコール フィルタとアシスタント選択設定の変更が含まれます。

デバイスと到達可能性の冗長性

デバイス レベルでの Unified CM Assistant の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、マネージャおよびアシスタントの電話機と Unified CM Assistant RP は、デバイス登録用のデバイス プールと Cisco Unified CallManager グループ設定の組み合せによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、Unified CM Assistant RP はコール制御機能に関して CTIManager にも依存するため、前の項で説明したプライマリおよびバックアップ CTIManager に依存する必要があります。Unified CM Assistant Console デスクトップ アプリケーションも、冗長性と機能がコンポーネント サービスに依存します。Assistant Console デスクトップ アプリケーションは、マネージャの着信コールの処理を持続できるように、プライマリ Unified CM Assistant サーバからバックアップ サーバ（およびその反対）への自動フェールオーバーをサポートしています。この自動フェールオーバーに要

する時間は、Cisco Unified CM Assistant Console Heartbeat Interval および Cisco Unified CM Assistant Console Request Timeout のサービス パラメータを使用して制御できます（P.20-15 の「Unified CM Assistant のサービス パラメータ」を参照してください）。ハートビートまたはキープアライブの頻度は、Unified CM Assistant サーバの障害がデスクトップ アプリケーションですばやく検出されるように設定しますが、キープアライブをあまり頻繁に送信することで、ネットワークに悪影響を与えないように注意してください。多数の Assistant Console アプリケーションが使用されている場合、この考慮事項は特に重要です。

マネージャおよびアシスタントの到達可能性に確実に冗長性を与えるフェールオーバー メカニズムは、他にもいくつかあります。第 1 に、（プロキシ回線モードで）Unified CM Assistant アプリケーションを通じてマネージャのアシスタントに送信されるコールは、設定した時間の経過後にそのコールへの応答がない場合、次の応答可能なマネージャのアシスタントに転送します。設定した時間の経過後に次のアシスタントがコールに応答しない場合、そのコールは次の応答可能なマネージャのアシスタントに再び転送され、それ以降も同様に転送が続けられます。このメカニズムは、Cisco Unified CM Assistant RNA Forward Calls および Cisco Unified CM Assistant RNA Timeout のサービス パラメータを使用して設定します（P.20-15 の「Unified CM Assistant のサービス パラメータ」を参照してください）。第 2 に、前述したように、クラスタ ノードのすべての Unified CM Assistant と CTI サービスに障害が発生した場合、Unified CM Assistant RP は使用できなくなります。ただし、Unified CM Assistant RP の CFNA 設定に基づいて、すべてのマネージャの DN に対するコールはマネージャの電話機に直接呼び出され、マネージャの到達可能性に十分な冗長性が与えられます。

Unified CM Assistant のガイドラインと制限

Unified CM Assistant には、重複および共有内線番号に関して次の制限があり、ディレクトリ番号のプロビジョニングを計画する場合に注意する必要があります。

- プロキシ回線モードの Unified CM Assistant では、アシスタントの電話機のプロキシ回線番号は、異なるパーティション間でも一意にする必要があります。
- プロキシ回線モードの Unified CM Assistant では、2 人のマネージャは異なるパーティション間でも、同じ Unified CM Assistant 制御回線番号（DN）を持つことができません。

また、Unified CM Assistant アシスタントは、Cisco Unified CallManager Release 4.*x* から Cisco Unified CallManager 5.0 にアップグレードする場合、Unified CM Assistant Assistant Console デスクトップ アプリケーションが最新バージョンに自動的にアップグレードされないことに注意してください。代わりに、旧バージョンの Unified CM Assistant Console デスクトップ アプリケーションをアンインストールし、新しいバージョンをインストールする必要があります。

Unified CM Assistant のパフォーマンスとキャパシティ

Cisco Unified CM Assistant アプリケーションは、次のキャパシティをサポートしています。

- マネージャあたり最大 10 人のアシスタントを設定できる。
- 1 人のアシスタントに対して最大 33 人のマネージャを設定できる。
- MCS-7845 サーバが含まれるクラスタあたり最大 1250 人のアシスタントと 1250 人のマネージャを設定できる。
- クラスタあたり最大 2 つの Unified CM Assistant サーバを配置できる（プライマリとバックアップ）。
- Unified CM Assistant 用として、クラスタあたり最大 4 つの CTIManager を設定できる（2 つの Unified CM Assistant サーバのそれぞれに対してプライマリおよびバックアップの CTIManager を指定できます）。

Cisco Unified CM Assistant アプリケーションは、回線監視および電話制御のために CTIManager と対話します。Unified CM Assistant またはマネージャの電話機の各回線は、CTIManager への接続を生成します。また、各 Unified CM Assistant ルート ポイントが CTIManager への接続を生成します。Unified CM Assistant を設定する場合、CTI 接続に対する全体的なクラスタ制限に関して、必要な CTI 接続の数を検討する必要があります（MCS-7845 プラットフォームのあるクラスタあたり 10,000 CTI 接続または MCS-7835 および MCS-7825 サーバが含まれるクラスタあたり 3200 CTI 接続）。他のアプリケーション用に追加の CTI 接続が必要な場合、Unified CM Assistant のキャパシティが制限されることがあります。

Unified CM Assistant のキャパシティの詳細については、次の Web サイトにある Cisco Unified CallManager と Unified CM Assistant のデータ シート、マニュアル、およびリリース ノートを参照してください。

http://www.cisco.com

Unified CM Assistant と EM の相互作用

Unified CM Assistant のマネージャは、EM を使用して、プロキシ回線モードとシェアドライン モードの両方でそれぞれの電話機にログインできます。ただし、そのマネージャは、エンドユーザ ディレクトリの Cisco Unified CM Assistant Manager 設定ページで、Mobile Manager として設定する必要があります。Unified CM Assistant と組み合せて EM を使用する場合、ユーザが EM を使用して複数の電話機にログインできないようにする必要があります。この動作は、EM サービス パラメータの Multiple Login Behavior を使用して有効または無効にできます（P.20-9 の「EM のサービス パラメータ」を参照してください）。クラスタ内で同じユーザによる複数の EM ログインが必要な場合、EM を使用する Unified CM Assistant のマネージャに、複数の電話機にログインしないよう指示する必要があります。マネージャが EM で 2 つの異なる電話機にログインすることを許可すると、2 人のマネージャは異なるパーティション間でも同じ Unified CM Assistant 制御回線番号（DN）を持つことができないという、前述の制限に違反することになります。

（注）　Unified CM Assistant のアシスタントは、Mobile Assistant の概念がないため、EM を使用してそれぞれの電話機にログインすることはできません。

Attendant Console

Cisco Unified CallManager Attendant Console（AC）アプリケーションを使用すると、受け付け係が企業内でコールに応答して転送したり、コールを送信したりすることができます。係員は Windows 2000 または Windows XP を実行している PC に、クライアント / サーバ Java アプリケーションの Attendant Console をインストールできます。Attendant Console は Cisco CallManager Attendant Console Server（Cisco Unified CallManager AC Server）に接続し、ログイン サービス、回線状態、およびディレクトリ サービスを提供します。1 つの AC サーバに複数の Attendant Console を接続できます。

AC Phone のサポート

次の SCCP 電話機が AC 機能をサポートしています。

- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified IP Phone 7940G、7941G、および 7941G-GE
- Cisco Unified IP Phone 7960G、7961G、および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

SIP 電話機では、AC はサポートされていません。

Cisco Unified CallManager および AC のサービス パラメータ

AC アプリケーションを有効にするには、システム管理者は Cisco Unified CallManager Serviceability インターフェイスからいくつかの Cisco Unified CallManager 機能サービスをアクティブにし、起動する必要があります。また、AC サービス パラメータは、AC アプリケーションの動作を決定するための設定およびカスタマイズのオプションを提供します。

AC 用の Cisco Unified CallManager サービス

AC アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco CallManager Attendant Console Server
- Cisco CTIManager

Cisco CallManager Attendant Console Server サービスは AC Desktop アプリケーションへのインターフェイスを提供し、Cisco CTIManager サービスおよび Cisco Unified CallManager データベースと対話します。Cisco CTIManager サービスは、電話とコールの制御のために Cisco CallManager Service および Cisco CallManager Attendant Console Server サービスとインターフェイスし、対話します。AC Desktop アプリケーションともインターフェイスします。

AC のサービス パラメータ

次の項目は、AC 機能に関連する Cisco CallManager Attendant Console Server サービス パラメータの一部のリストです。

- Directory Sync Period（デフォルト値 = 3）

  このパラメータは、AC サーバの AutoGenerated.txt ファイルと Cisco Unified CallManager のエンドユーザ ディレクトリの同期のための間隔を、時間単位で指定します。エンドユーザ ディレクトリへの変更は、この間隔が経過するまで AutoGenerated.txt ファイルに反映されません。

- JTAPI Username（デフォルト値 = ac）

  このパラメータは、AC サーバが CTIManager にログインし、通信するために使用するアプリケーション ユーザ名を指定します。

AC のアプリケーション ユーザ

AC が正しく動作するには、**ac** という名前のアプリケーション ユーザを Cisco Unified CallManager で設定する必要があります。ac アプリケーション ユーザは、AC サーバが CTIManager と対話するために必要です。このアプリケーション ユーザが設定されていないと、コンソール担当者はコールを受信できません。

(注)　アプリケーション ユーザは、Cisco Unified CallManager 5.0 データベース内のエンド ユーザとは異なり、ディレクトリ内のエンド ユーザとは別に保存されます。したがって、ディレクトリ検索ではアプリケーション ユーザ エントリが返されません。Cisco Unified CallManager 5.0 のアプリケーション ユーザとエンド ユーザの詳細については、P.16-1 の「LDAP ディレクトリ統合」を参照してください。

ac ユーザには、アプリケーション ユーザの設定ページで次のグループ アクセス権を設定する必要があります。

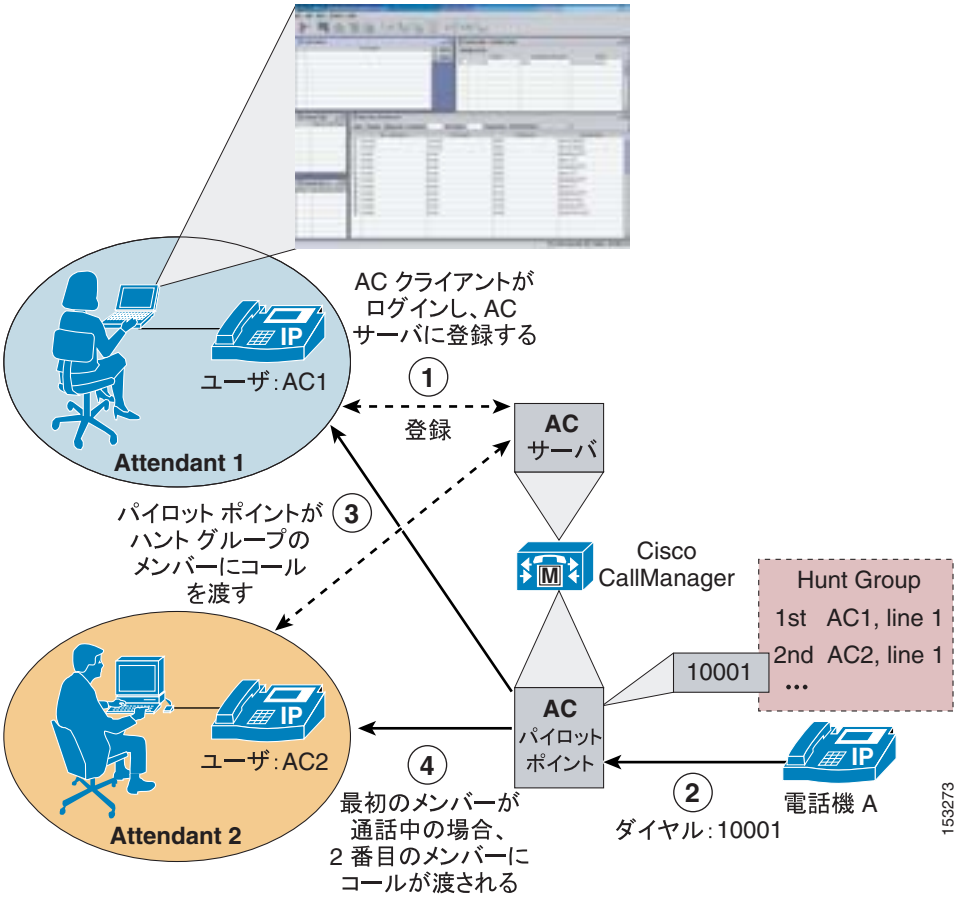
- Standard CTI Allow Control of All Devices
- Standard CTI Allow Call Park Monitoring
- Standard CTI Enabled

管理者は、このアプリケーション ユーザ名を ac 以外の名前に変更できます。ac 以外のユーザ名に設定した場合、JTAPI Username サービス パラメータに新しいユーザ名を設定する必要があります（P.20-29 の「AC のサービス パラメータ」を参照してください）。

AC の機能とアーキテクチャ

図 20-11 は、AC の機能と動作の基本的な例を示しています。最初に、AC クライアントは Cisco Unified CallManager 上の AC サーバにログインし、登録されます（ステップ 1）。電話機 A は Cisco Unified CallManager の AC パイロット ポイントに対して設定されたディレクトリ番号（DN）をコールします（ステップ 2）。AC パイロット ポイントはこのコールを代行受信し、ハント グループ設定に基づいて、使用可能なメンバーの 1 つにコールを転送します。この場合、コールは Attendant ユーザ AC1 の電話機の回線 2 に送信されます（ステップ 3）。AC1 がまだ最初のコールで通話しているときに、パイロット ポイント番号 10001 に 2 番目のコールが着信した場合、そのコールはハント グループの別の使用可能なメンバーにルーティングされます。この場合、そのコールは、Attendant ユーザ AC2 の電話機の回線 1 に転送されます（ステップ 4）。

図 20-11　基本的な AC の動作



コールをルーティングするには、パイロット ポイントが次のいずれかのルーティング アルゴリズムに基づいて、ハント グループの次の使用可能なメンバーを決定します（パイロット ポイントの「Route Calls to」フィールドで設定します）。

- First available

  このアルゴリズムでは、着信コールが、使用可能なグループの最初のメンバーにルーティングされます。

- Longest idle

  このアルゴリズムでは、着信コールが、アイドル状態（コールの処理なし）の最も長かったメンバーにルーティングされます。

- Circular hunting

  このアルゴリズムでは、着信コールが、使用可能なメンバーにラウンドロビン方式でルーティングされます。

- Broadcast hunting

  このアルゴリズムでは、着信コールがキューに入れられ、すべての使用可能なメンバーの AC デスクトップ アプリケーションに対して同時に通知が送信されます。

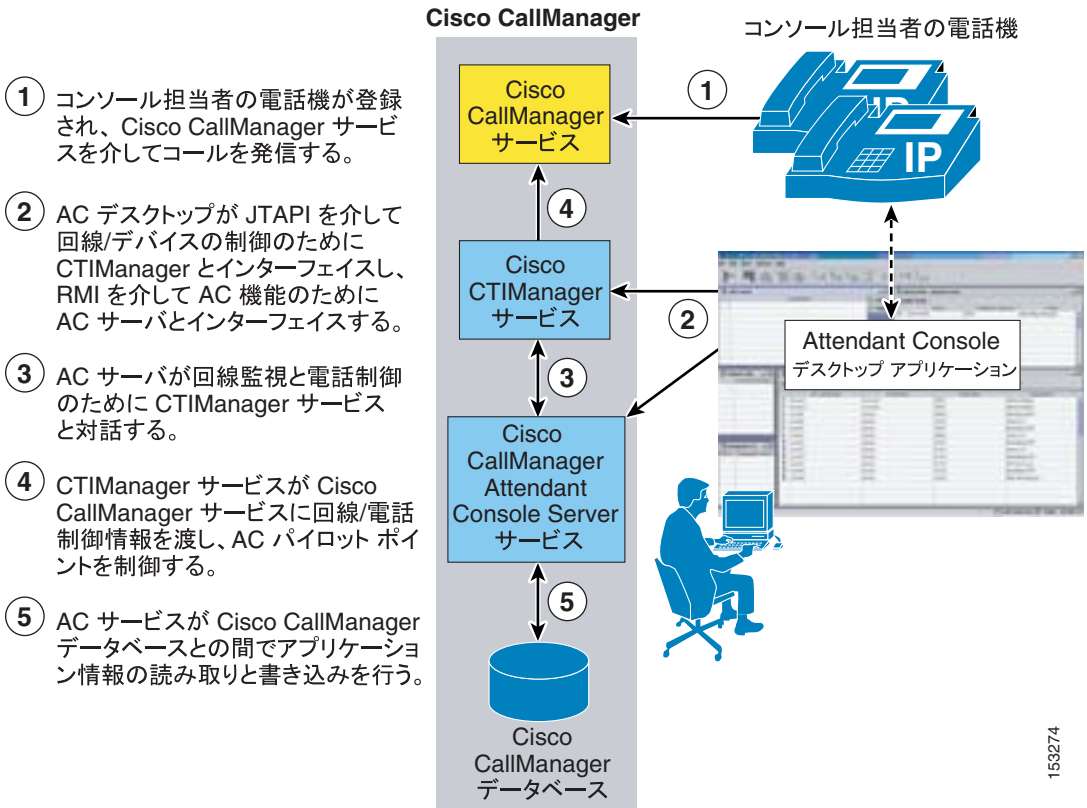
図 20-11 に示す例では、First Available アルゴリズムを使用しています。ハント グループのルーティング アルゴリズム、および Broadcast ルーティング アルゴリズムのキュー設定は、すべて Cisco Unified CallManager の Pilot Point 設定ページで設定します。

AC のアーキテクチャ

AC アプリケーションの機能と同様に、そのアーキテクチャについて理解することも重要です。図 20-12 は、AC のメッセージ フローとアーキテクチャを示しています。AC ユーザ用に AC を設定すると、次の一連の対話とイベントが発生します。

1. コンソール担当者の電話機は Cisco Unified CallManager サービスに登録され、コール フロー処理にキーパッドとソフトキーが使用されます（図 20-12 のステップ 1 を参照してください）。
2. Attendant Console デスクトップ アプリケーションは、JTAPI を使用して電話と回線の制御のために CTIManager サービスと通信し、インターフェイスします。また、このデスクトップ アプリケーションは、Remote Method Invocation（RMI）を介して AC 機能のために AC サービスおよびサーバとインターフェイスします（図 20-12 のステップ 2 を参照してください）。
3. 次に、AC サーバは、回線監視情報および電話制御情報を交換するために、CTIManager サービスと対話します（図 20-12 のステップ 3 を参照してください）。
4. 同様に、CTIManager サービスは、Cisco CallManager Service に AC 電話制御情報を渡し、さらに AC パイロット ポイントを制御します（図 20-12 のステップ 4 を参照してください）。
5. それと並行して、AC サービスは、Cisco Unified CallManager データベースとの間で、AC アプリケーション情報の読み取りと書き込みを行います（図 20-12 のステップ 5 を参照してください）。

図 20-12　AC のアーキテクチャ



1. コンソール担当者の電話機が登録され、Cisco CallManager サービスを介してコールを発信する。
2. AC デスクトップが JTAPI を介して回線/デバイスの制御のために CTIManager とインターフェイスし、RMI を介して AC 機能のために AC サーバとインターフェイスする。
3. AC サーバが回線監視と電話制御のために CTIManager サービスと対話する。
4. CTIManager サービスが Cisco CallManager サービスに回線/電話制御情報を渡し、AC パイロット ポイントを制御する。
5. AC サービスが Cisco CallManager データベースとの間でアプリケーション情報の読み取りと書き込みを行う。

（注） 図 20-12 は、すべて同じノードで実行されている Cisco Unified CallManager、CTIManager、および Attendant Console Server サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

Attendant Console デスクトップ アプリケーション

Attendant Console デスクトップ アプリケーションは、グラフィカルな仮想コンソールを通じてコールを処理するため、コンソール担当者で使用されます。コール処理に加えて、このアプリケーションは、クリックダイヤルの短縮ダイヤルとディレクトリ エントリ、環境の設定、ディレクトリおよび短縮ダイヤル ウィンドウでの他のユーザに対する回線ステータスおよび可用性の表示など、追加の機能を備えています。

Attendant Console のインストール

Attendant Console デスクトップ アプリケーションは、次の URL からダウンロードできます。

https://<*Server_IP-Address*>:8443/plugins/CiscoAttendantConsoleClient.exe

（ここで、<*Server_IP-Address*> は、クラスタ内のいずれかのノードの IP アドレスです）

CiscoAttendantConsoleClient.exe ファイルは、コンソール担当者の PC にダウンロードしたら、インストールも実行する必要があります。

Attendant Console の QoS

Attendant Console デスクトップ アプリケーションのインストール後、コンソール担当者は、（Cisco Unified CallManager の Cisco Unified CM Attendant Console User ページの設定に従って）AC のユーザ ID およびパスワードを入力して、このコンソール アプリケーションにログオンします。

（注） AC のユーザ ID は AC デスクトップ アプリケーションへのログインに必要で、エンドユーザ ディレクトリで設定されるユーザおよび Cisco Unified CallManager のアプリケーション ユーザとは異なります。これらのユーザはエンドユーザ ディレクトリとは別に保存されるため、ディレクトリ検索で AC ユーザ エントリは返されません。

AC ユーザがログオンすると、AC デスクトップ アプリケーションは、主に Remote Method Invocation（RMI）および Java Telephony Application Programming Interface（JTAPI）を使用して、Cisco Unified CallManager と通信します。RMI は、登録、キープアライブ、および情報交換などのデスクトップ クライアントと AC サーバとの間の通信に使用されます。RMI トラフィックは、TCP ポート 1101 ～ 1129 の Cisco Unified CallManager、および 1 つ以上の一時的な TCP ポートのデスクトップ アプリケーションから発生します。すべての RMI トラフィックは、ベストエフォートとしてマーキングされます。

JTAPI トラフィックは、Cisco Unified CallManager 上の CTIManager と AC デスクトップ アプリケーションとの間で、デバイスおよび回線制御情報とコール制御トラフィックを伝送します。JTAPI トラフィックは、TCP ポート 2748 の Cisco Unified CallManager、および一時的な TCP ポートのデスクトップ アプリケーションから発生します。

CTIManager と AC クライアント間の JTAPI トラフィックはコール制御（コール フローの生成と処理）に使用されるため、24 の DSCP（CS3 の PHB）で、Cisco Unified CallManager により QoS マーキングされます。この方法により、AC 電話制御トラフィックは、その他のすべてのコール シグナリング トラフィックと同様に、ネットワークを通じてキューに入れることができます。対称的なマーキングとキューを保証するため、Cisco Unified CallManager TCP ポート 2748 を宛先とする Attendant Console アプリケーション トラフィックも DSCP 24（PHB CS3）としてマーキングする必要があります。これにより、このトラフィックが、Cisco Unified CallManager および CTIManager に向かうネットワーク パスに沿って適切なコール シグナリング キューに配置されます。ただし、AC

クライアント アプリケーションはすべてのトラフィックをベストエフォートとしてマーキングするため、アクセス コントロール リスト（ACL）は、このトラフィックに適切に再マーキングするように設定する必要があります。

AC サーバおよびデスクトップ クライアントのマーキングは、次のように要約できます。

- Cisco Unified CallManager は、24 の DSCP（CS3 の PHB）で TCP ポート 2748 から発生するすべての JTAPI トラフィックを適切にマーキングします。
- Attendant Console デスクトップ アプリケーションは、Cisco Unified CallManager TCP ポート 2748 を宛先とする JTAPI トラフィックをベストエフォートとしてマーキングします。つまり、ACL は、0 の DSCP から 24 の DSCP（CS3 の PHB）まで、アプリケーションが Cisco Unified CallManager および AC サーバに送信する JTAPI トラフィックを再マーキングするように、スイッチ ポート レベルで適用する必要があります。

Attendant Console のディレクトリ ウィンドウ

Attendant Console デスクトップ アプリケーションのディレクトリ ウィンドウを使用すると、コンソール担当者は Cisco Unified CallManager テレフォニー環境内のエンドユーザを検索できます。一般に、ディレクトリのリストは、Cisco Unified CallManager ディレクトリ自体の検索ではなく、ディレクトリ ファイルの検索によって取得されます。AC アプリケーション ユーザがディレクトリ ウィンドウに検索条件を入力すると、次のいずれかのディレクトリ ファイルが検索されます。

- User list

  このディレクトリ ファイルは、ローカル PC またはローカル ドライブ パスに格納されています。このファイルを検索するには、Attendant Settings ダイアログボックスの Advanced タブの Path Name of Local Directory File フィールドで、その名前と場所を設定する必要があります。このフィールドでファイル名と場所が設定されていない場合、このオプションはスキップされ、ディレクトリ検索はその他のいずれかのディレクトリ ファイルに対して実行されます。

- AutoGenerated.txt

  このディレクトリ ファイルは、AC サーバによって Cisco Unified CallManager データベースのエンドユーザ テーブルから自動的に生成され、Cisco Unified CallManager サーバに格納されています。ローカル ディレクトリのユーザ リスト ファイルが設定されていない場合、AC デスクトップ アプリケーションは、Cisco Unified CallManager からこのファイルを自動的にダウンロードします。AutoGenerated.txt ファイルは、このファイルの情報が正確になるように、AC サーバにより定期的にエンドユーザ ディレクトリから再生成または同期されます。この同期の頻度は、Directory Sync Period AC サービス パラメータで決定されます（P.20-29 の「AC のサービス パラメータ」を参照してください）。デフォルトでは、このパラメータは 3 時間に設定されるため、AutoGenerated.txt ファイルは 3 時間ごとに更新されます。

- CorporateDirectory.txt

  このファイルは、Cisco Unified CM Attendant Console User File Upload ツール（**Application** > **Cisco Unified CM Attendant Console**）を使用して、管理者が Cisco Unified CallManager に手動でインポートした場合にだけ使用できます。アップロードされると、Cisco Unified CallManager サーバの AutoGenerated.txt ファイルがこのファイルで置き換えられます。したがって、ローカル ユーザ リスト ファイルが設定されていない場合、AC デスクトップ アプリケーションは AutoGenerated.txt ファイルではなくこのファイルをダウンロードします。

AC デスクトップ アプリケーションが起動するたびに、上記のいずれかのディレクトリ ファイルがダウンロード（AutoGenerated または Corporate Directory.txt ファイルの場合）およびロードされます。アプリケーションが動作している限り、そのディレクトリ ファイルは、Attendant Settings ダイアログボックスの Advanced タブの Directory Reload Interval 設定に基づいて定期的にダウンロードまたは再ロード（あるいはその両方）が行われます。すべてのディレクトリ ファイルは、各行が 1 つのユーザ エントリのカンマ区切り形式になります。

デスクトップ アプリケーション内で、ディレクトリ ウィンドウ検索のためにディレクトリ ファイルをダウンロードすることで生成される追加のトラフィックは一般にわずかですが、いくつかの理由のために問題が生じることがあります。第 1 に、Cisco Unified CallManager ディレクトリ サイズが大きい場合、コンソール アプリケーションでダウンロードされる、ディレクトリ全体を含んだディレクトリ ファイルによって、ネットワークに大量のトラフィックが発生することがあります。この要因に、ネットワーク内の多数の AC デスクトップ アプリケーションがある、ダウンロード間隔が短い、集中型のコール処理が配置されている、コンソール アプリケーションが低速 WAN リンクを通じてリモート サイトで実行される、などの条件が加わると、ネットワーク輻輳、遅延、およびキューの発生する可能性が非常に高くなります。

デスクトップ アプリケーション用 PC でローカル ユーザ リスト ファイルを使用すると、ネットワーク帯域幅や輻輳に関する多くの問題が解消されますが、AC デスクトップのディレクトリ ウィンドウ内の Advanced search 機能で問題が発生しやすくなります。AC デスクトップ アプリケーションのディレクトリ ウィンドウ内のその他のすべてのディレクトリ検索は、ローカル ユーザ リスト ファイルまたはダウンロードされたファイルのいずれかに対して実行されますが、ディレクトリ ウィンドウの Advanced ボタンで開く Advanced search ウィンドウを使用して実行する検索には例外があります。Advanced search ウィンドウを使用した検索では、ディレクトリ ファイル検索規則がバイパスされ、実行時に Cisco Unified CallManager エンドユーザ ディレクトリに対して直接生成されます。つまり、定期的なディレクトリ ファイルのダウンロード以上に、ネットワーク上に追加のトラフィックが生じます。さらに、Advanced search 機能を使用してダウンロードできるエントリ数には制限がありません。このようなリアルタイム検索と取得で追加のネットワーク負荷が発生するだけでなく、返されるエントリに制限がないため、この追加の負荷は非常に大きくなることがあります。ディレクトリ ファイルのダウンロードと Advanced directory search の両方で発生するトラフィックは、ベストエフォートとしてマーキングされる RMI プロトコルを使用するため、ネットワーク パスでプライオリティ ボイス メディアおよびプロビジョニングされたコール シグナリング キューに輻輳の発生するリスクはありません。ただし、AC デスクトップ アプリケーション ディレクトリのトラフィックによって、ベストエフォート キューの輻輳が発生し、ディレクトリ トラフィックおよびその他のベストエフォート ネットワーク データ トラフィックのドロップにつながる可能性が残ります。

AC デスクトップ アプリケーションのディレクトリ ファイルのダウンロードおよびディレクトリ検索では、ネットワークの輻輳が発生する可能性があるため、次の対策を取ることをお勧めします。

- 管理者は、すべての Attendant Console ユーザに、Advanced directory search 機能の使用制限を求める必要があります。さらに、ユーザがこの機能を使用する場合は、返されるエントリの数を減らすために、Advanced search のパラメータ フィールドにできる限り多くの情報を入力してもらう必要があります。
- 集中型のコール処理配置シナリオでは、低速 WAN リンクを通じた Cisco Unified CallManager からのディレクトリ ファイルの定期的なダウンロードをなくすために、リモート サイト AC ユーザに対して AC クライアント PC またはネットワーク共有のユーザ リスト ファイルを利用する必要があります。最小限の管理オーバーヘッドでこの目標を達成する 1 つの方法は、各リモート サイトのローカル ネットワーク共有にユーザ リスト ファイルを提供することです。このファイルは、Cisco Unified CallManager データベースと同期するようにスケジューリングし、オフピーク時間または深夜にリモート ネットワーク共有に自動的にロードすることで、ピーク業務時間中にネットワーク輻輳が発生する可能性を抑えます。このようにすると、毎朝、AC ユーザがデスクトップ コンソールを起動するときに、このアプリケーションは最新のディレクトリ ユーザ リストをダウンロードできます。

これらの推奨事項は、次の 1 つ以上の条件が該当する場合は特に重要です。

- Cisco Unified CallManager クラスタ内に多数の AC ユーザが存在する。
- 低速 WAN リンクによって Cisco Unified CallManager から分離された多数の AC ユーザが存在する。
- エンドユーザ ディレクトリが非常に大きい。

AC の冗長性

AC アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、AC サービスまたはサーバの冗長性、および CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。
- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性は、コンソール担当者の電話機、AC パイロット ポイント、および Attendant Console デスクトップ アプリケーションに関連して検討し、さらにコンソール担当者とパイロット ポイントの到達可能性に関する冗長性として検討する必要があります。

サービスとコンポーネントの冗長性

図 20-12 に示すように、AC 機能は、主に Cisco CallManager Attendant Console Server サービスおよび Cisco CTIManager サービスに依存します。いずれの場合にも、冗長性は Cisco Unified CallManager クラスタ アーキテクチャに組み込まれます。AC Server サービスと CTIManager サービスの両方に対する冗長性は、各サービスが実行されるクラスタ内のノード数によって決定されます。冗長性は、サーバで障害が発生しても必要なサービスを提供し続けることができる障害の最大数で決まります。この数は、公式（N - 1）で表現でき、N はサービスを実行しているサーバの数です。たとえば、クラスタ内の 3 台のサーバが AC Server サービスを実行している場合は、N = 3 です。このサービスの冗長性を計算すると、(3 - 1)、つまり 2 になるため、最大 2 台のサーバの障害に対して冗長性が確保されることになります。CTIManager の冗長性は、同じ公式を使用して計算できます。これらのサービスで最大限の冗長性を得るには、クラスタ内のすべてのコール処理ノードで AC Server サービスと CTIManager サービスの両方を実行することをお勧めします。これに対し、最小限の冗長性を得るには、これらの各サービスを、クラスタ内の少なくとも 2 つのコール処理ノードで実行する必要があります。

パブリッシャは、Cisco Unified CallManager データベースへの書き込み時に単一の障害点となります。AC アプリケーションに対するパブリッシャの障害の影響はわずかです。パブリッシャに障害が発生しても、AC アプリケーションのすべての部分は引き続き動作します。ただし、AC アプリケーション設定を変更できなくなります。パブリッシャが復元するまで、AC パイロット ポイント、ハント グループ、およびコンソール担当者の電話機の設定は変更できません。

デバイスと到達可能性の冗長性

デバイス レベルでの AC の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、コンソール担当者の電話機と AC パイロット ポイントは、デバイス登録用のデバイス プールと Cisco Unified CallManager グループ設定の組み合せによって提供される組み込み冗長性に依存します。

また、一部のデバイスは、追加の冗長性および機能のためにコンポーネント サービスに依存します。たとえば、AC パイロット ポイントはコール制御機能で CTIManager にも依存するため、前の項で説明した CTIManager の冗長性に依存する必要があります。

Attendant Console デスクトップ アプリケーションも、冗長性および機能がコンポーネント サービスに依存します。AC デスクトップ アプリケーションは、着信コールの処理を継続できるように、冗長 AC Servers サービスと CTIManager サービス間の自動フェールオーバーをサポートしています。AC デスクトップ アプリケーションから見ると、これらのサービスの冗長性は以下に説明するように、Cisco Unified CallManager グループ メカニズムによって決定されます。第 1 に、AC デスクトップ アプリケーションが起動され、コンソール担当者がログインすると、このアプリケーションはデ

バイス プールおよび Cisco Unified CallManager グループ設定に基づいて、Cisco Unified CallManager のリストをダウンロードします。このリストは、ローカル PC の GlobalSettings.xml ファイルに保存され、デスクトップ用の CTIManager サービスの冗長性を決定します。

(注) Attendant Settings ダイアログボックスの Basic タブの Attendant Server Host Name フィールドまたは IP Address フィールドには、コンソール担当者の電話機に対して Cisco Unified CallManager グループで設定したプライマリ Cisco Unified CallManager サーバの IP アドレスを入力することをお勧めします。このように入力すると、障害が発生した場合、コンソール担当者の電話機と AC デスクトップ アプリケーションの両方が、電話機に設定された Cisco Unified CallManager グループの次のサーバに同時にフェールオーバーします。

次に、デスクトップ アプリケーションは AC サーバの冗長性に関して、デバイス プールおよび（コンソール担当者の電話機がメンバーとなっている）AC パイロット ポイントの Cisco Unified CallManager グループに依存します。いずれの場合にも、Cisco Unified CallManager グループには最大 3 台のサーバを設定できるため、最大 3 次の冗長性が実現します。

デスクトップ アプリケーションに対して、これらのサービスの冗長性をさらに与えるには、Attendant Settings ダイアログボックスの Advanced タブの Call Processing Server Host Names フィールドまたは IP Addresses フィールドを使用します。このフィールドで Cisco Unified CallManager サーバのカンマ区切りリストを設定すると、Cisco Unified CallManager グループ メカニズムを超える冗長性を実現できます。ただし、この追加の冗長性はグループ メカニズムを使い切った場合にだけ役に立つため、不要なことがあります。この追加の冗長性は、実際上、コンソール担当者の電話機と AC パイロット ポイントに登録サービスを提供している最初の 3 つのサーバが使用できない（つまり、コンソール担当者の電話機と AC パイロット ポイントも使用できない）場合にだけ利用されます。電話機とパイロット ポイントが使用できない場合、デスクトップ アプリケーションは使用できません。

最後に、AC パイロット ポイントでハント グループ メカニズムに組み込まれた到達可能性の冗長性（これにより、所定の冗長性が着信コールの発信者に提供されます）のほかに、追加の冗長性を AC パイロット ポイントの障害に対して提供することもできます。AC パイロット ポイントに障害が発生した場合、パイロット ポイント番号をダイヤルする着信コールの発信者にはビジー トーンが聞こえます。パイロット ポイントにフェールオーバー メカニズムを提供するには、パイロット ポイント回線設定画面の Call Forward No Answer（CFNA）フィールドで、別のパイロット ポイント番号を設定します。この CFNA メカニズムによって、障害の発生したパイロット ポイントへの発信者は、コールの処理およびルーティングのために別のパイロット ポイントに確実に転送されます。

AC のガイドラインと制限

AC は JTAPI レベルでパーティションを認識するため、Attendant Console デスクトップ アプリケーションは回線制御という点に関してパーティションを認識します。これに対し、他の AC コンポーネントはパーティションを認識しなかったり、重複や共有内線番号に関していくつかの制限があったりします。ディレクトリ番号のプロビジョニングを計画する場合は、次のガイドラインに注意してください。

- ハント グループ
  - シェアドラインは、ハント グループ メンバーが使用することはできません。
  - 重複内線番号は、ハント グループ メンバーが使用することはできません。
  - ハント グループ メンバーのディレクトリ番号は、Cisco Unified CallManager 回線グループに追加することはできません。

- パイロット ポイント
  - シェアドラインは、パイロット ポイントのディレクトリ番号として使用することはできません。
  - パイロット ポイントのディレクトリ番号は、Cisco Unified CallManager 回線グループに追加することはできません。
- コンソール ディレクトリと短縮ダイヤル ウィンドウ

  コンソール ディレクトリおよび短縮ダイヤルのウィンドウ内の回線ステータス表示では、シェアドラインと重複内線番号については何もわかりません。このため、共有または重複回線が見つかった場合は、最近変更された回線インスタンスのステータスだけが表示されます。

また、ハント グループ メンバーのディレクトリ番号があるすべてのパーティションを含むコーリング サーチ スペースを、必ずすべての AC パイロット ポイントに設定してください。このように設定しないと、1 つ以上のメンバーが到達不可能になります。

AC のパフォーマンスとキャパシティ

Cisco AC アプリケーションは、次のキャパシティをサポートしています。

- クラスタあたり最大 500 のコンソール担当者。
- クラスタあたり最大 500 のパイロット ポイント。
- Cisco MCS-7845 サーバは最大 1250 の AC デバイスをサポートします。
- Cisco MCS-7835 サーバは最大 1000 の AC デバイスをサポートします。
- Cisco MCS-7825 サーバは最大 750 の AC デバイスをサポートします。

（注） AC デバイスのキャパシティ数は、ハント パイロットとハント パイロット メンバーの間で分割できます。たとえば、MCS-7845 サーバでは AC デバイスの最大数が 1250 ですが、このキャパシティをさまざまな方法で割り当てることができます。125 のハント パイロットを用意して各ハント パイロットに 10 メンバーを含めたり、10 のハント パイロットを用意して各ハント パイロットに 125 メンバーを含めたりすることができます。

Cisco AC アプリケーションは、回線監視および電話制御のために CTIManager と対話します。コンソール担当者の電話機の各回線が、CTIManager への接続を生成します。また、各 AC パイロット ポイントが CTIManager への接続を生成します。AC アプリケーションを設定する場合、CTI 接続に対する全体的なクラスタ制限に関して、必要な CTI 接続の数を検討する必要があります（MCS-7845 プラットフォームのあるクラスタあたり 10,000 CTI 接続または MCS-7835 および MCS-7825 サーバのあるクラスタあたり 3200 CTI 接続）。他のアプリケーションのために追加の CTI 接続が必要な場合、AC アプリケーションのキャパシティが制限されることがあります。

AC と EM の相互作用

AC Console ユーザは、EM を使用してそれぞれの電話機にログインできます。ただし、コンソール担当者の電話機で設定が変更されるたびに、AC デスクトップ アプリケーションでは、AC ユーザがアプリケーションからログアウトしてログインし直す必要があります。EM ログイン（またはログアウト）によって電話機で設定が変更されるため、AC と EM を組み合せて使用する場合、ユーザは EM を使用してそれぞれの電話機にログインしてから、AC デスクトップ アプリケーションにログインします。これによって、デスクトップ アプリケーションからログアウトしてログインし直す必要がなくなります。

また、EM および AC の DN は、Device Members ではなく User Members として AC パイロット ポイントのハント グループに追加する必要があります。このようにすると、EM を使用してそれぞれの電話機にログインしていないために利用不可となっている AC ユーザに、着信コールがルーティングされなくなります。ハント グループの User Members は、ユーザ名と回線番号の両方で設定されます。これに対して、Device Members は、ディレクトリ番号だけで設定されます。パイロット ポイントは、ディレクトリ番号がビジーでないことだけを確認してから、Device Members にコールをルーティングします。パイロット ポイントは、コンソール担当者の電話機の回線番号が使用可能で、AC ユーザがログオンし、オンラインであることを確認してから、User Members にコールをルーティングします。このため、User Members として EM AC ユーザをハント グループに追加することにより、EM AC ユーザがログインしている場合にだけ、ユーザの電話機にコールを送信することができます。

WebDialer

WebDialer は Cisco Unified CallManager のクリックダイヤル アプリケーションで、ユーザはサポートされる任意の電話デバイスを使用して自分の PC から簡単にコールを発信できるようになります。管理者が CTI リンクを管理したり、JTAPI または TAPI アプリケーションを作成したりするための要件はありません。Cisco WebDialer には、独自のユーザ インターフェイスと認証メカニズムを提供するための、簡単な Web アプリケーションまたは Simple Objects Access Protocol（SOAP）が用意されているからです。どちらの方法でも、このソリューションは Cisco Unified CallManager クラスタ全体を完全な冗長性でサポートできます。

WebDialer Phone のサポート

次の SCCP 電話機は WebDialer をサポートしています。

- Cisco Unified IP Phone 7902G
- Cisco Unified IP Phone 7905G
- Cisco Unified IP Phone 7911G
- Cisco Unified IP Phone 7912G および 7912G-A
- Cisco Unified IP Phone 7920
- Cisco Unified IP Phone 7940G、7941G、および 7941G-GE
- Cisco Unified IP Phone 7960G、7961G、および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

また、次の SIP 電話機は WebDialer をサポートしています。

- Cisco Unified IP Phone 7941G および 7941G-GE
- Cisco Unified IP Phone 7961G および 7961G-GE
- Cisco Unified IP Phone 7970G および 7971G-GE

（注） WebDialer は、SIP ロードを実行している Cisco Unified IP Phone 7905G、7911G、7912G、7912G-A、7940G、または 7960G ではサポートされません。

Cisco Unified CallManager および WebDialer のサービス パラメータ

WebDialer アプリケーションを有効にするには、システム管理者は Cisco Unified CallManager Serviceability インターフェイスからいくつかの Cisco Unified CallManager 機能サービスをアクティブにし、起動する必要があります。また、WebDialer サービス パラメータは、WebDialer アプリケーションおよびサービスの動作を決定するための設定およびカスタマイズのオプションを提供します。

WebDialer 用の Cisco Unified CallManager サービス

WebDialer アプリケーションは次の機能サービスに依存します。これらのサービスは、Serviceability ページから手動でアクティブにする必要があります。

- Cisco WebDialer Web Service
- Cisco CTIManager

Cisco WebDialer Web Service は WebDialer Web ベース アプリケーションまたはデスクトップ アプリケーションへのインターフェイスを提供し、Cisco CTIManager サービスおよび Cisco Unified CallManager データベースと対話します。Cisco CTIManager サービスは、電話とコールの制御のために Cisco CallManager Service および Cisco WebDialer Web Service とインターフェイスし、対話します。

WebDialer サービス パラメータ

次の項目は、WebDialer 機能に関連する Cisco WebDialer Web Service サービス パラメータの一部のリストです。

- CTIManager Connection Security Flag（デフォルト値 = False）

  このパラメータは、Cisco WebDialer Web サービスと CTIManager との間でセキュアなトランスポート レイヤ セキュリティ（TLS）接続を使用するかどうかを決定します。このパラメータを True に設定した場合、アプリケーション ユーザの WDSecureSysUser のインスタンス ID に対して設定した Certificate Authority Proxy Function（CAPF）プロファイルを使用して、セキュアな接続が設定されます。このインスタンス ID は、サービス パラメータの CAPF Profile Instance ID for Secure Connection to CTIManager で指定する必要があります。

  （注） アプリケーション ユーザの WDSecureSysUser は、インストール時に自動的に作成されるシステム アカウントです。削除することはできません。

- CAPF Profile Instance ID for Secure Connection to CTIManager（デフォルト値 = <None>）

  CAPF Profile Instance ID は、WDSecureSysUser アプリケーション ユーザに対して Cisco WebDialer Web サービスと CTIManager との間で確立される TLS 接続またはインスタンスを識別するために使用される、数値または文字（あるいはその両方）の一意のストリングです。CTI Manager Connection Security Flag パラメータを True に設定した場合、このパラメータに値を設定する必要があります

- Primary Cisco CTIManager（デフォルト値 = 127.0.0.1）

  このパラメータは、Cisco WebDialer Web サービスがコールを処理するために使用するプライマリ CTIManager の IP アドレスを指定します。これはクラスタ全体のパラメータで、プライマリとバックアップという 2 つの CTIManager サーバだけを設定できます。

- Backup Cisco CTIManager（デフォルト値 = < ブランク >）

  このパラメータは、プライマリ CTIManager がダウンしている場合に、この Cisco WebDialer Web サービスがコールの処理に使用するバックアップ CTIManager の IP アドレスを指定します。これはクラスタ全体のパラメータです。

- List of WebDialers（デフォルト値 = < ブランク >）

  このパラメータは、企業内のすべての WebDialer の IP アドレスとポート番号を指定します。複数のエントリを区切るにはスペースを使用します。このパラメータは、Redirector 機能が必要な場合にだけ入力する必要があります。

WebDialer の機能とアーキテクチャ

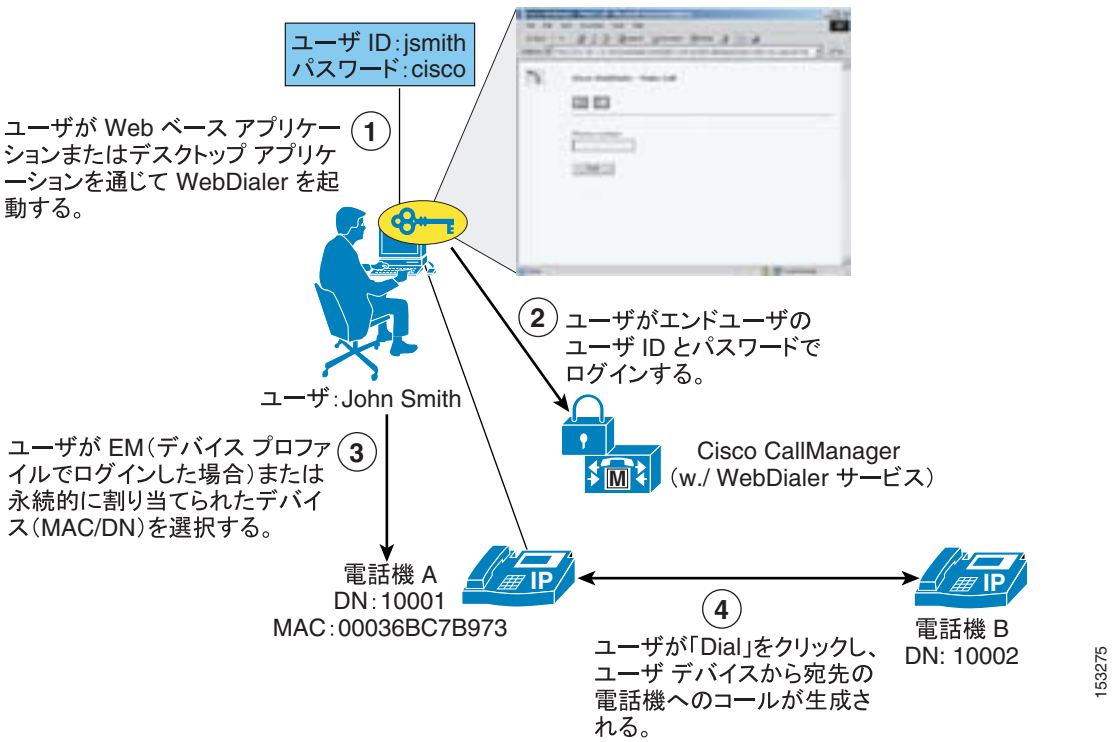
WebDialer アプリケーションには、WebDialer サーブレットと Redirector サーブレットの 2 つのサーブレットが含まれています。各サーブレットの動作と機能は似ていて、同時に実行するように設定できます。

WebDialer サーブレット

図 20-13 は、単純な WebDialer の例を示しています。この例で、ユーザ John Smith は、Web ベース アプリケーションまたはデスクトップ アプリケーションを通じて WebDialer を起動します（ステップ 1）。WebDialer は、ログイン クレデンシャル要求で応答します。ユーザは、Cisco Unified CallManager エンドユーザ ディレクトリで設定される有効なユーザ ID とパスワードで応答する必要があります。この場合、John Smith は userID = jsmith および password = cisco を送信します（ステップ 2）。次に、このログインに基づいて、WebDialer は Cisco WebDialer Preferences 設定ページで応答し、ユーザは「User permanent device」または「Use Extension Mobility」のいずれかを指定する必要があります（ユーザが EM デバイス プロファイルを持つ場合）。この場合、ユーザ John Smith は、「User permanent device」を選択し、設定ページのドロップダウン メニューからその電話機に対して適切な MAC アドレス（SEP00036BC7B973）とディレクトリ番号（10001）を選択します（ステップ 3）。最後に、コールする電話番号を要求する画面が表示され（この値はすでに表示されていることがあります）、ユーザは Dial をクリックする必要があります。この場合、John Smith が 10002 と入力し、Dial をクリックすると、その電話機から番号 10002 の電話機 B へのコールが自動的に生成されます（ステップ 4）。

（注） ユーザが以前に WebDialer アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。Cookie がブラウザでクリアされるか、または WebDialer サーバの再起動によってクリアされた場合は、再ログインが要求されます。

図 20-13　WebDialer サーブレットの動作



Redirector サーブレット

Redirector サーブレットは、マルチクラスタまたは分散型のコール処理環境において、WebDialer 機能を提供します。この機能を使用すると、すべての Cisco Unified CallManager クラスタ間で単一の企業全体の Web ベース WebDialer アプリケーションを使用できます。図 20-14 は、WebDialer アプリケーションの一部として Redirector サーブレットの基本的な動作を示しています。この例で、この会社には 3 つの Cisco Unified CallManager クラスタとして、New York、Chicago、San Francisco があります。3 つのクラスタはすべて、単一の WebDialer アプリケーションで設定されます。San Francisco クラスタは、Redirector として指定されます。企業全体の Redirector として San Francisco の WebDialer を指定するには、各クラスタ WebDialer サーバに独自の IP アドレス、および San Francisco の WebDialer IP アドレスで指定されたサービス パラメータ List of WebDialer が必要です（P.20-41 の「WebDialer サービス パラメータ」を参照してください）。San Francisco の WebDialer サーバには、独自の IP アドレスと、企業内のその他の WebDialer サーバすべてのアドレスが設定されます。この例に基づいて、各 WebDialer サーバの List of WebDialers サービス パラメータ フィールドは、次のように設定されます。

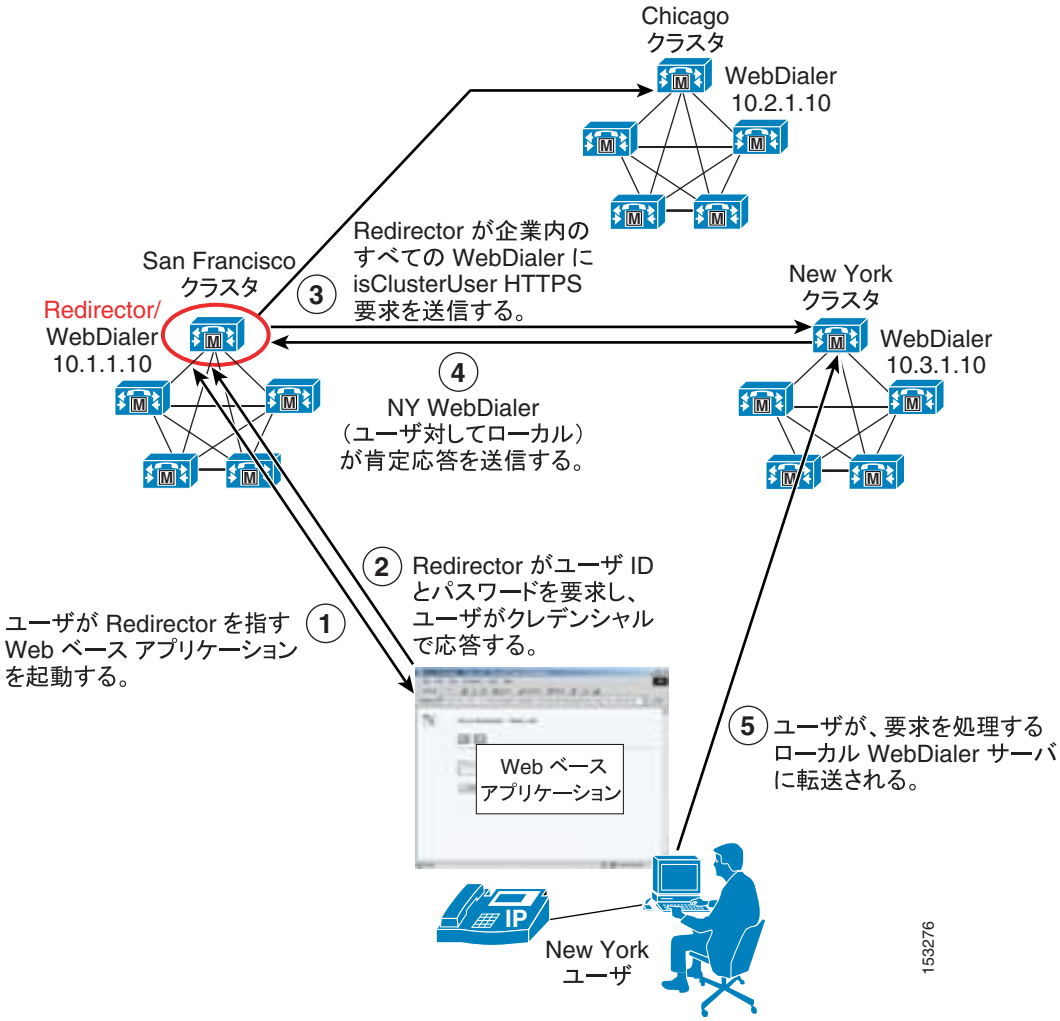
- New York の WebDialer：List of WebDialers: 10.1.1.10:8443 10.3.1.0:8443
- Chicago の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443
- San Francisco の WebDialer：List of WebDialers: 10.1.1.10:8443 10.2.1.0:8443 10.3.1.0:8443

企業全体の Web ベース アプリケーションは San Francisco の Redirector を指し、New York のユーザから起動されます（図 20-14 のステップ 1 を参照してください）。次に、Redirector はユーザのログインを要求し、New York ユーザは自分のユーザ ID とパスワードで応答します（図 20-14 のステップ 2 を参照してください）。

（注） ユーザが以前に Redirector アプリケーションにログインし、Web ブラウザおよびサーバの Cookie がまだアクティブになっている場合、次の要求時に再ログインは求められません。

次に、Redirector は、（List of WebDialers サービス パラメータの設定に従って）企業内のすべての WebDialer に isClusterUser HTTPS 要求を送信します。この例で、要求は Chicago および New York の WebDialer サーバに送信されます（図 20-14 のステップ 3 を参照してください）。New York ユーザは New York クラスタに対してローカルであるため、New York の WebDialer は肯定応答を返します（図 20-14 のステップ 4 を参照してください）。最後に、New York ユーザはアプリケーション要求を処理するローカル WebDialer サーバに転送されます（図 20-14 のステップ 5 を参照してください）。この転送はユーザに通知されません。ただし、ブラウザのアドレス バーの URL は、ユーザが Redirector から WebDialer サーバに転送されたときに変更されます。

図 20-14　Redirector サーブレットの動作



(注)

Redirector アプリケーションは、Cisco Unified CallManager データベースでのユーザ認証の必要な企業全体のアプリケーションであるため、すべての Cisco Unified CallManager クラスタですべてのエンドユーザのユーザ ID を一意にすることを強くお勧めします。一意でない場合、Redirector アプリケーションが isClusterUser 要求に対する複数の肯定応答を受信する可能性があります。この場合、Redirector アプリケーションによって、ユーザは自分のローカル WebDialer サーバを手動で選択するように求められます。このため、ユーザは自分のローカル サーバを知っている必要があります。正しくないサーバを選択した場合、WebDialer 要求は失敗します。

WebDialer のアーキテクチャ

WebDialer アプリケーションの機能と同様に、そのアーキテクチャについても理解することが重要です。図 20-15 は、WebDialer のメッセージ フローとアーキテクチャを示しています。次の一連の対話とイベントが発生します。

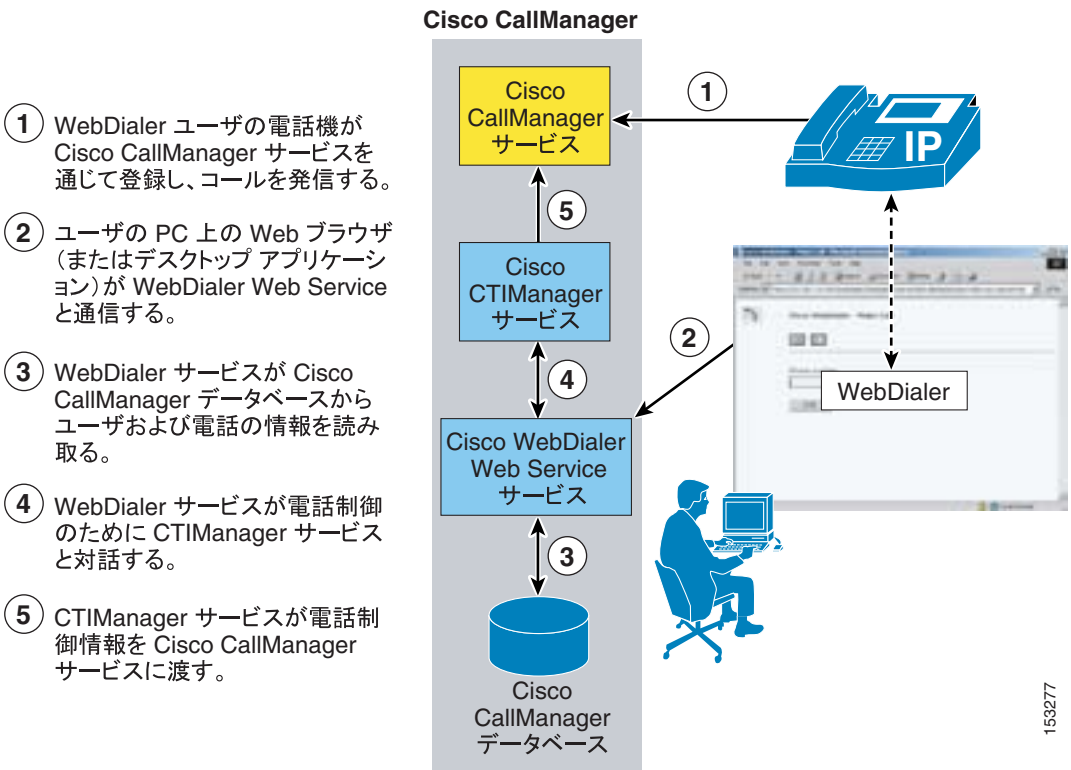
1. WebDialer ユーザの電話機は、Cisco CallManager サービスを通じて登録し、コールの発信と受信を行います（図 20-15 のステップ 1 を参照してください）。

2. ユーザの PC 上の WebDialer アプリケーションは、次のいずれかのインターフェイスを通じて Cisco WebDialer Web Service と通信します（図 20-15 のステップ 2 を参照してください）。
   - HTML over HTTPS

     このインターフェイスは、HTTPS プロトコルに基づいて Web ベースのアプリケーションで使用されます。これは、Redirector サーブレットへのアクセスを提供する唯一のインターフェイスです。
   - SOAP（Simple Object Access Protocol）over HTTP

     このインターフェイスは、SOAP インターフェイスに基づいてデスクトップ アプリケーションで使用されます。
3. WebDialer Web サービスは、Cisco Unified CallManager データベースからユーザおよび電話の情報を読み取ります（図 20-15 のステップ 3 を参照してください）。
4. 次に、WebDialer Web サービスは、回線と電話の制御情報を交換するために、CTIManager サービスと対話します（図 20-15 のステップ 4 を参照してください）。
5. CTIManager サービスは、WebDialer 電話制御情報を Cisco CallManager サービスに渡します（図 20-15 のステップ 5 を参照してください）。

図 20-15　WebDialer のアーキテクチャ



（注） 図 20-15 は、すべて同じノードで実行されている Cisco Unified CallManager、CTIManager、および WebDialer Web Service サービスを示していますが、この設定は必須ではありません。これらのサービスはクラスタ内の複数のノードに分散できますが、説明を簡単にするためにここでは同じノードにあるものとしています。

WebDialer の URL

Web ベースのアプリケーションから HTML-over-HTTPS インターフェイスを通じて WebDialer アプリケーションにアクセスするには、次の URL を使用します。

- WebDialer サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Webdialer?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行しているクラスタ内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

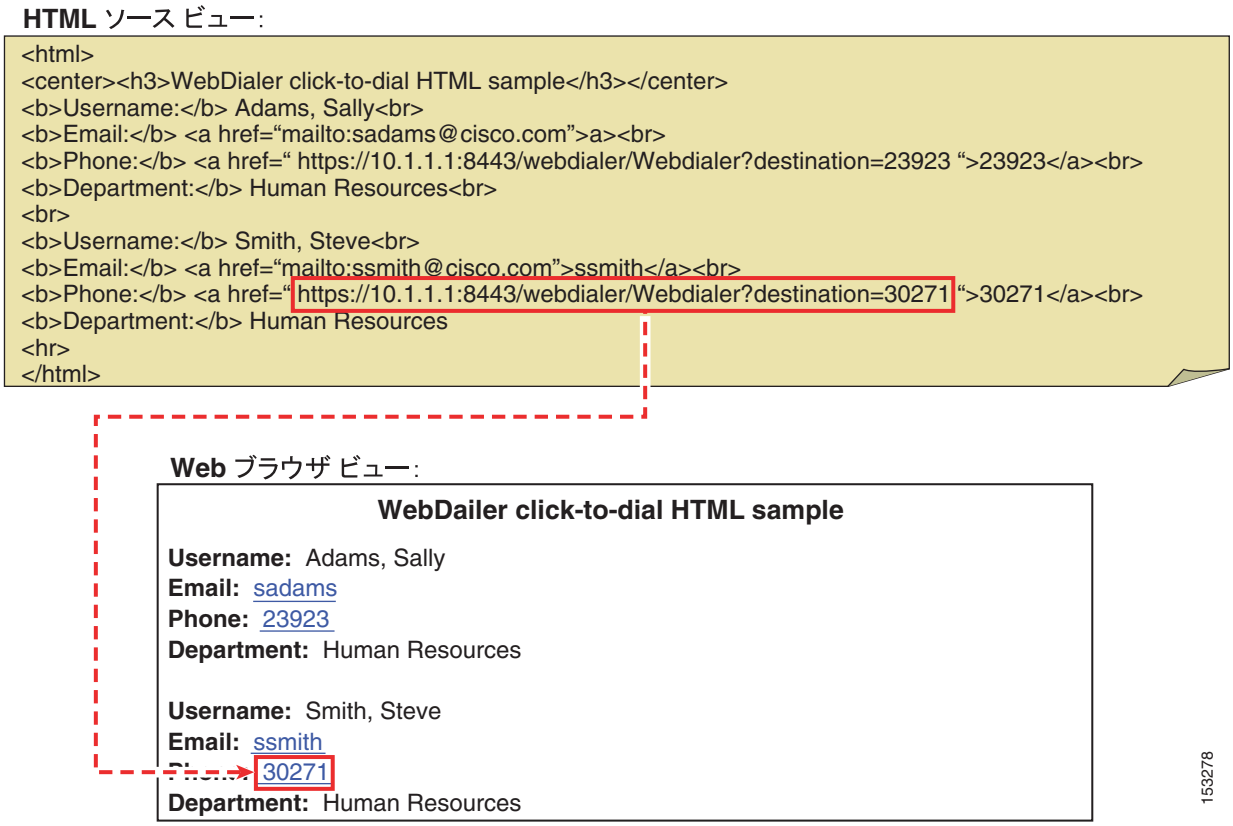
- Redirector サーブレット

  https://<*Server-IP_Addr*>:8443/webdialer/Redirector?destination=<*Number_to_dial*>

  （ここで、<*Server_IP-Address*> は、Cisco WebDialer Web Service サービスを実行している企業内のノードの IP アドレスで、<*Number_to_dial*> は WebDialer ユーザがダイヤルする番号です）

図 20-16 は、Cisco WebDialer アプリケーションをコールするクリックダイヤル Web ベース アプリケーションで使用される、HTML ソース コードの例を示しています。この例で、HTML ソース ビューの URL https://10.1.1.1:8443/webdialer/Webdialer?destination=30271 は、Web ブラウザ ビュー内のユーザ Steve Smith 用の「Phone: 30721」リンクに対応しています。ユーザがこのリンクをクリックすると、WebDialer アプリケーションが起動し、ログイン後に Dial をクリックすると、そのユーザの電話機から Steve Smith の電話機へのコールが生成されます。URL を https://10.1.1.1:8443/webdialer/Redirector?destination=30271 に変更すると、Redirector を使用するクリックダイヤル アプリケーションで同じコードを使用できます。

図 20-16　WebDialer URL の HTML の例



WebDialer の冗長性

WebDialer アプリケーションの冗長性は、次の 2 つのレベルで実現できます。

- コンポーネント レベルとサービス レベルでの冗長性

  このレベルでの冗長性については、冗長性を、WebDialer サービスおよび CTIManager サービスの冗長性に関して検討する必要があります。同様に、パブリッシャの冗長性の欠如、およびこのコンポーネントの障害の影響も検討する必要があります。

- デバイス レベルと到達可能性レベルでの冗長性

  このレベルでの冗長性については、ユーザの電話機および WebDialer ユーザ インターフェイスに関連して検討する必要があります。

サービスとコンポーネントの冗長性

図 20-15 に示すように、WebDialer 機能は、主に Cisco WebDialer Web Service および Cisco CTIManager サービスに依存します。WebDialer サービスの場合は、List of WebDialers サービス パラメータ（P.20-41 の「WebDialer サービス パラメータ」を参照）に複数の WebDialer サーバの IP アドレスをリストし、クラスタ内の複数のノードでサービスを有効にすることで、冗長性を実現します。CTIManager の場合、冗長性は、プライマリおよびバックアップのメカニズムを使用して自動的に組み込まれます。Primary Cisco CTIManager および Backup Cisco CTIManager のサービス パラメータを使用すると、クラスタ内に 2 つの CTIManager サーバまたはサービスを定義できます（P.20-41 の「WebDialer サービス パラメータ」を参照してください）。これらのパラメータを設定すると、CTIManager サービスに冗長性を与えることができます。このため、プライマリ CTIManager に障害が発生した場合でも、CTIManager サービスはバックアップ CTIManager から提供できます。Web ベース（またはデスクトップ）アプリケーションが指している WebDialer サーバに障害が発生し、クラスタ ノード上のプライマリおよびバックアップ CTIManager サービスにも障害が発生した場合、WebDialer アプリケーションはダウンします。

前述のように、パブリッシャは Cisco Unified CallManager データベースへの書き込み時に単一の障害点となります。WebDialer アプリケーションに対するパブリッシャの障害の影響はわずかです。パブリッシャに障害が発生しても、WebDialer アプリケーションのすべての部分が引き続き動作します。

デバイスと到達可能性の冗長性

デバイス レベルでの WebDialer の冗長性は、いくつかのメカニズムに依存しています。まず第 1 に、ユーザの電話機は、デバイス登録用のデバイス プールと Cisco Unified CallManager グループ設定の組み合せによって提供される組み込み冗長性に依存します。

WebDialer アプリケーションには、サーバから見た場合の冗長性を与えることはできますが、WebDialer のユーザ インターフェイスにはデフォルトで冗長性がありません。WebDialer ユーザ インターフェイスは、WebDialer サーバとの接続を Web ブラウザまたはデスクトップ アプリケーションに依存しているため、WebDialer URL またはデスクトップ アプリケーションのポインタは、IP アドレスで WebDialer サーバをコールします。WebDialer サーバに障害が発生すると、ユーザ インターフェイスは WebDialer アプリケーションと通信できなくなります。フェールオーバー メカニズムが Web ベース アプリケーションまたはデスクトップ アプリケーションに組み込まれない限り、アプリケーション内でフェールオーバーを実現することはできません。その代わりに、図 20-3 に示すようなサーバ ロード バランシング（SLB）メカニズムを使用して、フェールオーバーを実現できます。この場合、Web ベース アプリケーションまたはデスクトップ アプリケーションは、クラスタ内で設定された WebDialer サーバの実 IP アドレスのフロントエンドとなる仮想 IP アドレスを指します。このようにすると、同じユーザ インターフェイス内で WebDialer 間のフェールオーバーが可能になります。

WebDialer のガイドラインと制限

次のガイドラインと制限は、Cisco Unified CallManager テレフォニー環境内の WebDialer の配置と動作に関連して適用されます。

- 管理者は、すべての WebDialer ユーザを Cisco Unified CallManager エンドユーザ ディレクトリの電話機またはデバイス プロファイルに関連付ける必要があります。
  - 電話機が関連付けられていない状態でユーザが Cisco WebDialer Preferences 画面の「Use permanent device」を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

    「No supported device configured for user」
  - デバイス プロファイルが関連付けられていない状態で（またはプロファイルを使用してログインしないで）ユーザが Cisco WebDialer Preferences 画面の Use Extension Mobility を選択すると、Dial ボタンを押したときに次のメッセージが表示されます。

    「Call to <*dialed_ number*> failed: User not logged in on any device」

（注）　WebDialer および EM アプリケーションは組み合せて使用できます。WebDialer と EM の相互作用の詳細については、P.20-48 の「WebDialer と EM の相互作用」を参照してください。

- List of WebDialers サービス パラメータ（P.20-41 の「WebDialer サービス パラメータ」を参照）を設定するときは、WebDialer IP アドレスと同時にポート番号 8443 を指定する必要があります。
- Client Matter Codes（CMC）または Forced Authorization Codes（FMC）を使用している場合、WebDialer ユーザはトーンが聞こえたときに、電話機のキーパッドを使用して適切なコードを入力する必要があります。トーンが聞こえたときに適切なコードを入力しないと、コールの失敗を示すリオーダー トーンが聞こえます。

WebDialer と EM の相互作用

WebDialer ユーザは、EM を使用してそれぞれの電話機にログインできます。EM ユーザは、Cisco WebDialer Preferences ページで Use Extension Mobility 設定を選択するだけで、WebDialer を使用できます。

推奨されるハードウェアとソフトウェアの組み合せ

Cisco Unified CallManager ベースの Cisco Unified Communications System の配置で推奨されるハードウェア プラットフォーム、ソフトウェア リリース、およびファームウェア バージョンの最新情報については、次の Web サイトで入手可能な最新の『*System Release Notes for IP Telephony*』を定期的に確認してください。

http://www.cisco.com/univercd/cc/td/doc/systems/unified/unified1/relnotes/rnc50ipt.htm

(注) 『*System Release Notes for IP Telephony*』で推奨されているプラットフォームとソフトウェア バージョンだけが、サポートされる配置オプションとなるわけではありません。この表のオプションは、シスコによる広範囲にわたるシステム レベルのテストに対応するハードウェアとソフトウェアの組み合せを表しています。十分な検証を重ねてきましたが、その検証には、さまざまな配置モデル、複数のエンド ステーション サイズのカテゴリ、および実際のコール フロー、トラフィック パターン、導入事例が使用されています。Cisco Unified Communications の配置で使用できるハードウェアとソフトウェアのその他のオプションの詳細については、製品を購入された代理店にお問い合せください。

Cisco Unified Communications System に関する追加情報については、次の Web サイトで入手可能な資料を参照してください。

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

A

AA	自動応答機能
AAD	警告とアクティビティの表示
AAR	Automated Alternate Routing
AC	Cisco Attendant Console
ACD	自動着信呼分配
ACF	アドミッション確認
ACL	アクセス コントロール リスト
ACS	アクセス コントロール サーバ
AD	Microsoft Active Directory
ADUC	Active Directory ユーザとコンピュータ
AFT	ALI フォーマット ツール
AGM	Cisco アクセス ゲートウェイ モジュール
ALG	アプリケーション レイヤ ゲートウェイ
ALI	自動ロケーション識別
AMI	交互マーク反転
AMIS	Audio Messaging Interchange Specification
ANI	自動番号識別
AP	アクセス ポイント
API	アプリケーション プログラミング インターフェイス
ARJ	アドミッション拒否
ARP	アドレス解決プロトコル
ARQ	アドミッション要求
ASA	適応型セキュリティ アプライアンス
ASP	Active Server Pages

ASR 自動音声認識

ATA Cisco Analog Telephone Adapter

ATM 非同期転送モード

B

BAT Cisco Bulk Administration Tool

BBWC バッテリ バックアップ付き書き込みキャッシュ

BGP ボーダー ゲートウェイ プロトコル

BHCA Busy Hour Call Attempts

BHCC Busy Hour Call Completions

BPDU ブリッジ プロトコル データ ユニット

bps ビット / 秒

BRI 基本速度インターフェイス

BTN 請求先番号

C

CA 認証機関

CAC コール アドミッション制御

CAM 連想メモリ

CAMA Centralized Automatic Message Accounting

CAPF 認証機関プロキシ機能

CAR Cisco CDR 分析とレポート

CAS 個別線信号方式

CBWFQ クラスベース WFQ

CCA Clear Channel Assessment

CCS 共通線信号方式

CDP シスコ検出プロトコル

CDR コール詳細レコード

CGI Common Gateway Interface

CIR 認定情報レート

CKM Cisco Centralized Key Management

CLEC	競争的地域通信事業者
CLID	発呼回線 ID
CMC	クライアント証明書コード
CME	Cisco Unified CallManager Express
CMI	Cisco Messaging Interface
CMM	Cisco コミュニケーション メディア モジュール
CNG	コンフォート ノイズ生成
CO	セントラル オフィス
COM	コンポーネント オブジェクト モデル
COR	制限クラス
CoS	サービス クラス
CPCA	Cisco Unity Personal Assistant
CPI	Cisco Product Identification ツール
CPN	発番号
CRS	Cisco Customer Response Solutions
cRTP	Compressed Real-Time Transport Protocol（RTP ヘッダー圧縮）
CSUF	クロススタック UplinkFast
CTI	コンピュータ / テレフォニー インテグレーション
CUE	Cisco Unity Express

D

DC	ドメイン コントローラ
DDNS	ダイナミック ドメイン ネーム サーバ
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル
DID	ダイヤルイン方式
DIT	ディレクトリ インフォメーション ツリー
DMZ	非武装地帯
DN	ディレクトリ番号
DNIS	着信番号識別サービス
DNS	ドメイン ネーム システム
DoS	サービス拒絶

DPA Digital PBX Adapter

DSCP DiffServ コード ポイント

DSE Digital Set Emulation

DSP デジタル シグナル プロセッサ

DTMF Dual Tone Multifrequency

DTPC ダイナミック伝送パワー コントロール

DUC Domino Unified Communications Services

E

E&M 受信と伝送（Ear and Mouth）

EAP 拡張可能認証プロトコル

EC エコー キャンセレーション

ECM エラー訂正モード

ECS Empty Capabilities Set

EI Enhanced Image

EIGRP Enhanced IGRP

ELIN 緊急ロケーション識別番号

EM エクステンション モビリティ

ER Cisco Emergency Responder

ERL 緊急応答ロケーション

ESF 拡張スーパ フレーム

F

FAC 強制アカウント コード

FCC 米国連邦通信委員会

FIFO ファーストイン ファーストアウト

FR フレーム リレー

FWSM ファイアウォール サービス モジュール

FXO Foreign Exchange Office

FXS Foreign Exchange Station

G

GARP 一般属性登録プロトコル

GC グローバル カタログ

GKTMP ゲートキーパー トランザクション メッセージ プロトコル

GMS グリーティング管理システム

GPO グループ ポリシー オブジェクト

GUI グラフィカル ユーザ インターフェイス

GUP Gatekeeper Update Protocol

H

H.225D H.225 デーモン

HP Hewlett-Packard

HSRP ホットスタンバイ ルータ プロトコル

HTTP ハイパーテキスト転送プロトコル

Hz ヘルツ

I

IANA Internet Assigned Numbers Authority（インターネット割り当て番号局）

IAPP アクセス ポイント間プロトコル

ICCS Intra-Cluster Communication Signaling

ICMP インターネット制御メッセージ プロトコル

ICS IBM 配線システム

ICT クラスタ間トランク

IETF Internet Engineering Task Force（インターネット技術特別調査委員会）

IGMP インターネット グループ管理プロトコル

IIS Microsoft Internet Information Server

IntServ 統合サービス

IntServ/DiffServ 統合サービス / ディファレンシエーテッド サービス

IP インターネット プロトコル

IPCC Cisco IP コンタクト センター

IPIPGW IP-to-IP ゲートウェイ

IPSec IP Security

ISO 国際標準化機構

ITEM CiscoWorks IP Telephony Environment Monitor

ITU 国際電気通信連合

IVR 音声自動応答装置

J

JTAPI Java Telephony Application Programming Interface

K

Kbps キロビット / 秒

KPML Key Press Markup Language

L

LAN ローカルエリア ネットワーク

LBR 低ビット レート

LCD 液晶ディスプレイ

LCF ロケーション確認

LDAP Lightweight Directory Access Protocol

LDAPS LDAP over SSL

LDIF LDAP Data Interchange Format

LDN Listed Directory Number

LEAP 簡易拡張可能認証プロトコル

LEC 地域通信事業者

LFI Link Fragmentation and Interleaving

LLQ 低遅延キューイング

LRJ ロケーション拒否

LRQ ロケーション要求

LSC ラベル スイッチ コントローラ

M

MAC	メディア アクセス制御
MAN	メトロポリタン エリア ネットワーク
Mbps	メガビット / 秒
MCM	Multimedia Conference Manager
MCS	Media Convergence Server
MCU	マルチポイント コントロール ユニット
MFT	Multiflex Trunk
MGCP	メディア ゲートウェイ コントロール プロトコル
MIC	製造元でインストールされる証明書
MIPS	100 万命令 / 秒
MISTP	マルチインスタンス スパニング ツリー プロトコル
MITM	中間者
MLA	Cisco マルチレベル管理
MLP	マルチリンク ポイントツーポイント プロトコル
MLPP	Multilevel Precedence and Preemption
MLTS	Multi-Line Telephone System
MoH	Music on Hold
MPLS	Multiprotocol Label Switching
MRG	メディア リソース グループ
MRGL	メディア リソース グループ リスト
ms	ミリ秒
MTP	メディア ターミネーション ポイント
mW	ミリワット
MWI	メッセージ待機インジケータ

N

NAT	ネットワーク アドレス変換
NENA	National Emergency Number Association
NFAS	ノンファシリティ アソシエーテッド シグナリング
NIC	ネットワーク インターフェイス カード

NPA 番号計画エリア

NSE Named Service Event

NSF Network Specific Facilities

NTE Named Telephony Event

NTP ネットワーク タイム プロトコル

O

OSPF Open Shortest Path First

OU 組織ユニット

P

PAC Protected Access Credential

PBX 構内交換機

PC パーソナル コンピュータ

PCI Peripheral Component Interconnect

PCM パルス符号変調

PD 受電装置

PHB Per-Hop Behavior

PIN Personal Identification Number

PINX Private Integrated Services Network Exchange

PIX プライベート インターネット エクスチェンジ

PLAR Private Line Automatic Ringdown

PoE Power over Ethernet

POTS 一般電話サービス

pps 1 秒当たりのパケット数

PQ プライオリティ キュー

PRI Primary Rate Interface

PSAP Public Safety Answering Point

PSE 電源機器

PSTN 公衆電話交換網

PVC 相手先固定接続

Q

QBE	Quick Buffer Encoding
QBSS	QoS 基本サービス セット
QoS	Quality of Service
QSIG	Q シグナリング

R

RADIUS	Remote Authentication Dial-In User Service
RAS	登録アドミッション ステータス
RCP	リモート コピー プロトコル
RDNIS	Redirected Dialed Number Information Service
RF	無線周波数
RFC	Request for Comments
RIP	Routing Information Protocol
RSP	Route/Switch Processor
RSSI	相対信号強度インジケータ
RSTP	敏速スパニング ツリー プロトコル
RSVP	リソース予約プロトコル
RTMT	Cisco Real-Time Monitoring Tool
RTP	Real-Time Transport Protocol
RTT	ラウンドトリップ時間

S

S1、S2、S3、および S4	サービス リクエストのための重大度のレベル
SCCP	Skinny Client Control Protocol
SCSI	Small Computer System Interface
SDK	ソフトウェア開発キット
SDL	信号配信レイヤ
SDP	Session Description Protocol

SE シスコ システム エンジニア

SF スーパー フレーム

SI Standard Image

SIP Session Initiation Protocol

SIW サービス インターワーキング

SLB サーバ ロード バランシング

SLDAP Secure LDAP

SMDI Simplified Message Desk Interface

SNMP 簡易ネットワーク管理プロトコル

SQL 構造化照会言語

SRND ソリューション リファレンス ネットワーク デザイン

SRST Survivable Remote Site Telephony

SRTP Secure Real-Time Transport Protocol

SRV サーバ

SS7 No.7 共通線信号方式

SSID サービス セット識別子

SSL Secure Sockets Layer

STP スパニング ツリー プロトコル

SUP1 Cisco スーパーバイザ エンジン 1

SUP2 Cisco スーパーバイザ エンジン 2

SUP2+ Cisco スーパーバイザ エンジン 2+

SUP3 Cisco スーパーバイザ エンジン 3

T

TAC Cisco Technical Assistance Center

TAPI テレフォニー アプリケーション プログラミング インターフェイス

TCD Telephony Call Dispatcher

TCER Total Character Error Rate

TCL Tool Command Language

TCP 伝送制御プロトコル

TCS 端末機能セット

TDD Telephone Device for the Deaf

TDM 時分割多重

TEHO テールエンド ホップオフ

TFTP Trivial File Transfer Protocol

TLS トランスポート レイヤ セキュリティ

ToD 時間帯

ToS タイプ オブ サービス

TRaP 電話機による録音と再生

TSP テレフォニー サービス プロバイダー

TTL 存続可能時間

TTS テキストと音声間の変換

TTY ターミナル テレタイプ

TUI テレフォニー ユーザ インターフェイス

U

UAC ユーザ エージェント クライアント

UAS ユーザ エージェント サーバ

UDC ユニバーサル データ コネクタ

UDLD 単方向リンク検出

UDP ユーザ データグラム プロトコル

UN Unsolicited SIP Notify

UNC 汎用命名規則

UPS 無停電電源装置

URI ユニフォーム リソース識別子

USB ユニバーサル シリアル バス

UTIM Cisco Unity Telephony Integration Manager

UTP シールドなしツイストペア

UUIE ユーザ間情報要素

V

V3PN	シスコの音声およびビデオ対応バーチャル プライベート ネットワーク
VAD	音声アクティビティ検出
VAF	ボイス適応型フラグメンテーション
VATS	ボイス適応型トラフィック シェーピング
VIC	音声インターフェイス カード
VLAN	バーチャル LAN
VMO	ViewMail for Outlook
VoIP	Voice over IP
VoPSTN	Voice over the PSTN
VPN	バーチャル プライベート ネットワーク
VWIC	音声 /WAN インターフェイス カード

W

WAN	ワイドエリア ネットワーク
WEP	Wired Equivalent Privacy
WFQ	重み付け均等化キューイング
WINS	Windows Internet Naming Service
WLAN	無線 LAN
WLSM	Cisco 無線 LAN サービス モジュール

X

XML	eXtensible Markup Language

Symbols

!、ルート パターン内の　10-18
@、ルート パターン内の　10-18

Numerics

1700 シリーズ ルータ　6-10, 6-12
1A および 2A ケーブリング　3-22
2 層ハブアンドスポーク トポロジ　9-42
2800 シリーズ ルータ　6-9, 6-12, 6-18, 6-24
3500 シリーズ ビデオ ゲートウェイ　4-34
3800 シリーズ ルータ　6-9, 6-12, 6-18, 6-24
4ESS　4-17, 4-18
508 準拠　2-28
5ESS　4-17, 4-18
7902G IP Phone　19-7
7905_7912 ダイヤル規則　10-14, 10-78
7905G IP Phone　19-7
7911G IP Phone　19-7
7912G IP Phone　19-7
7914 拡張モジュール　19-10
7920 Wireless IP Phone　15-51, 19-16, 19-37
7935 IP Conference Station　19-21
7936 IP Conference Station　19-21
7940_7960_OTHER ダイヤル規則　10-14, 10-78
7940G IP Phone　19-8
7941G IP Phone　19-8
7941G-GE IP Phone　19-8
7960G IP Phone　19-9
7961G IP Phone　19-9
7961G-GE IP Phone　19-9
7970G IP Phone　19-10
7971G-GE IP Phone　19-10
7985G IP Video Phone　19-24, 19-25, 19-41
802.1s　3-4
802.1w　3-4, 3-6
802.3af PoE　3-21
9.@ ルート パターン　10-18
911 コール　10-63, 11-1
911 コール用のインターフェイス タイプ　11-4
911 へのテスト コール　11-14

A

AAR
　Cisco Unity を使用した　13-9
　Voice Over the PSTN 用　2-11, 2-13
　ダイヤル プランの考慮事項　10-28
　ハント パイロットを使用した　10-97
　ビデオ コールの　4-38, 15-9
　無線 IP Phone を使用した　19-20
AC　1-7, 8-15, 20-29
ac のアプリケーション ユーザ名　20-30
Access Control Server（ACS）　3-67
ACF　10-45
ACL　18-26, 18-28, 19-40
ACS　3-67
Active Directory（AD）　3-67, 16-11, 16-14, 16-17, 16-22
AD　3-67, 16-11, 16-14, 16-17, 16-22
Adaptive Security Appliance（ASA）　18-31, 18-33
AFT　11-20
Aironet　15-51
ALI　11-4, 11-20
ALI フォーマット ツール（AFT）　11-20
Analog Telephone Adapter（ATA）　19-6, 19-29
ANI　4-13, 11-4, 11-6, 11-7
Annex M1　5-12
Annunciator　6-20
AP　3-62, 3-65, 19-16
ARJ　10-45
ARP　3-66, 18-21
ARQ　10-45
ASA　18-31, 18-33

Assistant Console 20-23
ATA 19-6, 19-29
ATM 2-7, 2-16, 3-31
Attendant Console（AC） 1-7, 8-15, 15-49, 20-29
Audio Server 14-6, 14-41
AutoGenerated.txt ディレクトリ ファイル 20-34

B

B チャネル 4-41
BackboneFast 3-6
Bearer Capabilities Information Element（bearer-caps） 4-44
bearer-caps コマンド 4-44
BHCA 2-25, 8-19, 8-20, 10-99
BHCC 10-99
BPDU 3-6
BTN 11-4
Busy Hour Call Attempts（BHCA） 2-25, 8-19, 8-20, 10-99
Busy Hour Call Completions（BHCC） 10-99

C

C542 チップセット 6-7
C5421 チップセット 6-5
C549 チップセット 6-6
C5510 チップセット 6-4
CAC（「コール アドミッション制御」を参照）
CallManager（「Cisco Unified CallManager」を参照）
CallManager Express（CME） 2-18, 8-33
CallManager キャパシティ ツール 8-16, 8-17, 8-18
CAM 18-14
CAMA 11-5
CanMapAlias 5-12
CCA 3-66
CDP 18-13, 19-22
CDR 2-22
Centralized Automatic Message Accounting（CAMA） 11-5
CIF 19-26
CIR 3-37
Cisco Aironet 15-51
Cisco Centralized Key Management（Cisco CKM） 19-17
Cisco Discovery Protocol（CDP） 18-13, 19-22
Cisco Emergency Responder（ER） 11-9, 11-13, 15-48, 19-20
Cisco IOS
  ゲートウェイ 4-28, 4-29
  ゲートキーパー 15-24
  コール ルーティング 10-39, 10-42
  コール特権 10-52
  サービス クラス 10-92
  サポートされる DSP リソース 6-4, 6-5, 6-6, 6-7
  ソフトウェア MTP 6-18
  番号操作 10-55
  必要な最小リリース 19-3
Cisco IP Communicator 19-33, 19-43
Cisco IP Conference Station 19-21, 19-29
Cisco IP SoftPhone 11-13, 15-50, 19-12, 19-33, 19-43
Cisco IP Voice Media Streaming Application 6-20
Cisco LEAP 3-67, 19-16, 19-17
Cisco Messaging Interface（CMI） 12-2
Cisco Multimedia Conference Manager（MCM） 5-12, 15-38
Cisco Product Identification（CPI）ツール xxvi
Cisco Security Agent 18-42
Cisco Technical Assistance Center（TAC） xxvi
Cisco Unified CallManager
  FAX とモデム サポート用の Cisco IOS ゲートウェイの設定 4-29
  H.323 5-10
  IP ビデオ テレフォニー用の機能拡張 15-2
  MeetingPlace との統合 14-1
  Release 3.3 10-33
  Release 4.0 10-33
  Release 4.0 からの移行 15-47
  同じクラスタにバージョンが異なる 3-18
  同じ場所にあるクラスタ 9-54
  キャパシティ ツール 8-16, 8-17, 8-18
  グループ 2-24, 2-27
  混在モード動作 3-18
  サービス 20-2, 20-8, 20-14, 20-29, 20-40
  冗長性 14-43
  冗長性グループ 14-39
  説明 1-5
  ディレクトリ属性 16-12
  リージョン 14-13
  ロード バランシング 14-43
Cisco Unified CallManager Assistant（Unified CM Assistant） 1-7, 8-14, 15-49
Cisco Unified CallManager Express（CME） 2-18, 8-33

Cisco Unified CallManager のアップグレード 8-8
Cisco Unified IP-IVR 15-22, 15-49
Cisco Unified MeetingPlace 15-50
Cisco Unified Video Advantage
説明 19-22
トラフィックの分類 19-40
Cisco Unified Wireless IP Phone 7920 15-51
Cisco Unity 13-1
Cisco Unity Connection のポート グループ 13-7
Cisco Unity Personal Assistant（CPCA） 13-3
Cisco Unity Telephony Integration Manager（UTIM） 13-12, 13-14
Cisco Unity でのネイティブ トランスコーディング 13-10
Cisco Unity との統合 13-7
Cisco Unity の複数のクラスタ 13-7
Cisco Unity の分離統合 13-7
Cisco.com xxv
CKM 19-17
Clear Channel Assessment（CCA） 3-66
CLEC 11-4
CLID 4-13, 10-19
CMC 10-20
CME 2-18, 8-33
CMI 12-2
CMM 7-3, 19-5
COM 16-4
Common Intermediate Format（CIF） 19-26
Communicator 19-11, 19-33, 19-43
Component Object Model（COM） 16-4
Compressed Real-Time Transport Protocol（cRTP） 3-34
Conference Station 19-21, 19-29
Contact Center 1-1, 15-49
Continuous-Presence 会議ビュー 15-16
COR 10-52, 10-92
CorporateDirectory.txt ディレクトリ ファイル 20-34
CoS 3-4, 14-12, 19-29
CPCA 13-3
CPI xxvi
CPN 11-4
cRTP 3-31, 3-34
CTI 8-13, 15-2, 15-48
CTI Manager 8-4, 8-13
CTI ルート ポイント 6-18, 8-21

D

DAI 18-20, 18-21
DHCP
オプション 150 3-13
サーバ 3-15
スターベーション攻撃 18-19
スヌーピング 18-17, 18-20
説明 3-12
配置オプション 3-14
バインディング情報 18-20
リース期間 3-13
DID 4-13, 11-4
Differentiated Services Code Point（DSCP） 3-4, 3-32, 14-12
DiffServ 14-12
Digital PBX Adapter（DPA） 12-4, 12-7
Digital Set Emulation（DSE） 12-4
DMZ 14-16, 14-30, 18-48
DN 10-99
DNS 3-11, 14-15, 14-30
Domino Unified Communications Services（DUC） 13-3
DPA 12-4, 12-7
DS0 8-20
DSCP 3-4, 3-32, 14-12
DSE 12-4
DSP リソース
C542 チップセット 6-7
C5421 チップセット 6-5
C549 チップセット 6-6
C5510 チップセット 6-4
PVDM 6-23
音声インターフェイスの 6-3
計算 6-25
コール数 6-4, 6-5, 6-6, 6-7
説明 6-2
単一サイト配置モデルの 2-3
マルチサイト配置モデルの 2-7, 2-16
DTMF 4-3, 4-6, 5-13, 6-16, 6-17
Dual Tone Multifrequency（DTMF） 4-3, 4-6, 5-13, 6-16, 6-17
DUC 13-3
Dynamic ARP Inspection（DAI） 18-20, 18-21
Dynamic Host Configuration Protocol（DHCP） 3-12, 18-17, 18-19, 18-20

E

E1 トランク 14-23
E.164 アドレス 10-73, 10-74, 11-4, 11-7, 14-39
E911 11-1, 11-3
EAP 3-67
EAP-FAST 3-67, 19-16
ECM 4-23
ECS 15-2
ELIN 11-6, 11-7
EM（「エクステンション モビリティ」を参照）
Emergency Responder（ER） 10-63, 11-9, 11-13, 15-48
EMP 14-33, 15-15
Empty Capabilities Set（ECS） 15-2
Enhanced Media Processor（EMP） 14-33, 15-15
Enhanced Media Termination Point 15-3
Enterprise MCM 8-22
ER 10-63, 11-13, 15-48, 19-20
ERL 11-6, 11-7, 11-13
ettercap ウイルス 18-21
Extensible Authentication Protocol（EAP） 3-67, 19-16
Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling（EAP-FAST） 3-67, 19-16

F

FAC 10-20
Fast Start 6-14
FAX
- T.38 4-30
- インターフェイス モジュール 19-2, 19-3
- エラー訂正モード 4-23
- 機能の相互運用性 4-26
- クロッキング ソース 4-30
- ゲートウェイ サポート 4-3, 4-22
- サポートされる機能 4-27
- サポートされるプラットフォームと機能 4-24
- サポートされるプロトコル 4-25
- パススルー モード 4-22
- リレー モード 4-22

FAX とモデム サポートのクロッキング ソース 4-30
Firewall Services Module（FWSM） 18-31, 18-33, 18-39
Foreign Exchange Office（FXO） 11-6
Foreign Exchange Station（FXS） 12-3
FWSM 18-31, 18-33, 18-39
FXO 11-6
FXS 12-3

G

GARP 18-7, 18-21
Gatekeeper Transaction Message Protocol（GKTMP） 5-12
Gatekeeper Update Protocol（GUP） 5-4, 8-25
Gateway System Integrity Manager（GWSIM） 14-12, 14-18
GKTMP 5-12
Gratuitous Address Resolution Protocol（GARP） 18-7, 18-21
GUP 5-4, 8-25
GWSIM 14-12, 14-18

H

H.225 トランク 5-4, 5-11
H.245 4-31
H.320 15-35, 15-41
H.323
- Annex M1 5-12
- Cisco Unified CallManager における 5-10
- Cisco Unified MeetingPlace でのサポート 14-19
- Fast Start 6-14
- FAX とモデムのサポート 4-25
- MCU リソース 14-9, 15-19
- SIP IP Gateway 14-6, 14-20, 14-42
- T.38 FAX リレー 4-33
- アナログ ゲートウェイ 4-14
- クライアント 14-39, 15-28, 15-38
- ゲートウェイ 4-3
- コール 5-11
- コール ヘアピン 8-33
- サービス クラス 10-92
- ゾーン プレフィックス 15-38
- ダイヤル ピア、コール ルーティングのための 10-39
- 単一サイト配置モデルの 2-5
- デジタル ゲートウェイ 4-16, 4-17, 4-18, 4-19
- 動的アドレッシング 14-39
- トランク 5-3, 5-9
- ビデオ エンドポイント 15-2, 19-41
- 補足サービス 6-14

NM-HD-1V/2V/2VE モジュール 6-9, 6-12, 6-18

HSRP 2-17, 3-7, 8-22, 8-23

I

IBM Cabling System（ICS） 3-22
IButton 10-15
ICCS 2-20, 2-25, 8-5
ICMP 4-12
ICS 3-22
IDS 2-20, 18-31
IM ゲートウェイ 14-2
Informix Dynamic Server（IDS） 2-20
Intra-Cluster Communication Signaling（ICCS） 2-20, 2-25, 8-5
Intrusion Detection System（IDS） 18-31
IntServ/DiffServ モデル 3-44, 3-47
IntServ モデル 3-42, 3-47
invia 9-31, 10-46, 15-36
IOS
ゲートキーパー 15-24
コール ルーティング 10-39, 10-42
コール特権 10-52
サービス クラス 10-92
サポートされる DSP リソース 6-4, 6-5, 6-6, 6-7
ソフトウェア MTP 6-18
番号操作 10-55
必要な最小リリース 19-3
IP 14-18
IP Communicator 1-5, 19-11, 19-33, 19-43
IP Conference Station 19-21, 19-29
IP Contact Center（IPCC） 15-49
IP/H323 機能セット 8-22
IP-IP ゲートウェイ（IPIPGW） 9-30, 9-36, 9-59, 10-46
IP Phone 19-7
IP Phone Service 20-2
エクステンション モビリティ 20-8
サービス 20-2
サービス パラメータ 20-2, 20-3, 20-8, 20-9, 20-14, 20-15
ソフトウェアベースの 1-5
IP Phone Service 20-2
IP Phone サービス 1-7
IP Phone の設定 18-10
IP Security Protocol（IPSec） 2-7, 2-16
IP SoftPhone 15-50
IP-to-IP ゲートウェイ（IPIPGW） 9-30, 9-36, 9-59, 10-46
IP Voice Media Streaming Application 6-9, 6-18, 6-20, 6-22, 8-13
IP VOICE 機能セット 8-33
IP アドレス
隠蔽 6-29
セキュリティ 18-5
IP ゲートウェイ 14-6, 14-42
IP 公衆網 6-29
IP ソース ガード（IPSG） 18-24
IP テレフォニー 1-1, 1-3, 14-1
IP テレフォニー機能に関するアクセシビリティ 2-28
IP ビデオ テレフォニー
Cisco CallManager における機能拡張 15-2
MTP 15-3
コンポーネント 15-1
セキュリティ 18-10
説明 1-1, 1-6, 15-1
トランスコーディング 15-3
IP ビデオ テレフォニー用の Cisco Unified CallManager の機能拡張 15-2
IP ビデオ会議（IP/VC） 14-32, 14-40, 14-44
IP ポート 14-23
IP 優先順位 3-4, 3-32, 14-12
IPCC 15-49
IPIPGW 9-30, 9-36, 9-59, 10-46
iPlanet Directory Server 16-11, 16-15
IPSec 2-7, 2-16
IPSG 18-24
IP/VC 3500 シリーズ ビデオ ゲートウェイ 4-34
IP/VC Enhanced Media Processor（EMP） 14-33
IP/VC MCU 14-32, 14-40, 14-44
ISDN 2-8, 2-11, 4-41
IVR 2-6, 15-22, 15-49

J

JTAPI 8-13, 15-2

K

Keypad Markup Language（KPML） 10-3, 10-10, 10-12
KPML 10-3, 10-10, 10-12

L

LAN インフラストラクチャ　3-4
LBR　6-27
LCF　8-29, 10-46
LCR　4-40
LDAP　8-5, 16-1
LDN　11-4
LEAP　3-67, 19-16, 19-17
LEC　11-2, 11-11
LFI　3-31, 3-34, 3-35
Lightweight Directory Access Protocol（LDAP）　8-5, 16-1
Link Fragmentation and Interleaving（LFI）　3-31, 3-34, 3-35
Listed Directory Number（LDN）　11-4
LLQ　3-31, 3-32
LMHOSTS ファイル　3-11
Low-Latency Queuing（LLQ）　3-31, 3-32
LRJ　10-46
LRQ　8-29, 10-46
LRQ ブラスト　8-29

M

MAC アドレス　18-14
Manager Assistant　15-49
Maximum Serving Count サービス パラメータ　3-19
MC　15-15
MCM　5-12, 8-22, 15-24, 15-38
MCS　14-28
MCU
　H.323 または SIP　15-19
　Skinny Client Control Protocol（SCCP）と　15-17
　キャパシティとサイズ選定　14-9, 15-21
　ゲートキーパへの登録　14-40
　冗長性　14-44
　設定　14-32, 15-33
　ゾーン　15-39
　ゾーン プレフィックス　15-40
　ビデオ テレフォニー　15-1, 15-15
Media Convergence Server（MCS）　14-28
Media Streaming Application　6-9, 6-18, 6-20, 6-22, 8-13
MeetingPlace
　Audio Server　14-6, 14-41
　H.323/SIP IP Gateway　14-6, 14-20, 14-42
　IP テレフォニー ネットワークとの接続　14-12
　IP テレフォニーとの統合　14-1
　Web サーバ　14-28, 14-43
　ゲートキーパの登録　14-40
　コンポーネント　14-6
　コンポーネントで使用されるポート　14-16, 14-19, 14-29, 14-30
　サーバの推奨事項　14-2
　サポートされるプロトコル　14-18
　システムのサイズの選定　14-8
　説明　1-6
　ビデオ アプリケーション　14-31, 14-44
　ビデオ会議　15-50
MeetingPlace と IP テレフォニーの統合　14-1
MGCP　2-5, 4-3, 4-15, 4-20, 4-25, 15-2
Microsoft Active Directory（AD）　16-11, 16-14, 16-17, 16-22
Microsoft ViewMail for Outlook（VMO）　13-3
MISTP　3-4
MLP　3-31
MLPP　6-20
MLTS　11-2
MoH　2-26, 7-1
MP　15-15, 15-16
MPLS　2-7, 2-16, 3-28, 3-31, 9-12, 9-46
MRG　6-25, 9-20, 15-18
MRGL　6-25, 9-20, 15-18
MTP
　Named Telephony Event　6-15
　エンドポイントの IP アドレスの隠蔽　6-29
　オーディオ コンファレンス ブリッジ　6-19
　および H.323 トランク　5-9
　および SIP トランク　5-13
　公衆網コールの　6-29
　説明　6-14
　ソフトウェア リソース　6-18
　単一サイト配置モデルの　2-3
　ハードウェア リソース　6-18, 6-19
　ビデオ コールの　15-3
　マルチサイト配置モデルの　2-7, 2-16
　要件、トランク　8-21
Multilevel Precedence Preemption（MLPP）　6-20
Multi-Line Telephone System（MLTS）　11-2
Multimedia Conference Manager（MCM）　5-12, 8-22, 15-24
Multiple Instance Spanning Tree Protocol（MISTP）　3-4
Multipoint Controller（MC）　15-15
Multipoint Processor（MP）　15-15, 15-16

Multiprotocol Label Switching（MPLS） 2-7, 2-16, 3-28, 3-31, 9-12, 9-46
Music On Hold（MoH） 2-26, 7-1
Music On Hold に使用されるフラッシュ 7-18
MWI 12-7

N

Named Service Event（NSE） 4-25, 4-31
Named Telephony Event（NTE） 4-7, 6-14
National Emergency Number Association（NENA） 11-6, 11-20
NENA 11-6, 11-20
Netscape Directory Server 16-11, 16-15
Network Specific Facilities（NSF） 4-18
NFAS 2-5, 4-18
NIC チーミング 8-3
NM-HDV モジュール 6-10, 6-12
NM-HDV2 モジュール 6-9, 6-12, 6-18
No.7 共通線信号方式 2-5
NPA（番号計画エリア） 10-29
NSE 4-25, 4-31
NSF 4-18
NTE 4-7, 6-14
NTP 3-20, 14-15

O

Open Shortest Path First（OSPF） 18-36
Open 認証 3-67, 19-16, 19-17
OSPF 18-36
outvia 9-31, 10-46, 15-36

P

PA 15-50
PAC 3-67, 19-16
passive-interface コマンド 3-10
PC
  IP Phone のポート 18-6, 19-22
  音声 VLAN へのアクセス 19-22
PCS-1 ビデオ エンドポイント 19-25
PCS-TL50 ビデオ エンドポイント 19-25
Per-Port/Per-VLAN ACL 19-41
Personal Assistant（PA） 15-50
Personal Communicator 1-5
ping ユーティリティ 2-22
PINX 12-7
PIX 18-31, 18-33
PoE 3-21
PortFast 3-6
POTS 11-6
Power over Ethernet（PoE） 3-21
PRI 11-4
Primary Rate Interface（PRI） 11-4
Private Integrated Services Network Exchange（PINX） 12-7
Private Internet Exchange（PIX） 18-31, 18-33
progress_ind alert enable 8 コマンド 11-12
Protected Access Credential（PAC） 3-67, 19-16
Protocol Auto Detect 5-11
PSAP 11-2, 11-8, 11-14, 19-20
PSTN 2-11
Public Safety Answering Point（PSAP） 11-2, 11-8, 11-14, 19-20
PVDM 6-23

Q

QBSS 3-66, 19-18
QBSS 差分しきい値 19-18
QCIF 19-26
QoS
  Attendant Console 20-33
  Cisco Unified CallManager Assistant 20-23
  Cisco Unified MeetingPlace の 14-12
  LAN の 3-23
  Music On Hold 7-13
  RSVP 3-41
  WAN の 3-28, 3-31
  一般的な 1-4
  セキュリティ 18-25
  設定例 19-28
  無線 LAN の 3-68
QoS Basic Service Set（QBSS） 3-66, 19-18
QoS がない場合の障害 3-27
Q.SIG 5-12
QSIG 4-16, 4-21, 12-7, 14-23, 17-4
Quality of Service（QoS）
  Cisco Unified MeetingPlace の 14-12
  LAN の 3-23
  Music On Hold 7-13

RSVP 3-41
WAN の 3-28, 3-31
一般的な 1-4
セキュリティ 18-25
設定例 19-28
無線 LAN の 3-68
Quarter Common Intermediate Format（QCIF） 19-26

R

RADIUS 3-67
Rapid Spanning Tree Protocol（RSTP） 3-4, 3-6
RAS 5-4, 9-16, 10-42, 14-19, 14-39, 15-24
RASAggregator トランク 15-27, 15-32, 15-33
Rate Matching（RM）モジュール 15-15, 15-17
RBOC 11-2
RCP 18-22
RDNIS 13-9
Real Time Monitoring Tool（RTMT） 16-2
Real-Time Transport Protocol(RTP) 2-17, 14-12, 14-18, 15-2
Redirected Dialed Number Information Service（RDNIS） 13-9
Redirector サーブレット 20-43
Registration Admission Status（RAS） 5-4, 9-16, 10-42, 14-19, 14-39, 15-24
Registration Confirm（RCF） 15-43
Registration Request（RRQ） 15-43
Relative Signal Strength Indicator（RSSI） 19-18
Remote Authentication Dial-In User Service（RADIUS） 3-67
Remote Copy Protocol（RCP） 18-22
Reservationless Single Number Access（RSNA） 14-40
Retry Video Call as Audio 15-9
RF 19-16
RCF 15-43
RFC 2833 4-7, 6-14
RIP 18-36
RJ-45 3-22
RM 15-15, 15-17
Route/Switch Processor（RSP） 4-23
Routing Information Protocol（RIP） 18-36
RRQ 15-43
RSNA 14-40
RSP 4-23
RSSI 19-18
RSSI 差分しきい値 19-18
RSTP 3-4, 3-6
RSVP
Cisco RSVP Agent 9-20, 9-22, 9-56
IP-to-IP ゲートウェイ 9-30
RSVP に対応するロケーション 9-18, 15-3
WAN インフラストラクチャ 3-28
コール アドミッション制御 9-8
説明 3-38
ポリシー 9-25
RSVP Agent あたりの最大セッション 9-23
RSVP Agent の登録 9-22
RSVP のアプリケーション ID 3-45, 3-54, 9-29, 15-3
RTMT 16-2
RTP 2-17, 14-12, 14-18, 15-2
RTP ヘッダー圧縮（cRTP） 3-31, 3-34
RTT 2-22, 2-25

S

SCCP
FAX とモデムのサポート 4-25
MCU 上のポート 14-9
MCU リソース 15-17
Music On Hold（MoH） 7-22
ゲートウェイ サポート 4-3
ダイヤル パターン認識 10-3
電話機 10-9
電話機でのユーザ入力 10-9
ビデオ エンドポイント 14-13, 15-2, 19-22, 19-25
SDK 16-4
SDP 4-31, 6-15
Section 255 2-28
Section 508 2-28
Section 508 への準拠 2-28
Sequenced Routing Update Protocol（SRTP） 3-49
Service Set Identifier（SSID） 3-62, 3-66
Session Description Protocol（SDP） 4-31, 6-15
Session Initiation Protocol（SIP）
Annunciator 6-20
Music On Hold（MoH） 7-25
アナログ ゲートウェイ 4-14
ゲートウェイ 4-12, 14-20
ゲートウェイ サポート 4-7
タイプ A 電話機 10-10
タイプ B 電話機 10-12
ダイヤル パターン認識 10-3

ダイヤル規則 10-14, 10-78
デジタル ゲートウェイ 4-16, 4-17, 4-18, 4-19
電話機 10-10, 10-12, 19-27
トランク 5-13, 13-11
ビデオ エンドポイント 15-2, 19-41
分散型コール処理 2-17
Simplified Message Desk Interface（SMDI） 12-1
SIP
Annunciator 6-20
Music On Hold（MoH） 7-25
アナログ ゲートウェイ 4-14
ゲートウェイ 4-12, 14-20
ゲートウェイ サポート 4-7
タイプ A 電話機 10-10
タイプ B 電話機 10-12
ダイヤル パターン認識 10-3
ダイヤル規則 10-14, 10-78
デジタル ゲートウェイ 4-16, 4-17, 4-18, 4-19
電話機 10-10, 10-12, 19-27
トランク 5-13, 13-11
ビデオ エンドポイント 15-2, 19-41
分散型コール処理 2-17
SIW 2-7, 2-16, 3-31
Skinny Client Control Protocol（SCCP）
FAX とモデムのサポート 4-25
MCU 上のポート 14-9
MCU リソース 15-17
Music On Hold（MoH） 7-22
ゲートウェイ サポート 4-3
ダイヤル パターン認識 10-3
電話機 10-9
電話機でのユーザ入力 10-9
ビデオ エンドポイント 14-13, 15-2, 19-22, 19-25
SMDI 12-1
sn 属性 16-11
SNMP 11-9
SoftPhone 11-13, 15-50, 19-12, 19-33, 19-43
Software Development Kit（SDK） 16-4
Sony エンドポイント 19-25
Spanning Tree Protocol（STP） 3-6
SQL データベース 14-29
SRND xxiii
SRST 2-8, 7-18, 8-4, 10-97, 11-3
SRTP 3-49
SS7 2-5
SSID 3-62, 3-66
standby preempt コマンド 3-7
standby track コマンド 3-7
STP 3-6, 3-22
Sun ONE Directory Server 16-11, 16-15
Survivable Remote Site Telephony（SRST） 2-8, 7-18, 8-4, 10-97, 11-3

T

T1 トランク 14-22
T-1000 ビデオ エンドポイント 19-25
T.120 アプリケーション共有 15-50
T.38 FAX リレー 4-30
T-550 ビデオ エンドポイント 19-25
TAC xxvi
Tandberg エンドポイント
説明 15-1, 19-25
トラフィックの分類 19-41
TAPI 8-13, 15-2
TCP 14-16, 14-19, 14-29, 14-30
TCP/UDP ポート 19-40
TCS 15-12
Technical Assistance Center（TAC） xxvi
TEHO 10-58
Telecommunications Act 2-28
TFTP 3-13, 3-15, 8-4, 8-12, 19-22
ToD 10-38
ToS 14-12
TRaP 13-3
Trivial File Transfer Protocol（TFTP） 3-13, 3-15, 8-4, 8-12, 19-22
TTL 15-43
TUI 13-3
Tunneled Q.SIG 5-12

U

UAC 19-6
UAS 19-6
UDC 3-22
UDLD 3-6
UDP 2-17, 3-34, 5-4, 14-16, 14-18, 14-19
UN 4-7
Unified CM Assistant 1-7, 8-14, 15-49
Unified Communications 1-1
Unified Personal Communicator 1-5

Unified Video Advantage
説明 19-22
トラフィックの分類 19-40
Unity 13-1
Unity Telephony Integration Manager（UTIM） 13-7, 13-12, 13-14
Universal Data Connector（UDC） 3-22
Unsolicited SIP Notify（UN） 4-7
UplinkFast 3-6
UPS 3-21
UserID 16-11
User-to-User Information Element（UUIE） 5-11
UTIM 13-7, 13-12, 13-14
UUIE 5-11

V

V.34 モデム 4-24
V3PN 2-7, 2-16
V.90 モデム 4-24
VAD 4-23, 8-14, 15-15
VAF 3-35
VATS 3-37
VG224 音声ゲートウェイ 4-14, 12-2, 19-5, 19-28
VG248 Analog Phone Gateway 4-29, 12-3, 19-6, 19-28
VIC 19-2, 19-3
ViewMail for Outlook（VMO） 13-3
Virtual LAN（VLAN） 3-4
VLAN
VLAN ID 19-28
VLAN ごとのデバイス数 3-4
Voice 18-13
アクセス コントロール リスト（ACL） 18-26
音声 18-8
音声とデータの VLAN の分離 3-62
ビデオ 18-13
VMO 13-3
Voice
VLAN 18-13
Voice-Activated 会議ビュー 15-15
Voice over IP（VoIP） 3-49
Voice Over the PSTN（VoPSTN） 2-11
voice rtp send-recv コマンド 11-12
Voice-Adaptive Fragmentation（VAF） 3-35
Voice-Adaptive Traffic Shaping（VATS） 3-37
VoIP 3-49
VoPSTN 2-11
VPN 2-7, 2-16
VWIC 19-2

W

Wait for Far-End to Send TCS 15-12
WAN
アグリゲーション ルータ 3-3
インフラストラクチャ 3-28
WAN を介したクラスタ化
Cisco Unity 13-21, 13-23
Cisco Unity でのフェールオーバー 13-26
MeetingPlace 14-5
Music On Hold 7-21
WAN の考慮事項 2-19
説明 2-19
トラブルシューティング 2-23
リモート フェールオーバー 2-27
ローカル フェールオーバー 2-23
Web
IP Phone からのアクセス 18-9
会議 14-9, 14-14, 14-28
サーバ 14-28, 14-43
Web 会議のネットワーク使用率 14-14
Web セッションあたりの送信データ 14-14
WebDialer 1-7, 20-13, 20-40
WebDialer の URL 20-46
WEP 3-67, 19-16
Wi-Fi Protected Access Pre-Shared Key（WPA-PSK） 19-17
Wi-Fi Protected Access（WPA） 3-67, 19-16
Windows Internet Naming Service（WINS） 3-15
WINS 3-15
Wired Equivalent Privacy（WEP） 3-67, 19-16
WLAN インフラストラクチャ 3-62
WLAN 上のマルチキャスト トラフィック 3-65
WPA 3-67, 19-16
WPA-PSK 19-17
WS-SVC-CMM-ACT モジュール 6-10, 6-12, 6-19
WS-X6608-E1 モジュール 6-10, 6-13, 6-19
WS-X6608-T1 モジュール 6-10, 6-13, 6-19
WS-X6624 モジュール 12-2, 12-3
WS-X6624-FXS アナログ インターフェイス モジュール 19-5

X

XML 14-21
XML サービス 15-51

あ

アーキテクチャ
Attendant Console の 20-30
Cisco Unified CallManager Assistant の 20-16, 20-18
IP Phone Service の 20-3
IP テレフォニーの 1-3
WebDialer の 20-41, 20-44
エクステンション モビリティの 20-10
ディレクトリの 16-8
アクセス コード 10-8, 10-29
アクセス コントロール リスト（ACL） 18-26, 18-28, 19-40
アクセス ポイント（AP） 3-62, 3-65, 19-16
アクセス ポート 14-27
アクセス レイヤ 3-4
アップスピード 4-23
宛先、コール 10-29
アドミッション確認（ACF） 10-45
アドミッション拒否（ARJ） 10-45
アドミッション制御（「コール アドミッション制御」を参照）
アドミッション要求（ARQ） 10-45
アドレス
H.323 クライアント 14-39
MAC 18-14
アドミッション要求（ARQ） 10-45
解決 10-45, 10-46
セキュリティ 18-5
アドレス解決プロトコル（ARP） 3-66, 18-21
アナログ
インターフェイス モジュール 19-2, 19-3
ゲートウェイ 4-2, 4-14, 4-24, 19-2
アプリケーション
Attendant Console 20-29
IP Phone Service 20-2
WebDialer 20-40
一般的な 1-7
エクステンション モビリティ 20-8, 20-28, 20-38, 20-48
サードパーティ製 1-1
サイズの選定とスケーラビリティ 8-14
セキュリティ 18-42
説明 20-1
ビデオ テレフォニー 15-48
アプリケーション ユーザ 16-8
暗号化
シグナリングの 3-58, 3-59
電話機の 18-11
アンチウイルス 18-43

い

移行
Cisco Unified CallManger 4.0 からの 15-47
IP テレフォニーへの 17-1
静的ロケーションから RSVP コール アドミッション制御へ 9-26
段階的な方法 17-2
パラレル カットオーバー 17-3
一般電話サービス（POTS） 11-6
移動、追加、および変更 11-9
インスタント メッセージング（IM）ゲートウェイ 14-2
インターネット プロトコル（IP） 14-18
インターネット制御メッセージ プロトコル（ICMP） 4-12
インターフェイス モジュール 19-2
インフラストラクチャ ゲートキーパー 15-25
インフラストラクチャ（「ネットワーク インフラストラクチャ」を参照）
インライン パワー 3-21

え

エクステンション モビリティ（EM）
Attendant Console との相互作用 20-38
Cisco Unified CallManager Assistant（Unified CM Assistant）との相互作用 20-28
WebDialer との相互作用 20-48
サーバのキャパシティとパフォーマンス 8-14, 8-20
説明 1-7, 20-8
ダイヤル プラン 10-31, 10-83, 10-89
プロファイル 8-20
エグゼクティブ IP Phone 19-9
エコー キャンセレーション 4-23
エラー訂正モード（ECM） 4-23

エラー率 2-22
エリア コード 10-29
エンド ユーザ 16-8
エンドポイント
H.323 19-41
H.323 クライアント 15-28
IP アドレスの隠蔽 6-29
SCCP 19-22
SIP 19-41
Sony 19-25
Tandberg 19-25, 19-41
アナログ ゲートウェイ 19-2
回線グループ デバイス 10-38
機能 19-43
ゲートキーパー 15-25, 15-27
ゲートキーパー出力 8-28
ゲートキーパの登録 8-28
サポートされるコーデック 15-6
ソフトウェアベースの 1-5, 19-11, 19-33
存続可能時間 15-43
代替 5-12
タイプ 19-1
定義済み 1-5
ディレクトリ アクセス 16-4
ビデオ 1-6, 14-28, 15-1, 19-22, 19-40
補足サービス 6-14
無線 1-6, 19-16
エンドポイント ゲートキーパーの要約 15-44
エンドポイントの IP アドレスの隠蔽 6-29
エンドポイントの機能 19-43

お

応答監視 11-12
オーディオ ソース 7-3, 7-11
オーディオ会議 14-8, 14-25, 14-28
オーバーラップ
チャネル 3-63
オープン フォーラム会議 14-30
同じクラスタにバージョンの異なる Cisco Unified CallManager がある 3-18
同じ場所にある Cisco Unified CallManager クラスタ 9-54
オプション 150 3-12, 3-13
オフネット ダイヤリング 10-4
重み付け均等化キューイング 3-32
音声
VLAN 18-8
会議 14-8, 14-25, 14-28
ゲートウェイ 4-1, 19-2, 19-5
終端 6-2
帯域幅の要件 3-34
トランスレーション プロファイル 10-55
ベアラ トラフィック 3-49, 3-53
ポート統合 13-12, 13-14
リンク 14-31
音声 /WAN インターフェイス カード（VWIC） 19-2
音声アクティビティ検出（VAD） 4-23, 8-14, 15-15
音声インターフェイス カード（VIC） 19-2, 19-3
音声およびビデオ対応 IPSec VPN（V3PN） 2-7, 2-16
音声自動応答装置（IVR） 2-6, 15-22, 15-49
音声トラフィックのキューイング 3-26, 3-69
音声のみのコール 15-9
音声パケットのヘッダー 3-49
オンネット ダイヤリング 10-4, 10-5, 10-7, 10-62, 10-64, 10-70

か

会議
MeetingPlace 1-6
Web 14-14, 14-28
オーディオ 14-25
音声 14-25
カスケード化 14-27, 14-30, 14-38
機能 1-6
組み込みリソース 6-10
システムのサイズの選定 14-8
使用率の計算 14-8, 14-9
スケジューリング 14-27, 14-33
セグメント化 14-30
説明 6-8, 14-25
ソフトウェア リソース 6-9
タイプ 14-34
ネットワーク使用率 14-14
ハードウェア リソース 6-9, 6-10
ビデオ 14-30
ビデオ エンドポイントを使用したオーディオ専用 14-28
ビデオ会議への参加 14-34
ポート 14-27, 14-30, 14-33
リソース 6-8, 15-15, 15-22

リッチメディア　1-1
会議のスケジューリング　14-27, 14-33
解決、アドレス　10-45, 10-46
回線 / デバイス アプローチ、サービス クラスへの　10-84
回線グループ　10-33, 10-37, 10-99
回線グループ デバイス　10-38
回線上の突起物　18-36
回線速度のミスマッチ　3-36
改訂の履歴　xxiv
確実な接続解除監視　12-12
拡張モジュール 7914　19-10
過剰予約ポート　14-27, 14-33
数
ゲートウェイ　8-20
コール　8-21
電話機　8-19
トランク　8-21
カスケードされた会議　14-27, 14-30, 14-38
カスタマー コンタクト　1-1
カスタマー サポート　xxvi
仮想 LAN（VLAN）　3-62, 19-28
仮想タイ ライン　3-61
カットオーバー　17-1, 17-3
カテゴリ 3 ケーブリング　3-21
カバレッジ、コールの　10-96
可変長のオンネット ダイヤル プラン　10-7, 10-64, 10-70
簡易ネットワーク管理プロトコル（SNMP）　11-9
関連資料　xxiii

き

キープアライブ メッセージ　14-35
技術上の問題に関するサポート　xxvi
機能交換、T.38 FAX リレーの　4-31
キャパシティ ツール　8-16, 8-17, 8-18
キャパシティ プランニング
Cisco Unified CallManager サーバ　8-16, 8-17, 8-18
CTI ルート ポイントとポート　8-21
Music On Hold　7-15
ゲートウェイ　8-20
サードパーティ制御の回線　8-21
電話機　8-18
トランク　8-21
無線ネットワーク　19-17
キャンセレーション、エコーの　4-23
キャンパス
アクセス スイッチ　3-3
インフラストラクチャ要件　3-1
キュー項目数　3-60
休止トラフィック　3-61
強制アカウント コード（FAC）　10-20
競争的地域通信事業者（CLEC）　11-4
共存サーバ　3-15, 7-3
共有
T.120 アプリケーション　15-50
鍵認証　19-17
緊急応答ロケーション（ERL）　11-6, 11-7, 11-13
緊急コール　10-63
緊急コール ストリング　11-10
緊急コールのコール ルーティング　11-19
緊急サービス　11-1
緊急プライオリティ　10-19
緊急ロケーション識別番号（ELIN）　11-6, 11-7

く

組み込み会議　6-10
クライアント
H.323　15-28
ゾーン　15-36
クライアント証明書コード（CMC）　10-20
クラスタ
Emergency Responder（ER）　11-19
同じ場所にある　9-54
サービス　8-4
冗長性　8-10
設計ガイドライン　8-2
複数、Cisco Unity の　13-7
クラスタ間トランク
SIP を使用した　5-13
ゲートキーパー制御　5-3
非ゲートキーパー制御　5-3
クラスタ全体のパラメータ　9-25
クリッピング　2-8
グループ
Cisco Unified CallManager の冗長性　5-3, 8-8
Emergency Responder（ER）　11-15, 11-16
回線番号（ハンティング）　10-33
コール ルーティング　10-21
ポート　13-7

メディア リソース 6-1

け

計算、サーバのキャパシティ 8-17
計算式
コーリング サーチ スペース 10-83, 10-87
帯域幅 3-57, 3-59
パーティション 10-83, 10-87
ゲートウェイ 4-31
911 サービス 11-11
Cisco IOS 4-28, 4-29
Cisco Unified CallManager での設定 4-42
Cisco Unified Videoconferencing 3500 シリーズ ビデオ ゲートウェイ 4-34
DS0 8-20
FAX サポート 4-22
FAX とモデム サポートの設定例 4-28
H.320 15-35, 15-41
H.323/SIP 14-6, 14-42
IP 14-6, 14-42
IP-to-IP 9-30, 9-36, 9-59, 10-46
Music On Hold 7-3
Named Service Event（NSE）を使用して制御される 4-31
QoS の設定例 19-28
QSIG サポート 4-21
SIP 4-7, 4-12
V.34 モデム サポート 4-24
V.90 モデム サポート 4-24
VG224 4-14, 12-2, 19-5
VG248 4-29, 12-3, 19-6
WS-X6624 12-2, 12-3
アナログ 4-2, 4-14, 4-24, 19-2
音声アプリケーション 4-1, 19-2, 19-5
機能 4-44, 19-43
キャパシティの計算 8-20
コア機能要件 4-3
サービス プレフィックス 4-37
サイト固有の要件 4-13
自動代替ルーティング 4-38
冗長性 4-11
セキュリティ 18-30
選択 4-3
全トランク使用中 11-11
ゾーン プレフィックス 15-42
デジタル 4-2, 4-16, 4-24
配置 11-11
番号操作 4-36
ビデオ テレフォニー用の 4-34
ファイアウォール 18-31
ブロック 11-11
プロトコル 4-3
モデム サポート 4-23
ローカル フェールオーバー用の 2-26
ゲートキーパー
H.225 トランク 5-4, 5-11
IOS 15-24
MCU の登録 14-40
MeetingPlace の登録 14-40
エンドポイントの 8-28, 15-25, 15-27
クラスタ間トランク 5-3
クラスタリング 8-25
コール アドミッション制御 2-17, 9-16
コール ルーティング 10-42
サポートされるプラットフォーム 15-27
集中型配置 10-47
出力例 8-28
冗長性 8-22, 8-29
スケーラビリティ 15-25
設計上の考慮事項 8-22
設定例 8-22
説明 14-39, 15-24
ゾーン 9-16, 15-36
代替 5-12, 8-25
中継ゾーン 9-31, 9-35, 10-46
地理的な復元性 15-25
ディレクトリ 8-29, 10-50
トランクの冗長性 5-4
非互換性 15-25
プロキシ 15-38, 15-40, 15-42
分散型配置 10-49
役割 15-25
要約 15-44
レガシー 9-35
ゲートキーパー制御
H.225 トランク 5-4, 5-11
H.323 クライアント 15-28, 15-32
クラスタ間トランク 5-3
ケーブリング
IBM タイプ 1A および 2A 3-22
カテゴリ 3 3-21

桁数、ダイヤルされる　10-5

こ

コア スイッチ　3-3
コア レイヤ　3-10
高可用性
　音声サービス　2-8
　ネットワーク サービス　3-4
高可用性サーバ　8-2
講義形式の会議　14-30
公衆電話交換網（PSTN）　2-3, 2-8, 2-16, 10-29, 11-2, 14-22
公衆網　2-3, 2-8, 2-16, 6-29, 10-29, 11-2, 14-22
高性能サーバ　8-2
高密度アナログ インターフェイス モジュール　19-3
コーデック
　MeetingPlace の　14-13, 14-18
　Music On Hold　7-10
　エンドポイント デバイスでサポートされている　15-6, 19-26
　サポートされる（複雑度モード別）　6-4
　選択　19-11, 19-14
　タイプ　7-3, 19-11, 19-14
　低ビット レート（LBR）　6-27
　パススルー　9-24
　ビデオ テレフォニー　19-25
　複雑度モード　6-2
　フレックス モード　6-3
コーデックの複雑度モード　6-2
コーデックのフレックス モード　6-3
コーリング サーチ スペース　10-22, 10-24, 10-64, 10-83, 10-87
コール
　911　11-1
　DSP リソースごとのコール数　6-4, 6-5, 6-6, 6-7
　H.323　5-11
　Music On Hold　7-1
　音声のみ　15-9
　カバレッジ　10-96
　緊急　10-63
　クラスタ間のフロー　15-11
　クラスタ内部　10-63, 10-67, 10-72
　サポートされるタイプ　15-2
　シグナリング　4-43
　シナリオ　15-10
　制限　10-52
　速度　3-52
　着信　4-36, 4-41, 10-63, 10-69, 10-76
　転送　10-26, 10-91
　特権　10-22
　トロンボーニング　13-16
　発信　4-37, 4-42, 10-63, 10-67, 10-73
　分類　10-20
　ヘアピン　13-16
　保留　7-7
　メディア保留　7-29
　ルーティング　4-36, 4-37, 10-16, 10-39, 10-42, 11-19
コール アドミッション制御
　Cisco IP Communicator　19-12
　Cisco IP SoftPhone の　19-15
　MPLS　9-12
　Music On Hold　7-17
　RSVP　3-47
　RSVP 対応ロケーション　9-18
　ゲートキーパー　8-22, 9-16, 10-42
　コンポーネント　9-13
　集中型コール処理　9-39, 9-43, 9-48, 9-53
　静的ロケーション　9-13
　静的ロケーションから RSVP への移行　9-26
　設計上の考慮事項　9-38
　説明　9-1, 14-13
　帯域幅設定　14-13
　帯域幅の管理　9-16
　帯域幅の要件　9-14
　トポロジ　9-38
　トポロジ対応　9-8
　トポロジ非対応　9-4
　分散型コール処理　9-40, 9-45, 9-50, 9-56
　ベスト プラクティス　9-3
　別のロケーションへのデバイスの移動　11-13
　無線アクセス ポイント　19-19
　要素　9-13
　リージョン　14-13, 15-5
　ロケーション　15-8
コール シグナリングのタイマー　4-43
コール フロー
　MeetingPlace オーディオ コール　14-25
　MeetingPlace ビデオ コール　14-35
　Music On Hold　7-6, 7-22, 7-25
　メディア保留　7-29

コール関連トラフィック　3-61
コール詳細レコード（CDR）　2-22
コール処理
　エージェント　1-5, 2-18
　ガイドライン　8-1
　ゲートキーパーを使用した　8-22
　サブスクライバ サーバ　8-7
　集中型　2-6, 9-39, 9-43, 9-48, 9-53, 13-15, 13-17
　冗長性　4-3, 8-8
　ハードウェア プラットフォーム　8-2
　分散型　2-15, 9-40, 9-50, 9-56
　分散型配置　9-45
コール処理のエージェント　1-5, 2-18
コール制御トラフィック　3-56, 3-61
コール制限　10-22, 10-52
コール特権　10-22, 10-52
コールの終端　6-2
コールの速度　3-52
コールの転送　10-26, 10-91
コールバック
　PSAP から　11-8, 11-14
　緊急サービス　11-8, 11-14
国際コール　10-18
コミュニケーション メディア モジュール（CMM）　7-3, 19-5
コラボレーション
　機能　1-6
　ソリューション　15-50
混在システム ポートのキャパシティ　14-23
混在モード動作　3-18
コンソール
　Unified CM Assistant アシスタントの　20-23
　コンソール担当者用　15-49, 20-29
コンピュータ / テレフォニー インテグレーション（CTI）　8-13, 15-2, 15-48
コンポーネント
　IP ビデオ テレフォニー　15-1
　MeetingPlace　14-6
　メッセージング システム　13-6

さ

サードパーティ製
　SIP 電話機　19-27
　制御の回線　8-21
　ソフトウェア アプリケーション　1-1
　ビデオ エンドポイント　19-25
　ボイスメール システム　12-1, 12-12
サーバ
　Cisco Unified CallManager の　8-2
　CTI Manager　8-13
　DHCP の　3-15
　Music On Hold　7-3, 7-5, 7-14
　TFTP　8-12
　エクステンション モビリティ（EM）の　8-14
　キャパシティ プランニング　8-16, 8-17, 8-18
　共存　3-15, 7-3
　高可用性　8-2
　高性能　8-2
　最大数、デバイスの　8-17
　サブスクライバ　2-21, 8-7
　シャドウ サーバ　14-41
　冗長性　14-41
　推奨される配置　14-2
　スタンドアロン　3-15, 7-3
　セキュリティ　18-42, 18-44
　タイプ　8-2
　データ センター　3-10
　パフォーマンス　8-16
　パブリッシャ　2-21, 8-7
　ファーム　3-10
　複数の Cisco Unified CallManager サーバ　13-27
　メディア リソースの　6-1
　リモート マウント　3-19
サービス
　IP Phone 用　20-2
　クラスタ内部　8-4
　テンプレート　15-20
　～の要求　xxvii
　プレフィックス　4-37, 15-20, 15-34, 15-36
　補足　4-3
サービス インターワーキング（SIW）　2-7, 2-16, 3-31
サービス クラス（CoS）　3-4, 14-12, 19-29
サービス クラス、ユーザの　10-80, 10-84, 10-92
サービス パラメータ
　Attendant Console の　20-29
　Cisco Unified CallManager Assistant の　20-14, 20-15
　IP Phone Service の　20-2, 20-3
　Maximum Serving Count　3-19
　WebDialer の　20-40, 20-41
　エクステンション モビリティの　20-8, 20-9

サービス設定を定義するテンプレート　15-20
サイズの選定
　CallManager サーバ　8-16, 8-17, 8-18
　Cisco Unified MeetingPlace　14-8
　MCU　15-21
最低料金選択機能（LCR）　4-40
サイト
　ダイヤリング コード　10-7, 10-76
　無線ネットワークの調査　19-16
サブスクライバ サーバ　2-21, 8-7
サブネット　15-42
差分しきい値　19-18
サポート
　コーデック　15-6, 19-26
　コール タイプ　15-2
　プロトコル　15-2
サポート、利用　xxvi
サポートされる
　ゲートキーパーのプラットフォーム　15-27

し

シールド付きツイストペア（STP）　3-22
シェアド
　Cisco Unified CallManager Assistant のライン モード　20-17
　ライン アピアランス　3-59, 11-14
時間帯（ToD）ルーティング　10-38
しきい値、差分　19-18
シグナリングの暗号化　3-58, 3-59
時刻同期　3-20
ジッタ　2-20, 4-22, 4-24, 14-15
ジッタ用のバッファ サイズ　14-15
支店のルータ　7-18
自動検出　8-33
自動代替ルーティング（AAR）
　Cisco Unity を使用した　13-9
　Voice Over the PSTN 用　2-11, 2-13
　ダイヤル プランの考慮事項　10-28
　ハント パイロットを使用した　10-97
　ビデオ コールの　4-38, 15-9
　無線 IP Phone を使用した　19-20
自動ネゴシエーション　3-21
自動番号識別（ANI）　4-13, 11-4, 11-6, 11-7
自動ロケーション識別（ALI）　11-4, 11-20
シビラティのレベル、サービス リクエストの　xxvii
シャドウ サーバ　14-41
集中型ゲートキーパー配置　10-47
集中型コール処理
　Voice Over the PSTN　2-11
　コール アドミッション制御　9-39, 9-43, 9-48, 9-53
　コール カバレッジ　10-96
　集中型メッセージング　13-15
　配置モデル　2-6
　ハント リスト　10-96
　分散型メッセージング　13-17
集中型メッセージング　13-3, 13-15, 13-21, 13-27
従来のアプローチ、サービス クラスに対する　10-80
順次 LRQ　8-29
障害回復　14-41
冗長性
　Attendant Console　20-36
　Cisco Unified CallManager Assistant　20-24
　Cisco Unified MeetingPlace の　14-41
　IP Phone Service　20-6
　IP-to-IP ゲートウェイ　9-33
　Music On Hold　7-13
　TFTP サービス　3-16
　WebDialer　20-47
　エクステンション モビリティ　20-11
　クラスタ設定　8-10
　グループ　14-39
　ゲートウェイ サポート　4-3, 4-11
　ゲートキーパー　8-22
　コール処理　8-8
　ソフトウェアのアップグレード時　8-8
　トランクの　5-4
　リモート サイトの　2-8
　ロード バランシング　8-11
使用率
　DS0　8-20
　電話機　8-19
　トランク　8-21
省略ダイヤリング　10-4
資料
　関連　xxiii, xxviii
　入手　xxv, xxviii
　発注　xxv
信頼　19-28

す

推奨されるハードウェアとソフトウェアのバージョン 2-2, A-1
スイッチ
ポート セキュリティ 18-14
役割と機能 3-3
スイッチオーバー 9-22
スイッチバック 9-22
スキーマ 16-1
スケーラビリティ
Cisco Unified CallManager 8-1
ゲートキーパー 15-25
スタートポロジ 9-38
スタティック Wire Equivalent Privacy（WEP） 3-67
スタティック Wired Equivalent Privacy 3-67
スタンドアロン サーバ 3-15, 7-3
ステルス ファイアウォール 18-36
ストリームの再パケット化 6-14
ストリングの長さ 10-5
スヌーピング 18-17
すべてのポートを予約 14-30

せ

請求先番号（BTN） 11-4
制御シグナリング 3-56, 3-61
制限クラス（COR） 10-52, 10-92
静的 ANI インターフェイス 11-8
静的ロケーション 9-13
セキュリティ
Cisco Security Agent 18-42
DHCP スターベーション攻撃 18-19
DHCP スヌーピング 18-17
IP Phone の設定 18-10
MAC CAM フラッディング 18-14
QoS 18-25
Voice VLAN 18-8
Web アクセス 18-9
アクセス コントロール リスト（ACL） 18-26, 18-28
アンチウイルス 18-43
インフラストラクチャ 18-4
概要 1-8, 18-1, 18-2
クラスタ内通信 8-6
ゲートウェイ 18-30
サーバ 18-42, 18-44
スイッチ ポート 18-14
設定例 18-16, 18-19, 18-23, 18-25, 18-26, 18-28, 18-38, 18-40, 18-46
ディレクトリ 16-16
データ センター 18-42
電話機 18-6
電話機の PC ポート 18-6
ビデオ機能 18-10
ファイアウォール 18-33, 18-48
物理的なアクセス 18-4
不良ネットワーク拡張 18-16
ポリシー 18-2
無線ネットワーク 3-67
メディア リソース 18-30
レイヤ 18-3
ロビーに設置された電話機の例 18-46
セキュリティ レイヤ 18-3
セキュリティの概要 18-2
セグメント化会議 14-30
接続
MeetingPlace と IP テレフォニー コンポーネントとの間の 14-12
WAN のオプション 2-7, 2-16
設定例 15-36, 15-44
Cisco ATA 188 および IP Phone 19-29
Cisco Unified CallManager Express 8-33
DHCP スヌーピング 18-19
Dynamic ARP Inspection 18-23
FAX/ モデム サポート 4-28, 4-29
IP-to-IP ゲートウェイ 9-34
IP ソース ガード 18-25
QoS 19-28
VG224 ゲートウェイ 19-28
VG248 ゲートウェイ 19-28
Wireless IP Phone 7920 19-37
アクセス コントロール リスト（ACL） 18-26, 18-28
エンドポイント ゲートキーパー 15-44
ゲートキーパー 8-22
スイッチ ポート セキュリティ 18-16
ゾーン 15-36
ソフトウェアベースのエンドポイント 19-33
中継ゾーン ゲートキーパー 9-34
ファイアウォール 18-38, 18-40
ロビーに設置された電話機のセキュリティ 18-46
選択ルータ 11-3

全トランク使用中　11-11
全二重方式　3-21
専用回線　2-7, 2-16, 3-31

そ

相互運用性
　FAX とモデム機能の　4-26
　プロトコル　14-18
ソース ガード　18-24
ゾーン
　H.320 ゲートウェイ　15-41
　MCU　15-39
　クライアント　15-36
　ゲートキーパーの設定　15-36
　ゲートキーパー用の　9-16
　サブネット　15-42
　プレフィックス　9-35, 15-38, 15-40, 15-42
即時会議　14-30, 14-34
ソフト クライアント　11-13
ソフトウェア
　MTP リソース　6-18
　エンドポイント　19-11
　オーディオ コンファレンス ブリッジ　6-9
　推奨事項　2-2
　電話機　19-43
　バージョン　2-2, 19-3, 19-5, A-1
　メディア リソース キャパシティ　6-23
ソリューション リファレンス ネットワーク デザイン（SRND）　xxiii
損失、パケットの　4-22, 4-24
存続可能時間（TTL）　15-43

た

帯域幅
　Cisco Unity　13-8
　RSVP の　3-52, 3-59
　一般的な規則　2-20
　音声クラスの要件　3-34
　拡張公式　3-59
　仮想タイ ラインの　3-61
　管理　9-16
　コーデックの選択　14-13
　コール アドミッション制御の要件　9-14
　コール制御トラフィック　3-56, 3-58, 3-61
　シェアドライン アピアランスの　3-59
　消費　3-48, 3-50
　～の要求　5-12
　ビデオ帯域幅の選択アルゴリズム　14-14
　プロビジョニング　3-26, 3-30, 3-48, 14-13
　ベストエフォート型　3-30
　保証　3-30
　無線ネットワークの　3-70
　要件、ゲートキーパー　9-16
　リージョン　14-13
帯域幅計算の拡張公式　3-59
代替
　TFTP ファイル ロケーション　3-19
　エンドポイント　5-12
　ゲートキーパー　5-12, 8-25
タイプ A 電話機　10-2, 10-10
タイプ B 電話機　10-2, 10-12
タイプ オブ サービス（ToS）　14-12
ダイヤリングのパターン認識　10-3, 10-78
ダイヤル パターン認識　10-3, 10-78
ダイヤル パターンの認識　10-78
ダイヤル ピア　10-39, 10-52, 10-55
ダイヤル プラン
　911 コール　11-1
　Cisco Unified CallManager Assistant　20-20
　Cisco Unified MeetingPlace の　14-39
　Voice Over the PSTN 用　2-14
　アクセス コード　10-8
　エクステンション モビリティ　10-31, 10-83, 10-89
　オンネットとオフネット　10-4
　回線グループ　10-33, 10-37
　可変長のオンネット ダイヤリング　10-7, 10-64, 10-70
　機能　10-1
　緊急コール ストリング　11-10
　桁数　10-5
　コーリング サーチ スペース　10-83, 10-87
　コール ルーティング　10-16
　コール特権　10-22, 10-52
　国際コール　10-18
　サービス クラス　10-80, 10-84, 10-92
　サイト コード　10-7
　シェアドライン アピアランス　11-14
　省略ダイヤリング　10-4
　ストリングの長さ　10-5
　設計上の考慮事項　10-57

ダイヤル ピア　10-39, 10-52, 10-55
重複した内線番号　10-5, 10-64
定型オンネット ダイヤリング　10-5, 10-62
パーティション　10-83, 10-87
番号の分配　10-6
ハント リスト　10-33, 10-37
プランニングの考慮事項　10-3, 10-8
分散型コール処理の　10-59
～へのアプローチ　10-60
ボイスメール　10-64, 10-69, 10-76
マルチサイト配置用　10-57
要素　10-9
ダイヤルイン会議　15-22
ダイヤルイン方式（DID）　4-13, 11-4
ダイヤル規則　10-10, 10-12, 10-14, 10-78
単一サイト
配置モデル　2-3, 6-26, 7-16, 14-4
メッセージング モデル　13-3
段階的な移行　17-2
単方向リンク検出（UDLD）　3-6
端末機能セット（TCS）　15-12

ち

地域通信事業者（LEC）　11-2, 11-11
遅延
パケットの　2-19, 2-22, 4-22, 4-24
変動（ジッタ）　4-22, 4-24
チップセット
C542　6-7
C5421　6-5
C549　6-6
C5510　6-4
着信コール　4-36, 4-41, 10-63, 10-69, 10-76
チャネル
バインディング　4-41
ビデオ コールの　4-41
無線デバイスの　3-63
ロールオーバー　4-41
チャネル ビジーアウト　4-41
チャネルのバインディング　4-41
チャネルのロールオーバー　4-41
中央集中型 TFTP サービス　3-17, 3-18
中継ゾーン ゲートキーパー　9-31, 9-35, 10-46
重複
ダイヤル プラン　10-64
内線　10-5
重複受信　10-19
重複送信　10-19
地理的な復元性　15-25

つ

追加情報　xxiii, xxviii
月あたりの平均会議時間（分）　14-8

て

定型オンネット ダイヤル プラン　10-5, 10-62
ディストリビューション レイヤ　3-7
低ビット レート（LBR）コーデック　6-27
低密度アナログ インターフェイス モジュール　19-2
ディレクトリ
Attendant Console の　20-34
Cisco Unified CallManager 4.x での統合　16-6
Cisco Unified CallManager 5.0 での統合　16-6
Cisco Unified CallManager Assistant の　20-23
IP テレフォニー システムとの統合　16-1, 16-2
LDAP　16-1
sn 属性　16-11
UserID　16-11
アーキテクチャ　16-8
アクセス　16-4
検索ベース　16-12
スキーマ　16-1
セキュリティ　16-16
属性　16-12
同期　16-10, 16-11
ユーザの認証　16-10, 16-19
ディレクトリ ゲートキーパー　8-29, 10-50
ディレクトリ データの属性　16-12
ディレクトリの検索ベース　16-12
ディレクトリの同期　16-10, 16-11
ディレクトリ番号（DN）　10-99
データ センター　3-10, 18-42
データベース
Web サーバ上の　14-29
複製　8-5
テールエンド ホップオフ（TEHO）　10-58
適切なルートの選択　10-30
テクニカル サポート　xxvi
デジタル ゲートウェイ　4-2, 4-16, 4-24

デジタル シグナル プロセッサ（「DSP リソース」を参照）
デジタル トランク　14-22
デスクトップ電話機　19-7
デバイス
　回線グループ　10-38
　上限、1 サーバあたりの数　8-17
　ハント リスト　10-99
　プール　2-24, 2-27
　モビリティ　11-13, 19-20
　ルート グループ　10-22
デュアルモード設定　3-18
伝送制御プロトコル（TCP）　14-16, 14-19, 14-29, 14-30
伝搬、データベース　8-5
電話
　VT Advantage と　15-1
　組み込み会議　6-10
　ローミング　3-63
電話機
　7902G　19-7
　7905G　19-7
　7911G　19-7
　7912G　19-7
　7914 拡張モジュール　19-10
　7920 Wireless IP Phone　19-16, 19-37
　7940G　19-8
　7941G　19-8
　7941G-GE　19-8
　7960G　19-9
　7961G　19-9
　7961G-GE　19-9
　7970G　19-10
　7971G-GE　19-10
　7985G IP Video Phone　19-24, 19-25, 19-41
　911 用のロケーション　11-8
　Cisco Unified Video Advantage　19-22
　PC ポート　18-6
　QoS　19-29
　SCCP　10-9
　SIP　10-10, 10-12, 19-27
　Web アクセス　18-9
　エグゼクティブ モデル　19-9
　機能　19-43
　キャパシティの計算　8-18
　セキュリティ　18-6, 18-46
　設定　18-10, 19-18
　ソフトウェアベースの　19-11, 19-33
　タイプ A　10-2, 10-10
　タイプ B　10-2, 10-12
　ダイヤル パターン認識　10-78
　デスクトップ IP モデル　19-7
　認証および暗号化　18-11
　非固定　11-8
　ビジネス モデル　19-8
　ビデオ テレフォニー　19-40
　ベーシック モデル　19-7
　マネージャ モデル　19-8
　無線　1-6, 19-16, 19-37
　ユーザ入力　10-9, 10-10, 10-12
　ライン アピアランス　8-19
　ローミング　19-18, 19-20
電話での録音および再生（TRaP）　13-3
電話ユーザ インターフェイス（TUI）　13-3

と

透過ファイアウォール
　ASA または PIX　18-36
　FWSM　18-39
同期 H.323 クライアント　15-28
統合サービス（IntServ）モデル　3-42, 3-47
統合サービス / ディファレンシエーテッド サービス（IntServ/DiffServ）モデル　3-44, 3-47
動的 ANI インターフェイス　11-7
動的 H.323 アドレッシング　14-39
トークン リング　3-22
特権、コール発信のための　10-22, 10-52
トポロジ
　2 層ハブアンドスポーク　9-42
　MPLS ベース　9-46
　コール アドミッション制御のための　9-38
　スター　9-38
　ハブアンドスポーク　9-16, 9-38, 10-42
　汎用　9-52
トポロジ対応
　コール アドミッション制御　9-8
　ロケーション　15-3
トポロジ非対応コール アドミッション制御　9-4
ドメイン ネーム システム（DNS）　3-11, 14-15, 14-30
トラッキング ドメイン　11-18
トラフィック
　音声ベアラ トラフィック　3-49, 3-53
　キューイング　3-26, 3-69

休止 3-61
コール関連 3-61
コール制御 3-56, 3-61
シェーピング 3-36
～のプロビジョニング 3-49
ビデオ ベアラ トラフィック 3-51, 3-53
分類 3-4, 3-24, 3-68, 14-12, 19-28, 19-40
ベアラ トラフィック 3-49, 3-52
優先順位 3-32
トラフィックのシェーピング 3-36
トラフィックのマーキング 14-12
トラフィックの優先順位 3-32
トラブルシューティング、WAN を介したクラスタ化に関する 2-23
トランク
E1 14-23
H.225 5-4, 5-11
H.323 5-3, 5-9
MTP の要件 8-21
RASAggregator 15-27, 15-32, 15-33
SIP 5-13, 6-20, 13-11
T1 14-22
キャパシティの計算 8-21
クラスタ間、ゲートキーパー制御 5-3
クラスタ間、非ゲートキーパー制御 5-3
冗長性 5-4
説明 5-1
デジタル 14-22
ロード バランシング 5-4, 5-7
トランスコーディング
Cisco Unity 13-10
IP 公衆網 6-29
説明 6-11
ハードウェア リソース 6-12, 6-13
ビデオ テレフォニー 15-3
リソース 6-12
トロンボーニング 13-16

な

内線番号、重複した 10-5

に

二重 PBX 統合 12-5, 12-7
認証
Open 19-17
共有鍵 19-17
電話機の 3-67, 18-11, 19-16
ユーザ 16-10, 16-19
認定情報レート（CIR） 3-37

ね

ネットワーク インフラストラクチャ
Cisco Unified MeetingPlace の 14-11
LAN 3-4
WAN 3-28
WLAN 3-62
アクセス レイヤ 3-4
概要 1-4
コア レイヤ 3-10
高可用性 3-4
セキュリティ 18-4
ディストリビューション レイヤ 3-7
役割 3-3
要件 3-1
ネットワーク サービス 3-11
ネットワーク タイム プロトコル（NTP） 3-20, 14-15
ネットワーク トラフィックの優先順位設定 3-4, 3-32
ネットワーク モジュール 6-24
ネットワーク保留 7-7

の

～の要求
帯域幅 5-12
テクニカル サポートのサービス xxvii
ノンファシリティ アソシエーテッド シグナリング（NFAS） 2-5, 4-18

は

バースト 3-37
バーチャル プライベート ネットワーク（VPN） 2-7, 2-16
パーティション 10-22, 10-23, 10-64, 10-83, 10-87
ハードウェア
DSP リソース 6-4, 6-5, 6-6, 6-7
MTP リソース 6-18, 6-19

Music On Hold 7-14
アナログ インターフェイス モジュール 19-3
オーディオ コンファレンス ブリッジ 6-9, 6-10
ゲートキーパー 8-22
推奨事項 2-2, A-1
トランスコーダ 6-12, 6-13
プラットフォームのタイプ 8-2
メディア リソース キャパシティ 6-23
配置モデル
CallManager Express 8-34
Cisco Unity 13-3
DHCP 3-14
Music On Hold 7-16
Voice Over the PSTN 2-11
WAN を介したクラスタ化 2-19, 7-21, 14-5
集中型コール処理を使用するマルチサイト WAN 2-6, 6-27, 7-16, 10-96, 14-4
説明 2-1, 14-3
単一サイト 2-3, 6-26, 7-16, 14-4
分散型コール処理を使用するマルチサイト WAN 2-15, 6-28, 7-21, 10-59, 10-98, 14-4
マルチサイト ダイヤル プラン 10-57
メッセージング用の結合 13-19
パイロット番号、ハント リストの 10-33, 10-36, 10-99
バグ、報告 xxvi
パケット
ジッタ 2-20
損失 2-20, 4-22
遅延 2-19, 2-22, 4-24, 14-15
ヘッダー 3-49
パケット遅延の変動 14-15
パススルー コーデック 9-24
発呼回線 ID（CLID） 4-13, 10-19
発信コール 4-37, 4-42, 10-63, 10-67, 10-73
発番号（CPN） 11-4
ハブアンドスポーク トポロジ 3-3, 3-28, 9-16, 9-38, 10-42
パフォーマンス
コール レート 8-1
サーバ 8-16
パブリッシャ サーバ 2-21, 8-7
パラメータ
クラスタ全体 9-25
サービス パラメータ 20-2, 20-3, 20-8, 20-9, 20-14, 20-15, 20-29, 20-40, 20-41
パラレル カットオーバー 17-3
番号計画エリア（NPA） 10-29
番号操作 4-36, 10-19, 10-27, 10-55
番号の分配 10-27, 10-55
番号の変換
音声トランスレーション プロファイル 10-55
パターン 10-27
ハント
グループ 10-33
パイロット 10-33, 10-36, 10-99
リスト 10-33, 10-37, 10-99
半二重方式 3-21
汎用トポロジ 9-52

ひ

非 IOS ハードウェア プラットフォーム 6-7
ビーコン 3-66
非ゲートキーパー制御 H.323 クライアント 15-28, 15-33
非ゲートキーパー制御クラスタ間トランク 5-3
非互換性 15-25
非固定電話機 11-8
ビジネス IP Phone 19-8
ビデオ
MeetingPlace Video アプリケーション 14-31, 14-44
VLAN 18-13
エンドポイント 1-6, 14-28, 15-1, 19-22, 19-40
会議 14-9, 14-30
会議ポート 14-33
機能 1-1, 1-6, 18-10
ゲートウェイ 4-34
説明 15-1
トラフィック分類 3-25, 19-40
ベアラ トラフィック 3-51, 3-53
有効 / 無効 19-22
ビデオ テレフォニー（「IP ビデオ テレフォニー」を参照）
ビデオ会議への参加 14-34
ビデオ機能 18-10
ビデオ帯域幅選択のアルゴリズム 14-14
非同期 H.323 クライアント 15-28, 15-33
非同期転送モード（ATM） 2-7, 2-16, 3-31
非武装地帯（DMZ） 14-16, 14-30, 18-48
被保留側 7-6
標準サーバ 8-2
標準の会議 14-26, 14-34

ふ

ファイアウォール
- ゲートウェイの周囲 18-31
- 集中型配置 18-48
- ステルス モード 18-36
- 設定例 18-38, 18-40
- 説明 18-33
- トランスペアレント モード 18-36, 18-39
- ルーテッド モード 18-36, 18-39
- ロード上の突起物 18-36

フェールオーバー
- Cisco Unity 13-4, 13-25, 13-26
- WAN を介したクラスタ化 2-23, 2-27
- 公衆網への 10-73, 10-74
- サブスクライバ サーバ間の 2-21

復元性 5-4, 8-1
複数の Cisco Unified CallManager サーバ 13-27
複製、データベース 8-5
不正
- DHCP サービス 18-17

物理的なセキュリティ 18-4
プライオリティ キュー 3-54
プライオリティ、緊急 10-19
フラット アドレッシング 10-60, 10-70
プラットフォーム 2-2, 8-2, 8-22, 15-27
フランス国内番号計画 10-88
ブリッジ プロトコル データ ユニット（BPDU） 3-6
不良
- ネットワーク拡張 18-16

フレーム リレー 2-7, 2-16, 3-31
プレフィックス
- MCU 15-34
- アクセス コードの 10-29
- ゲートウェイ 15-36
- ゲートキーパー ゾーンに対する 9-35
- サービス 4-37, 15-20
- ゾーン 15-38, 15-40, 15-42

フロー
- クラスタ間のコール 15-11
- コール シグナリング 14-25
- ビデオ会議コール 14-35

フローティング ポート 14-33
プロキシ
- Cisco Unified CallManager Assistant の回線モード 20-16
- SIP 用サーバ 14-20
- ゲートキーパーの 8-22, 15-38, 15-40, 15-42

プロトコル
- ARP 3-66, 18-21
- CDP 18-13, 19-22
- cRTP 3-31, 3-34
- DHCP 3-12, 18-17, 18-19, 18-20
- GARP 18-7, 18-21
- GKTMP 5-12
- GUP 5-4, 8-25
- GWSIM 14-18
- H.225 5-4, 5-11
- H.245 4-31
- H.320 15-35, 15-41
- H.323 2-5, 4-3, 4-14, 4-16, 4-17, 4-18, 4-19, 4-25, 4-33, 5-3, 5-9, 8-33, 10-39, 10-92, 14-9, 14-19, 14-39, 15-2, 15-19, 15-28, 19-41
- HSRP 2-17, 3-7, 8-22, 8-23
- IP 14-18
- IPSec 2-7, 2-16
- JTAPI 15-2
- LDAP 8-5, 16-1
- MGCP 2-5, 4-3, 4-15, 4-20, 4-25, 15-2
- MISTP 3-4
- MLP 3-31
- MPLS 9-12
- NTP 3-20, 14-15
- RAS 10-42, 15-24
- RCP 18-22
- RIP 18-36
- RSTP 3-4, 3-6
- RSVP 3-28, 3-38, 9-8, 9-30, 15-3
- RTP 2-17, 14-12, 14-18, 15-2
- SCCP 4-3, 4-25, 7-22, 10-3, 10-9, 14-9, 14-13, 15-2, 15-17, 19-22, 19-25
- SDP 4-31, 6-15
- SIP 2-17, 4-7, 4-12, 4-14, 4-16, 4-17, 4-18, 4-19, 5-13, 6-20, 7-25, 10-3, 10-10, 10-12, 10-14, 10-78, 13-11, 14-20, 15-2, 19-27, 19-41
- SMDI 12-1
- SNMP 11-9
- SRTP 3-49
- STP 3-6
- TAPI 15-2
- TCP 14-16, 14-19, 14-29, 14-30
- TFTP 3-13, 3-15, 8-4, 8-12, 19-22
- UDP 2-17, 5-4, 14-16, 14-18, 14-19

サポートされる機能 15-2

相互運用性　14-18
ルーティング　3-10
プロビジョニング
H.320 ゲートウェイ　15-35
H.323 クライアント　15-28
MCU　15-33
サーバ　8-16, 8-17, 8-18
プロファイル、エクステンション モビリティ　8-20
分割アドレッシング　10-60, 10-64
分散型ゲートキーパー配置　10-49
分散型コール処理　2-15, 9-40, 9-45, 9-50, 9-56, 10-98
分散型メッセージング　13-4, 13-17, 13-23
分配、ダイヤル プランでの番号の　10-6
分類
コール　10-20
トラフィック　3-4, 3-24, 3-68, 14-12, 19-28, 19-40

へ

ヘアピン　8-33, 13-16
ベアラ トラフィック　3-49, 3-52
ベーシック IP Phone　19-7
ベスト プラクティス、～の
Cisco Unified CallManager Express（CME）　8-34
FAX サポート　4-22
IP-to-IP ゲートウェイ　8-37, 9-32
LDAP 同期　16-16
Music On Hold　7-10
RSVP　3-47
WAN の設計　3-28
回線 / デバイス アプローチ、サービス クラスを構築するための　10-88
コール アドミッション制御　9-3
集中型コール処理　2-8
単一サイト配置　2-5
分散型コール処理　2-17
モデム サポート　4-24
ベストエフォート型の帯域幅　3-30
ベル系地域通信事業者（RBOC）　11-2

ほ

ボイスメール
Cisco Unity　13-1
IP テレフォニー システムとの統合　12-1
SIP トランク　13-11
確実な接続解除監視　12-12
サードパーティ製のシステム　12-1, 12-10, 12-12
集中型　12-7
ダイヤル プラン　10-64, 10-69, 10-76
二重 PBX 統合　12-5, 12-7
ユニファイド メッセージング　13-1
ローカル フェールオーバー用の　2-26
ポート
Cisco Unified Video Advantage の　19-40
Cisco Unity と Cisco Unified CallManager の統合用　13-12, 13-14
CTI　8-21
E1　14-23
IP　14-23
IP Phone の　18-6
MCU 上の割り当て　14-9
PC 接続　19-22
T1　14-23
TCP　14-16, 14-19, 14-29, 14-30
UDP　14-16, 14-19
アクセス　18-15
管理　14-27, 14-33
グループ　13-7
コール シグナリングの　4-43
混在システムでのキャパシティ　14-23
すべてを予約　14-30
セキュリティ　18-14
有効 / 無効　19-22
保証帯域幅　3-30
補足サービス
H.323 エンドポイントの　6-14
ゲートウェイの　4-3, 4-8
ホットスタンバイ ルータ プロトコル（HSRP）　2-17, 3-7, 8-22, 8-23
ポリシー
RSVP の　3-54, 9-25
ネットワーク セキュリティの　18-2
保留　7-1, 7-7
保留側　7-6

ま

マスク、エンドポイントの IP アドレスの　6-29
マネージャ IP Phone　19-8
マルチキャスト Music On Hold　7-2, 7-9, 7-10, 7-12, 7-18, 7-22

マルチサーバ会議　14-27, 14-30, 14-38
マルチサイト WAN 配置モデル
　集中型コール処理を使用する　2-6, 6-27, 7-16, 10-96, 14-4
　分散型コール処理を使用する　2-15, 6-28, 7-21, 10-98, 14-4
マルチサイト ダイヤル プラン　10-57
マルチポイント コントロール ユニット（MCU）
　H.323 または SIP　15-19
　Skinny Client Control Protocol（SCCP）と　15-17
　キャパシティとサイズ選定　14-9, 15-21
　ゲートキーパへの登録　14-40
　冗長性　14-44
　設定　14-32, 15-33
　ビデオ テレフォニー　15-1, 15-15
マルチポイント会議　15-15
マルチメディア コラボレーション　1-6
マルチリンク ポイントツーポイント プロトコル（MLP）　3-31

み

ミーティング
　(「会議」も参照）
　タイプ　14-26, 14-30

む

無線
　IP Phone　1-6, 19-16, 19-37
　IP Phone 7920　15-51, 19-16, 19-37
　LAN　3-62
　エンドポイント　19-16
　ネットワーキング ソリューション　15-51
無線 LAN（WLAN）　3-62
無線周波数（RF）　19-16
無線通信への干渉　3-64
無線ネットワークの調査　19-16
無停電電源装置（UPS）　3-21

め

メッセージ待機インジケータ（MWI）　12-7
メッセージング
　Cisco Unity　13-1
　機能　1-6
　結合された配置モデル　13-19
　システム コンポーネント　13-6
　集中型　13-3, 13-15, 13-21, 13-27
　帯域幅の管理　13-8
　配置モデル　13-3
　フェールオーバー　13-4, 13-25, 13-26
　分散型　13-4, 13-17, 13-23
メッセージング用の結合された配置モデル　13-19
メディア ゲートウェイ コントロール プロトコル（MGCP）　2-5, 4-3, 4-15, 4-20, 4-25, 15-2
メディア ターミネーション ポイント（MTP）
　Named Telephony Event　6-15
　エンドポイントの IP アドレスの隠蔽　6-29
　および H.323 トランク　5-9
　および SIP トランク　5-13
　公衆網コールの　6-29
　説明　6-14
　単一サイト配置モデルの　2-3
　ビデオ コールの　15-3
　マルチサイト配置モデルの　2-7, 2-16
　要件、トランク　8-21
メディア リソース
　PVDM　6-23
　セキュリティ　18-30
　設計ガイドライン　6-25
　説明　6-1
　ハードウェアおよびソフトウェアのキャパシティ　6-23
　ローカル フェールオーバー用の　2-26
メディア リソース グループ（MRG）　6-25, 9-20, 15-18
メディア リソース グループ リスト（MRGL）　6-25, 9-20, 15-18
メディア保留　7-29

も

モデム
　V.34　4-24
　V.90　4-24
　アップスピード　4-23
　機能の相互運用性　4-26
　クロッキング ソース　4-30
　ゲートウェイ サポート　4-3, 4-23
　サポートされる機能　4-24, 4-27
　サポートされるプラットフォーム　4-24
　サポートされるプロトコル　4-25

パススルー モード　4-23
リレー モード　4-23
モデル、配置の（「配置モデル」を参照）
モバイル デバイス　19-20
問題、報告　xxvi

や

役割
ゲートキーパーの　15-25
ネットワーク インフラストラクチャ内の　3-3

ゆ

ユーザ
アプリケーション ユーザ　16-8
エンド ユーザ　16-8
サービス クラス　10-80, 10-84, 10-92
ディレクトリ検索ベース　16-12
電話機での入力　10-9, 10-10, 10-12
ライセンス　14-8
ユーザ エージェント クライアント（UAC）　19-6
ユーザ エージェント サーバ（UAS）　19-6
ユーザ データグラム プロトコル（UDP）　2-17, 3-34, 5-4, 14-16, 14-18, 14-19
ユーザ保留　7-7
ユニキャスト Music On Hold　7-2, 7-9, 7-12, 7-22
ユニファイド メッセージング（「メッセージング」も参照）　13-1

よ

要素、ダイヤル プラン　10-9
予約なしの会議　14-26, 14-30, 14-34

ら

ライセンス　14-8
ライン アピアランス　3-59, 8-19
ラウンドトリップ時間（RTT）　2-22, 2-25

り

リージョン　14-13, 15-5, 15-7
リース期間、DHCP の　3-13
リソース予約プロトコル（RSVP）　3-28, 3-38, 9-8, 9-30, 15-3
リッチメディア会議　1-1
利点、〜の
単一サイト配置　2-4
分散型コール処理　2-17
リモート RSVP Agent　9-56
リモート サイトのサバイバビリティ（呼処理の継続）　2-8
リモート フェールオーバー配置モデル　2-27
リモートマウント サーバ　3-19
履歴、改訂の　xxiv
リンク効率　3-34
リンクのオーバーサブスクリプション　3-36

る

ルータ
E911 用の選択　11-3
RSVP　3-41
アクセス コントロール リスト（ACL）　18-28
支店　7-18
フラッシュ　7-18
役割と機能　3-3
ルーティング
コール　10-16, 10-39, 10-42
最小コスト　4-40
時間帯（ToD）　10-38
着信コール　4-36
発呼回線 ID　10-19
発信コール　4-37
番号操作　10-19
プロトコル　3-10
ルーテッド ファイアウォール
ASA または PIX　18-36
FWSM　18-39
ルート
グループ　10-19, 10-21
グループ デバイス　10-22
選択　10-30
パターン　10-16, 10-18
フィルタ　10-18
リスト　10-21
ルート ガード　3-6

れ

レイヤ 2　2-17, 3-4
レイヤ 3　3-4
レガシー ゲートキーパー　9-35
連想メモリ（CAM）　18-14
連続会議　14-30, 14-34
連続会議サーバ　14-41

ろ

ローカル ダイヤリング エリア　10-30
ローカル フェールオーバー配置モデル　2-23
ロード バランシング　3-16, 5-4, 5-7, 8-11, 14-41
ローミング　3-63, 11-8, 19-18, 19-20
ロケーション
　RSVP 対応　9-18
　静的　9-13, 15-8
　トポロジ対応　15-3
ロケーション確認（LCF）　8-29, 10-46
ロケーション拒否（LRJ）　10-46
ロケーション要求（LRQ）　8-29, 10-46
ロビーに設置された電話機のセキュリティ　18-46

わ

ワイルドカード ルート パターン　10-18